ESTTA Tracking number: **ESTTA667317**
Filing date: **04/17/2015**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

Proceeding	91204456
Party	Plaintiff Intrust Financial Corporation
Correspondence Address	ALICIA E BODECKER FOULSTON SIEFKIN LLP 1551 N WATERFRONT PARKWAY, SUITE 100 WICHITA, KS 67206 UNITED STATES mnorton@foulston.com
Submission	Plaintiff's Notice of Reliance
Filer's Name	Michael Norton
Filer's e-mail	mnorton@foulston.com
Signature	/Michael Norton/
Date	04/17/2015
Attachments	2015-04-17 Rebuttal Notice of Reliance-Part 1.pdf(3434663 bytes) 2015-04-17 Rebuttal Notice of Reliance-Part 2.pdf(2936510 bytes) 2015-04-17 Second Rebuttal Notice of Reliance.pdf(2352673 bytes) 2015-04-17 Third Rebuttal Notice of Reliance.pdf(2298625 bytes)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

Intrust Financial Corporation,	)	
	)	
Opposer,	)	
	)	Opposition No. 91204456
v.	)	Application Serial No.: 85/250992
	)	Mark: NTRUST
nTrust Corp.,	)	
	)	
Applicant.	)	
	)	

Opposer's First Rebuttal Notice of Reliance

Opposer Intrust Financial Corporation ("Intrust"), pursuant to 37 C.F.R. §§ 2.121 and Rule 2.122 of the Trademark Rules of Practice, hereby gives notice that it introduces as evidence and intends to rely upon the documents and testimony identified herein, true and accurate copies of which are filed herewith and incorporated as Exhibits K-1 through K-53. Nothing submitted herein concedes any point or waives any rights or arguments of Opposer concerning the admissibility of any documents or testimony submitted by Applicant.

Except where expressly noted, the internet materials attached hereto display the date accessed and printed and the source URL in accordance with Trademark Rules and *Safer, Inc. v. OMS Investments, Inc*., 94 U.S.P.Q.2d 1031, 1039 (Trademark Tr. & App. Bd. Feb. 23, 2010). Exhibits K-7 through K-13, K-15, and K-20 through 25 are additionally admissible as website printouts of government reports, which are self-authenticating. *Safer*, U.S.P.Q.2d at 1039; 37 C.F.R. § 2.122(e).

Rebuttal Internet Materials re: Services Provided by Banks

Exhibits K-1 through K-17 are articles and papers offered in rebuttal of Applicant's Categories F and G which show that consumers increasingly expect banks to offer mobile person-to-person payment services, and that the Federal Reserve expects and encourages banks to be key players in the emerging stored value card and person-to-person payment markets. These exhibits also evidence that although the Federal Reserve defined "mobile banking" separately from "mobile payments" for purposes of conducting a survey on consumer use of mobile devices for financial transactions, "mobile payments" includes payments made using a bank account. Exhibits K-8, K10 and K-13 are reports that are available through the website for the Federal Reserve Bank of Boston, http://www.bostonfed.org/bankinfo/payment-strategies/mpiw/. Only PDF versions of these reports were available. The reports were accessed through links on Exhibits K-7, K-9 and K-12, respectively, which show the date that the PDFs were accessed and printed and also show the website URL.

Exhibits K-18 and K-19 are articles written by nTrust President Rod Hsu. They are also offered in rebuttal of the exhibits in Applicant's Categories F and G. They are relevant to show that the financial services offered by companies such as nTrust overlap with services that banks provide, and that consumers expect banks to provide, and that "banking" has evolved with technology.

Exhibits K-21 and K-23 are letters from the Comptroller of the Currency Administrator of National Banks. In Exhibit K-21, Chief Counsel for the Comptroller approves Citibank's application to engage in electronic bill payment and presentment services over the Internet and finding that electronic bill presentment is part of the business of banking. Exhibit K-23 contains approval for the development of an Internet bill payment service. These exhibits show that the

"financial services" described in Applicant's registration include services that are part of the business of banking and are offered in rebuttal to the Exhibits contained in Applicant's Categories F and G. Only PDF versions of these letters were available. They were accessed through the website for the Office of the Comptroller of the Currency ("OCC"), http://www.occ.gov/index.html, and more specifically through links shown on Exhibits K-20 and K-22, which show the date that the PDFs were accessed and printed and also show the website URL.

Exhibit K-25 is a Final Rule issued by the OCC in Vol. 67, No. 96 (May 17, 2002) of the Federal Register. This Exhibit is also offered in rebuttal to Applicant's Categories F and G. The OCC notes that national banks must be granted the authority to utilize modern methods and meet modern needs. Under revised § 7.5001, the OCC considers four factors in deciding whether electronic activities are part of the business of a national bank: (i) whether the activity is the functional equivalent to, or a logical outgrowth of, a recognized banking activity; (ii) whether the activity strengthens the bank by benefiting its customers or its business; (iii) whether the activity involves risks similar in nature to those already assumed by banks; and (iv) whether the activity is authorized for state-chartered banks. This Final Rule is a PDF and does not show the date accessed and printed or the URL. It is publically available through the OCC website, http://www.occ.gov/index.html and was accessed through a link on Exhibit K-24, which shows the date that the PDF was accessed and printed, as well as the URL.

Exhibits K-26 through K-53 are printouts of the bank websites of various banks offering mobile payment services and/or stored value cards. These exhibits are offered in rebuttal to Applicant's Category G, to show that person-to-person payment and stored value card services emanate from the same source as more "traditional" bank account services. Exhibit K-41 was

downloaded from the website for Mascoma Bank, at http://www.mascomabank.com/wp-content/uploads/2014/11/Person-To-Person-How-to-Send-a-Payment.pdf. Exhibit K-43 was uploaded from the website for Northeast Bank, at http://www.northeastbank-mn.com/personal/eservices/person-to-person-payments.html. These Exhibits are PDF documents that do not show the date accessed and printed or the URL. However, these documents were accessed through links on the webpages attached as Exhibit K-40 and Exhibit K-42, respectively, which show the date that the PDFs were accessed and printed.

Respectfully submitted,

Dated: April 17, 2015

Michael J. Norton, KS #18732
William P. Matthews, KS #18237
FOULSTON SIEFKIN LLP
1551 N. Waterfront Parkway, Suite 100
Wichita, Kansas 67206-4466
Telephone: 316-291-9743
Facsimile: 866-346-2031
Attorneys for Opposer

Certificate of Service

I certify that a copy of **Opposer's Rebuttal Notice of Reliance** was sent via email to counsel of record as follows:

James D. Nguyen
JimmyNguyen@dwt.com
Davis Wright Tremaine LLP
Suite 2400
865 S Figueroa Street
Los Angeles CA 90017
Attorney for Applicant

on this 17th day of April, 2015.

Michael J. Norton, KS #18732

THE MENTOR FACTOR NEW YORK CITY | MAY 5, 2015
WOMEN HELPING WOMEN BUILD FULFILLING CAREERS
Presented by AMERICAN BANKER
LEARN MORE

AMERICAN BANKER

Banks Should Act Now on Mobile Payments

Karim Ahmad and Gerard du Toit
MAY 19, 2014 12:00pm ET

While start-ups and tech giants have piloted mobile payment solutions over the past few years, most banks have sat on the sidelines waiting to see which, if any, of these efforts will gain traction. Most saw no need to rush in. Only a fraction of bank customers use mobile payments — the early adopters who have the right phones and who seek out willing retailers.

That's about to change. Many consumers are already using their mobile phones to shop online, according to Bain & Company's recent survey of about 25,000 consumers in the U.S. and major Western European markets. In the US, 6.6% of consumers said they have used their smartphones to make in-store purchases. Many more said they expect to begin shopping that way over the next few years. Mobile payments still represent a small percentage of in-store purchases, but that percentage rose by 103% in the U.S. between 2010 and 2013, according to Bain's analysis of reports from sources including Morgan Stanley, Credit Suisse, PayPal and Forbes.

Given these trends, it's time for banks to get serious about integrating mobile payments into their long-term digital strategies. Just as customers embraced online and then mobile banking, they will expect their banks to provide them with mobile payment solutions.

EXHIBIT
K-1

The good news for banks is that even though they're late to the game, no one is better suited to provide payment solutions and digital wallets. Our research shows that consumers trust banks with their data more than they trust retailers, technology companies or alternative payment providers.

But the time to act is now. Bain's research indicates that most customers will have only one or two payment apps on their phone. Banks that want to be one of them will have to act fast.

Lenders that wait for others to create their payment solutions may also find themselves cut out of the conversation between their customers and the payment solution provider. Mobile payments in the U.S. are likely to use the well-established credit card networks, but brand loyalty could shift to the name on the digital wallet such as PayPal or Google Wallet.

The best mobile payment solutions will go beyond treating phones like payment cards. Customers want mobile payment programs that deliver extra value, such as better loyalty rewards or apps that help them manage their money. Of course, these apps must also be secure, widely accepted and easy to use. Where possible, they should also make it easier for customers to shop — for example, by eliminating the need to key in long credit card numbers for online purchases.

As banks plan their mobile payments strategies, executives should keep in mind three important facts.

First, mobile payments are part of a broad transformation to a digital model that includes mobile banking, online payments and using the data from customers' transactions to personalize the banking experience. The payments technology that banks use must harmonize with their overall strategic roadmap.

Second, no single bank has the market power to develop and thrive with its own proprietary solution. Banks will need to build mobile payment systems that work together and depend on common standards. The ideal positioning could be a digital wallet that puts a bank's brand in front of its customers, while relying on existing payment networks.

Finally, banks should be prepared to build new capabilities to make the most of the new data that mobile payments will deliver. Banks will gain crucial insight into what consumers buy and when and where they buy it. This transactional and contextual information should inspire innovation for new products and services. But unless banks can put in place the right people and teams to build on this data, its potential value will remain untapped.

Karim Ahmad and Gerard du Toit are partners with Bain & Company. Karim, based in Atlanta, focuses on payments processing and credit card issuance. Gerard leads Bain's banking and payments practices in the Americas, from Boston.

© 2015 SourceMedia. All rights reserved.

AMERICAN BANKER

P2P Lending: 2B or Not 2B?

by Bonnie McGeer and Glen Fest
FEB 25, 2014 12:00am ET

Peer-to-peer lending is popping up a lot in banking circles all of a sudden, and reactions run the gamut.

At Wells Fargo, some employees received an email late last year saying they cannot participate in P2P lending because companies in that space are considered part of the competition. At the other extreme, tiny Titan Bank in Mineral Wells, Texas, is buying P2P loans for its own portfolio in an unusual alliance with the largest originator in this niche.

But even as more bankers take sides on what some see as a newly emerging battleground, it's fair to say that most have given little thought to the P2P sector so far. Websites such as Lending Club and Prosper, which match up consumers seeking to borrow money with other consumers willing to use their own money to fund those loans, are just not on their radar.

That's about to change.

Though still a microscopic part of the estimated $11 trillion consumer lending market, P2P is going to matter in a big way sooner than you think, say those familiar with the sector. The pioneers in this space are moving past the early losses and regulatory hiccups that held them back for years. They are growing fast, mostly through loans to consolidate credit card debt, and taking some of banks' best customers in the process.

Thanks to their success, more P2P startups are proliferating. Some, like Funding Circle, are using the same model to offer small-business loans.

Now P2P lenders are starting to recruit traditional players in financial services—banks like Titan and institutional investors—to help fund their loans and fuel their growth. A few also are paying banks for customer referrals.

EXHIBIT
K-2

And some online direct lending startups, though still considered part of the P2P sector, do not use "peers" at all in the funding part of the equation. Instead of having individual mom-and-pop contributors risk small amounts, they line up big investors like hedge funds to buy their loans in bulk.

Brendan Ross, president and portfolio manager at the hedge fund Direct Lending Investments, buys small-business loans from online lenders such as IOU Central and QuarterSpot for his fund. The way he sees it, P2P has created an entirely new bank model. It may not be fueled by "peers" as once envisioned. But it is all the more powerful in this new incarnation.

"People think of P2P lending as an Internet phenomenon, but it's not," Ross says. "It's a banking phenomenon."

He says P2P players do almost everything that banks do—market products, evaluate borrowers, underwrite and service loans. "The only thing they're not doing that a bank does is lending their own capital. They're lending other people's capital," he says. "They're like a bank without a balance sheet."

Unlike the spread lending done by traditional banks, this platform lending model, as Ross calls it, makes starting a new bank—or at least the functional equivalent of one—easier than ever, he says. Partly because they don't have the same regulatory burdens as traditional banks, the players in this space can use technology to evaluate risk in new ways and help borrowers that banks reject.

P2P makes sense for sophisticated investors as well. Ross says he generally buys loans that mature in a year or less, with interest rates ranging from 15% to 40%. Default rates usually run from 6% to 8%.

Ross predicts P2P is going to become a major force in lending and he says traditional banks need to figure out how they fit into the new paradigm.

"I believe this decade will see platform lending emerge to rival spread lending," he says.

In his view, the opportunity for banks is in "monetizing their declines," by vetting these new types of lenders, partnering with reputable ones, and referring customers who get turned down for bank loans. QuarterSpot recently began working with banks in this way, paying an origination fee for the referrals.

If bankers are skeptical, the peer-to-peer sector's bumpy start could be partly to blame. But those familiar with P2P say it is now in its "2.0" stage.

Companies like Lending Club and Prosper, which helped create this niche, look much different than they used to. Over the past year, they have been making headlines that illustrate as much.

Lending Club, for example, received a $125 million investment from Google and added Larry Summers, the former U.S. Treasurer, to an already substantial board that includes former Morgan Stanley titans John Mack and Mary Meeker. It has plans to do an initial public offering sometime this year.

Prosper received a $20 million investment from Sequoia Capital upon bringing in a new management team in early 2013. The team quickly made changes to improve the borrowing and lending experience. Just as significantly, it settled a longstanding class-action lawsuit by Prosper "1.0" investors for $10 million, putting a close to a problematic first stage in which defaults soared above 36%. The company also has high-profile board members of its own, including the Consumer Financial Protection Bureau's former deputy director, Raj Date.

Both Lending Club and Prosper expect this year to be particularly momentous for the P2P sector, given the growth tear they are on. Prosper, which began operating in 2006, surpassed the $1 billion mark in total loan issuance last year. Ron Suber, its head of global sales, says he expects the company will loan out another $1 billion in 2014 alone.

Lending Club, launched in mid-2007, had just $3.5 million in first-year originations. But its total lending has grown to $3.4 billion, with $2 billion of that coming in 2013. December was another record month, with $240 million issued through more than 17,000 personal loans.

Scott Sanborn, Lending Club's chief operating officer, says loan volume roughly doubled every year since inception. "We believe now we're one of the top five issuers of personal loans in the U.S."

With the economy recovering, the websites are attracting consumers with improving credit scores who want to swap their credit card debt for a loan. Applicants with high enough FICO scores can apply for a maximum of $35,000. Loan sizes average $13,625 through Lending Club and $6,830 through Prosper.

Peter Renton, whose LendAcademy.com blog tracks the P2P industry, says small-business owners also are increasingly turning to social- and direct-lending sites as a way to obtain credit that isn't available from banks, or as a less-onerous alternative to asset-backed or factor-type lending. He cites Funding Circle, QuarterSpot, and Fundation as examples.

"Some of these newer online lenders are providing lower interest rates than most cash-advance people, and providing same speed, and that's what I consider very interesting," says Renton. "If you can pay 18% APR on a loan, and have it in two days, that's a very attractive proposition for a lot of small-business owners."

But what's truly driving the market lately is a surge in interest from institutional investors like hedge funds, insurance companies and private equity looking to buy up loans.

According to Sanborn, more of these investors have been coming to Lending Club to shop for loans to add to portfolios, in search of high yields, short duration and tolerable risk.

"Over the last two to three years, we've seen a broad diversification on who's investing," Sanborn says. Instead of smaller investors placing opening lender accounts of $10,000 to $20,000, "we've moved into higher net worth individuals, and increased dealings with those individuals through registered investment advisors, family offices, and broker-dealers like Morgan Stanley."

Lending Club began adding community banks to the funding mix last summer as well. It has signed up seven so far, including Titan, and is recruiting more.

Based on the average one-month interest rate of 14.63% charged to Lending Club borrowers since 2007, minus fees and an annual default rate of 3%, Sanborn estimates investors are getting 6% to 10% returns on P2P loan portfolios.

A chief goal of the new management team at Prosper was to make the service more friendly to institutional investors. Aaron Vermut, Prosper's president, and his father, Stephan, the CEO, have experience in that market, as does Suber, from running their prime brokerage and hedge-fund advisor Merlin Securities. (All three moved to Wells Fargo after the San Francisco banking company bought Merlin from Sequoia Capital in 2012.)

What's attractive to institutional investors, says Vermut, is the opportunity "to get access to consumer credit directly" rather than through derivatives and securitization. He says P2P is "a totally unique asset class and value proposition" that allows them to create a customized portfolio comprised of pieces of loans or whole loans that fit their specific investment criteria.

Under its new management, Prosper adopted a bankruptcy-remote business model that shields the notes held by lenders from the company's business operations. This reassured investors that they were only exposed to the risk of the loans they held, and not any corporate misfortunes. (A similar structure already existed with Lending Club.)

Both Prosper and Lending Club make money from fees and interest. They charge a one-time fee to borrowers when the loan is originated, and a monthly fee to lenders for servicing. The fees equate to a small percentage of the loan amount. Lacking charters themselves, both companies originate their loans through WebBank, a $138 million-asset state-chartered industrial bank in Utah.

The online format means the operation costs are one-third that of a retail bank, according to Lending Club. "We don't have branch infrastructures and don't have capital reserve requirements," says Sanborn.

In its P2P arrangement with community banks, Lending Club originates the loans, which Titan (and the others) buy at face value. The banks receive the monthly loan payments and pay a monthly servicing fee, equal to a percentage of the underlying balance, back to Lending Club, which keeps the relationship with the borrower.

"Banks have been buying loans and participations forever," says Jonathan Morris, who oversees the P2P initiative at the $63 million-asset Titan and is president of its parent company, BMC Bancshares. "Nothing here is really that different."

Morris says new loans available to be purchased are posted four times a day. He says Titan electronically sifts through the loans, evaluates their credit quality based on its own criteria (it requires a FICO score of at least 700, for example), and chooses the ones it wants to take. He says Titan is still building up its portfolio of Lending Club loans, and would not disclose the size of it.

The bank typically buys credits rated "A" or "B" by Lending Club (the ratings go as low as "G"). The average interest rate is 7.82% for "A" loans and 11.74% for "B" loans, according to Lending Club's website, and the average return is 5.19% and 7.82%, respectively.

So far Morris is pleased with the performance of the loans, which typically have a duration of 36 months. "We're doing above average."

He says he started talking with Lending Club more than a year before the bank started buying the loans, partly because he likes to know about "what's emerging on the forefront of banking."

Working out the kinks in how a bank partnership might work also took a while. "We were really waiting for compliance and other components to be in place, where it made sense for a bank to play in this space," Morris says. "Once that all came together, we were pretty eager to get involved."

The biggest benefit for Titan is diversification. It concentrates on small-business lending, but is now able to put on its balance sheet unsecured consumer loans, which is a type of lending it could not afford to do on its own. "Lending Club has allowed our bank and other banks to play in a sector that wasn't efficient enough to be profitable—in many cases even if the loans performed," Morris says.

He dismisses the notion of Lending Club being a competitor, at least for community banks. "Lending Club is clearly meeting some kind of customer need that's not being filled," he says. "Who are they displacing? They're not displacing the small and medium banks. Let's face it: [those banks] haven't been making zero to $10,000 consumer loans with no collateral for a long time. It's not even an asset class that gets tracked anymore."

The biggest banks fill the need for such loans with credit cards, which Morris says is not a great product for consumers because of the high rates and fees, and not a viable product for small banks like his. "There's no way to compete in the credit card business against Wells Fargo and Citibank. How do we do that? We can't," he says. "Now that we have Lending Club as a data processor—which is how I look at them—all of a sudden we have that ability."

In an email to what it describes as a "small group" of employees who requested an ethics ruling on P2P, Wells Fargo reportedly deemed it a competitive activity.

"Going forward, please refrain from making any new P2P investments/loans," the message said, according to the Financial Times, which saw a copy and published a story about it in January. "If possible, exit existing investments as soon as practical (without forcing a loss) or when the loans are paid off."

Though the email mentions "loans" at least twice, a Wells Fargo spokeswoman says her understanding is that the guidance was meant to apply to investments in the stock of P2P companies. She says Wells Fargo's code of ethics prohibits employees from investing in businesses that compete with the bank.

She did not directly answer a question about whether that meant Wells Fargo employees are allowed to participate in P2P lending. She said employees would have to ask their compliance officer.

Ross, who operates the hedge fund, says banks are correct to view P2P lenders as competitors but short-sighted if they use that as a reason to steer clear.

"It's almost like we're literally watching the ostrich with its head in the sand," he says. "They should be figuring it out."

Morris was amused by Wells Fargo's email, and, like others, interprets it as a validation of sorts for P2P lending.

"Titan Bank is excited to be a competitive threat to Wells Fargo," Morris says. "If that's the perception of Wells Fargo—that this technology has been such an equalizer that even a Titan Bank is a competitive threat to them—I think it's a good thing for small banks and it's a good thing for the market."

The P2P pitch is attractive to consumers, says Ross, who also suggests that banks can pick up valuable lessons from it. "People seem to like the idea of being able to get out of debt in five years, and they're willing to pay an origination fee to do it," he says.

They are perhaps more willing now that the P2P industry has put some of its early reputational hits behind it.

A 2008 dispute with the Securities and Exchange Commission is often viewed as the dividing line between today's market and the original lending models envisioned by Prosper founder Chris Larsen (of E-Loan fame) and Lending Club founder Renaud Laplanche.

Both had been looking to erode dependence on traditional financial institutions in the personal loan space. But the SEC filed a cease-and-desist letter, arguing that they were selling unregistered securities in the form of loan promissory notes. Both firms settled and went through a formal registration process, complete with a dormant quiet period in which neither sold loans to the investing public. (Lending Club continued to issue loans to borrowers with its own funds.)

The prospect of waiting for registration approval prompted Zopa, a British player, to drop plans for a U.S. expansion. But by 2009, Prosper and Lending Club were back selling to investors in states where they were permitted to do so.

Regulation is still a threat now that the CFPB is in place, however. Questions emerged shortly after the passage of the Dodd-Frank Act as to what authority the bureau would have over P2P and direct online lenders, particularly those already under the auspices of SEC oversight.

In 2011, the U.S. Government Accountability Office released a much-anticipated study outlining the future roadmap of regulation for the P2P market. One path would continue with SEC oversight where federal-level securities regulation would govern lenders while states ensure compliance to borrowers' rights; another would involve the reclassification of P2P loan investments as consumer financial products that would place the industry under the CFPB's watch. The GAO did not recommend any particular option.

The surge in peer-to-peer lending volumes isn't the only evidence of the market taking off. So is the growing number of P2P startups.

Funding Circle, a U.K. P2P lender, has opened a U.S. arm based in San Francisco with a $35 million investment. Another fresh entry, FreedomPlus, a Freedom Financial Networks affiliate company that is headed by former Prosper and Lending Club executive Joseph Toms, plans to expand P2P to consumers with FICO scores below 660 (which is the cutoff for Prosper and Lending Club).

Given Prosper's poor experience with bad-credit borrowers, this would seem to be folly. But in working with debt-consolidation companies over the past five years, Freedom Financial has done well with a product targeting consumers who have average credit card balances of $16,300 and an average FICO of 576, according to Toms. "The default running rate was under 2%," Toms says. "There are a lot of people out there with large balances that have poor credit scores but have fundamentally put into place the necessary things that allow them to become better credit scores."

Then there are the P2P mainstays who are getting better at what they do and trying out new things, too.

Lending Club, for example, is testing a service with two community banks (Titan is one of them) in which they can offer a customized Lending Club application to bank customers who would otherwise get turned down for an unsecured personal loan. The bank gets a "little" referral fee, according to Titan's Morris, who says the larger appeal is in helping a customer. "I'd always rather have a solution for somebody than just a flat 'no.'"

Bonnie McGeer is managing editor of American Banker Magazine. Glen Fest is a senior editor at Leveraged Finance News.

SOURCEMEDIA

© 2015 SourceMedia. All rights reserved.

WEB SEMINAR
Managing AML/KYC Compliance Risk, Rather than Avoiding It
REGISTER TODAY
MAY 11, 2015
12PM ET / 9AM PT

AMERICAN BANKER

Smartphones Shaping What Consumers Expect from Banks

by Brian Browdie
JUN 19, 2013 12:08pm ET

People expect service, simplicity and the ability to share socially wherever they happen to live, especially if they wield a smartphone.

That's the conclusion of a survey published Wednesday by payments processor First Data, which found more than half of shoppers in 10 countries want to be able to move among their computers, phones and retail stores with ease.

The expectations extend to banking. 76% of U.S. consumers expect to be able to access their financial accounts in real time, compared with 71% of consumers worldwide. More than half of consumers globally bank online via a computer, while about 25% use their smartphones to view their accounts.

Consumers also want advertising and other messages from banks and other businesses to reflect their transaction histories and preferences. Overall, 58% of consumers expect their bank to do a better job of considering their individual circumstances, according to the survey, which found that consumers in the U.S., China and Mexico have the least tolerance for technology that's not intuitive and easy to use.

EXHIBIT
K-3

The most important predictor of consumers' expectations is whether they use a smartphone, First Data found. While mobile phone penetration neared 100% in the countries surveyed, smartphone use varies by location, with China (92%), Singapore (89%) and the Middle East (80%) showing the highest use of the devices.

"Much of this change in expectations is driven by the proliferation of smartphones, which have fundamentally altered how consumers around the world go about their daily lives," Larry Drury, First Data's chief marketing officer, said in a news release.

Consumers also are taking to Twitter, Facebook, Pinterest and other social media to tell others about their experiences — good, and especially bad - according to the survey, which found that half of consumers, on average, post reviews online.

People in China (83%), India (74%) and Germany (60%) tend to post reviews more frequently than their counterparts in the U.S. and the rest of Europe, according to the survey, which did not detail percentages of postings in America.

Nearly half of people surveyed say they prefer companies that use social media and technology smartly, the survey found.

The online survey of roughly 4,000 consumers who had a bank account or either a credit or debit card was conducted in the U.S., Brazil, China, Germany, India, Mexico, the Middle East, Poland, Singapore and the U.K.

SOURCEMEDIA™

© 2015 SourceMedia. All rights reserved.

WEB SEMINAR
Missed Opportunities in Global Remittances
APRIL 16, 2015
12:00 PM ET/9:00 AM PT
Duration: 1 Hour
REGISTER NOW

AMERICAN BANKER

What Do Bank Customers Want?

FEB 25, 2014 12:00am ET

At BankThink, blog posts on the bank model of the future might delve into predictions about the role of branches, the potential for partnerships with startups and the best use of big data. It all ties back to one central question: What does the customer want? On that, the pundits are divided.

So in a new series this year, we've asked consumers from different demographics to describe firsthand what they are looking for from the financial services firms they do business with. Our fundamental pitch was: "If you could design your perfect bank, what would it look like?" The responses are anecdotal, but taken together they could point to trends regarding what it is that drives consumers' banking choices, and what will determine their choices in the future.

Full versions of the edited excerpts published here, plus additional installments in the series, can be found online at americanbanker.com/bankthink/what-bank-customers-want. -Jeanine Skowronski

For much of my life I've been poor: as a child of undocumented immigrants, as a young adult in college, as I was starting out in the working world, and again years later, as a law student. Today, I make a good income, but I rarely have a lot of money for any amount of time. What I pay in student loans every month is what many families pay for rent in the San Francisco Bay area. I am what some banks might call a "high-transaction, low-balance" customer.

Fortunately, my work as a financial services advocate has given me insight on what to look for, including red flags. Any institution that hard-sells overdraft is not for me. With the number of transactions flying through my account, and the different kinds of transactions, including checks,

EXHIBIT
K-4

debit card purchases, electronic funds transfers and recurring automatic bill payments, I could (and several years ago, did) easily rack up a scary amount of fees.

Even accounts with lower overdraft fees, such as those offered by credit unions or those that withdraw money from a savings account rather than leaving a balance owed to the bank, would not work for me if the transactions are re-ordered to maximize the number of overdrafts or simply processed in an order that I can't predict.

I operate with an abundance of caution and have three accounts now. One is a credit union account with low insufficient-funds fees (just in case) from which all my bills are paid. Another is a "big bank" account that I get for free because I bank electronically. (This account does not allow overdrafts for debit card transactions.) I also have an Internet-based account that pays interest and covers out-of-network ATM fees.

Having embraced the digital lifestyle, banks haven't received much face-time from me. From credit card bills to the monthly paycheck, most of my money flows in an automated system that requires almost no effort on my part. And it's been great. The less I have to deal with the physical aspects of banking, the more I've come to appreciate my banks, JPMorgan Chase and Ally Financial.

But no matter how streamlined my finances are, there is one thing that has proven to be a regular nuisance. It's the need for a no-cost method of sending money to and from family and friends, without the friction that comes from having to provide hard-to-remember information like account numbers and routing numbers.

In two recent situations, I struggled to come up with ways to make and receive personal payments. A friend who uses Citibank could have used Citi's person-to-person payments feature (through Popmoney) to send me money, but I didn't want to deal with signing up for a Popmoney account. And when I wanted to send money to a family member who uses Bank of America, the relative didn't want to deal with entering hard-to-find information to collect money through Chase QuickPay, which I would have used to make the transfer.

Bank of America and Chase are both founding members of clearXchange. This peer-to-peer, or P2P, payment network allows customers of member banks to send money to each other with just an email address or phone number. According to the FAQs, there is no fee to send or receive money, which is all any consumer can ask for. But Chase is not yet capable of providing P2P payments through the clearXchange network.

The argument for third-party services may be brought into the discussion, but the likes of Google Wallet, Square Cash and PayPal can never earn the amount of consumer trust that exists when someone knows their money is moving between two financial institutions, as opposed to through a middleman.

-Simon Zhen is a writer and research analyst for MyBankTracker.com, a website that features consumer bank reviews, personal finance articles and bank product comparisons.

These institutions want me. They give me good service (most of the time), help me avoid fees and help me save more money that much faster. Between them, I have records that I am in fact a good bet for anyone considering lending money to me. When I am ready to commit to financing a home, a car or my kid's education, I will offer my business first to those institutions that helped get me there.

-Andrea Luquetta is a policy advocate at the California Reinvestment Coalition, a nonprofit promoting access to financial services for low-income communities and people of color.

I want to be able to trust my bank. More than anything I would like good customer service, close attention to my account security and really low fees.

Unfortunately, I almost never get what I want from my bank. For instance, a couple months ago, I received an email ostensibly notifying me about account changes. Only the message didn't contain any details. I sent an email to the bank asking for specifics about what was changing and when these changes would go into effect. The response, again, was unclear, so I called the bank for more information.

A month later, a charge for that call appeared on my checking account statement. When I protested the charge, the bank removed it from my account. But I'm still frustrated. Why is it hard to get the right information from your bank? The bad experience stuck in my head.

-Dominique Hall is a student in Oakland, Calif., and a participant in Game Theory Academy, an organization focused on improving the economic decision-making skills of young adults.

American Banker

BankThink Series: What Bank Customers Want

When: Ongoing since Jan. 13

Where: Online, at americanbanker.com/bankthink/what-bank-customers-want

Key themes:

* Ideal practices and services from banks

* Factors driving choices about how and where to bank

SOURCEMEDIA™

© 2015 SourceMedia. All rights reserved.

WEB SEMINAR
Distress Loan Sales:
An Update on FHFA's New NPL Sales Requirements
REGISTER NOW

AMERICAN BANKER

Why Banks Will Win the Payments War

Glen Fossella
JUL 29, 2014 12:00pm ET

WEB SEMINAR
Distress Loan Sales:
An Update on FHFA's New NPL Sales Requirements
REGISTER NOW

Those of us in the financial services industry are inundated with news of emerging services from upstart payments competitors: mobile wallets, bill payment and peer-to-peer payment solutions, micro-lending and personal finance tools. The general consensus is that banks are laggards held back by legacy thinking and heavy fixed costs for compliance and branches. They are constantly admonished to catch up with these new competitors or face disruption and disintermediation.

It's true that banks often move slower than startups, both in innovating and in deploying alternative solutions. But are banks really at risk of losing dominance in the payments space? The answer is a resounding no, based on several built-in advantages.

The compliance burden acts as a large and growing barrier to entry for non-traditional competitors. No one gets a seat at the table unless they can get past the regulators. Just ask Square, which coughed up $507,000 a year ago to pay a fine levied by the Florida Office of Financial Regulation for operating without a license.

Marc Andreseen and other Silicon Valley venture capitalists have been musing publicly recently about "getting around" stodgy banks and speeding innovation by building a pure software bank. However, it is faster and cheaper for startups to partner with institutions, as Dwolla has with Veridian Credit Union, or to just buy one, as Independence Bancshares chief Gordon Baird did for his payment services platform.

Moreover, branches give banks a major advantage for enrolling customers in new payment products and supporting them. We are still in the first inning of mobile banking and emerging payments. Count on these solutions to get very sophisticated over time, with banks offering the equivalent of

EXHIBIT
K-5

Apple's Genius Bar to make sure customers are getting full value from these services. Barclays has already deployed 7,000 branch employees in the United Kingdom as "digital eagles" to help customers learn to use online and mobile banking tools. Here in the U.S., UMB offers a similar service.

Banks can generate both goodwill and revenue by using branches to help customers solve problems and learn to use new features.

Emerging payment players' biggest challenge is acquiring and nurturing active customers. Banks have no such challenge. They already have access to a large user base familiar and comfortable with their brand. This also gives banks cost advantages and pricing flexibility, since new service offerings are incremental.

Consider high-profile debit card provider Moven. Despite an interesting feature set and business model, their active user base only grew from 5,000 in March 2013 to 10,000 today.

They will need to spend millions just to acquire enough customers to break even. Some argue that Apple and Amazon, with 800 million and 250 million user accounts respectively, are positioned to impact payments. This may be true, but each of those accounts is tied a credit card issued by a financial institution. This gives banks a broader view of customers' buying and banking activity, up- and cross-sell opportunities, a stronger hand in loyalty programming, and ultimately greater relationship control.

Banks have a similar advantage when it comes to acquiring customers through merchants. Banks with merchant businesses have ready-made channels for promoting and on-boarding current and new consumers with any new payment offering. For example, later this year, Wells Fargo will roll out beacon technology services to merchants. While the move is intended as a promotional tool for its merchant customers, Wells could potentially work with businesses to cross-promote the bank's products and services, including alternative payments.

Banks are also better positioned to form consortia and industry groups to set standards and implement common infrastructure, as they have done for decades. Whether it is ACH, Check 21, or other initiatives, what seems glacial in speed is more often a methodical movement toward interoperability. For example, the ClearXchange person-to-person network, with Bank of America, Capital One, Chase, and Wells Fargo as member banks, is now available to more than half of all mobile banking customers in the United States. While it is still too early to assess its long-term potential, ClearXchange is an example of how banks can quickly gain critical mass to bring solutions to the mass market.

But these built-in industry advantages do not translate into individual banks' success in emerging payments. Institutions should press their advantage by acquiring outside innovation in the payments space.

The most expensive and complex approach to acquiring additional innovation is direct investment in startups. For example, Citigroup operates a dedicated venture group and has invested alongside Andreessen's firm, Andreessen Horowitz, several times. Citi also operates a venture capital accelerator in Israel. BBVA and Fifth Third also operate formal venture arms. Venture investing can deliver big returns, but it is an expensive way to stay atop innovation.

Another approach now common in the startup world is the acqui-hire, that is, acquiring a company as much for its talent as its product. This was likely the reasoning behind BBVA's recent purchase of online bank Simple and Chase's purchase of Groupon-clone Bloomspot in December 2012. Banks acquiring startup solutions are in a position to drive product development more quickly and in-line with their strategy.

A more straightforward approach is to hire talent away from other innovators. Capital One recently poached Dan Makoski from Google's Advanced Technology and Projects team, while Chase has acquired talent from the likes of Yahoo, Google, and even Huffington Post. This is an approach that even smaller institutions can take to stay ahead in payments, ecommerce, and other areas of innovation.

While the industry's inborn advantages all but guarantee banks will win the payments war, individual institutions will need to win their own battles. Acquiring innovative companies and employees from the outside can help any bank stake out a competitive advantage that protects the business and contributes to long-term growth.

Glen Fossella is a technology industry executive with a background in payments and branch automation.

SOURCEMEDIA™

© 2015 SourceMedia. All rights reserved.

Consumers and Mobile Financial Services March 2012

Print

Preface
Executive Summary
Introduction
How Are Consumers Interacting with Financial Institutions?
Current Use of Mobile Banking and Payments
Other Mobile Financial Services
Appendix 1: Survey of Consumers' Financial Decisionmaking Using New Technologies--Questionnaire
Appendix 2: Consumer Responses to Survey Questionnaire

Current Use of Mobile Banking and Payments

In this Section:

Mobile Banking
Mobile Payments
Mobile Security

Mobile Banking

The Federal Reserve survey defines mobile banking as "using a mobile phone to access your bank account, credit card account, or other financial account. Mobile banking can be done either by accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone."

A significant number of mobile phone users have already adopted mobile banking. Nearly 21 percent of mobile phone users in the survey report that they used mobile banking in the past 12 months.[8] Moreover, among those consumers who do not currently use mobile banking, 11 percent report that they will "definitely" or "probably" use mobile banking in the next 12 months. An additional 17 percent of those who report that they are unlikely to use mobile banking in the next 12 months report that they will "definitely" or "probably" adopt mobile banking at some point. Adding all these respondents together would imply peak adoption of 42 percent of all mobile phone owners.[9] As smartphone users are more likely to adopt mobile banking than non-smartphone users, increasing smartphone adoption should further fuel mobile banking adoption.

Use of mobile banking appears to be highly correlated with age (table 2), as individuals between ages 18 and 29 account for approximately 44 percent of mobile banking users, relative to 22 percent of mobile phone users. Conversely, individuals age 60 and over account for only 6 percent of all mobile banking users, while at the same time they represent 24 percent of all mobile phone users.

Table 2. Use of mobile banking in the past 12 months by age
Percent, except as noted

Age categories	Yes	No	Total
18-29	43.5	16.8	22.4
30-44	35.7	24.7	27
45-59	14.7	30.2	26.9
60+	6.1	28.4	23.7
Number of respondents	**372**	**1,626**	**1,998**

Note: This is table B.89 in Appendix 2.

Non-Hispanic black and Hispanic users show a disproportionately high rate of adoption of mobile banking (table 3), at 16 percent and 17 percent of all mobile banking users relative to 11 percent and 13 percent of mobile phone users, respectively. Meanwhile, mobile banking users are split evenly between males and females, and use of mobile banking is generally unrelated to household income (table 4), with the share of mobile banking users by income category corresponding to their share of the mobile phone user population. As with online banking, exceptions occurred at the tails of the income distribution, with those individuals earning less than $25,000 per year being significantly less likely to use mobile banking than their share of the mobile phone user population would suggest, while those individuals earning more than $100,000 per year being significantly more likely to use mobile banking than their share of the mobile phone user population would suggest. Mobile banking is highly correlated with education (table 5): 73 percent of all mobile banking users have at least some college education, but this education group represents only 60 percent of all mobile phone users.

Table 3. Use of mobile banking in the past 12 months by race
Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	60.3	71.5	69.2
Black, Non-Hispanic	16.2	10	11.3

EXHIBIT K-6

Race/ethnicity	Yes	No	Total
Other, Non-Hispanic	5.2	5.8	5.6
Hispanic	17.1	11.6	12.8
2+ Races, Non-Hispanic	1.2	1.1	1.2
Number of respondents	**372**	**1,626**	**1,998**

Note: This is table B.92 in Appendix 2.

Table 4. Use of mobile banking in the past 12 months by income group
Percent, except as noted

Income group	Yes	No	Total
Less than $25,000	12.8	19.9	18.4
$25,000-$39,999	19	16.6	17.1
$40,000-$74,999	27.5	26.5	26.7
$75,000-$99,999	12.9	14	13.8
$100,000 or greater	27.9	22.9	24
Number of respondents	**372**	**1,626**	**1,998**

Note: Table B.101 in Appendix 2.

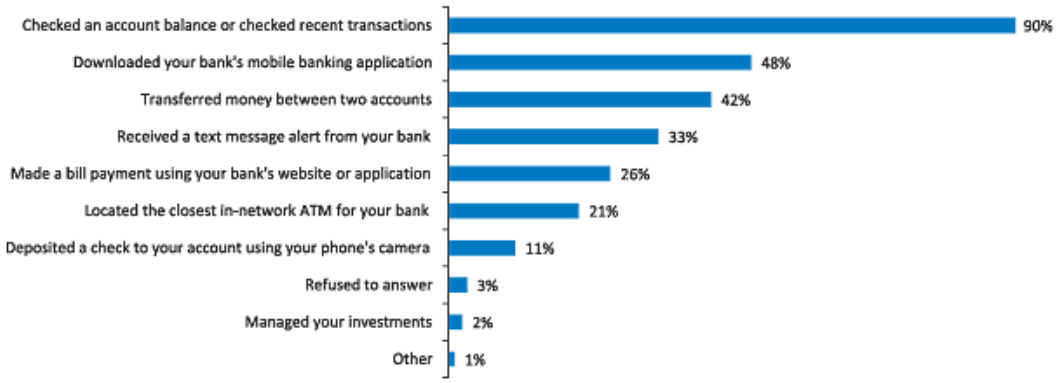
Table 5. Use of mobile banking in the past 12 months by education group
Percent, except as noted

Education (categorical)	Yes	No	Total
Less than high school	5.5	12.1	10.7
High school	21.5	31.8	29.6
Some college	39	27.4	29.8
Bachelor's degree or higher	34	28.8	29.9
Number of respondents	**372**	**1,626**	**1,998**

Note: Table B.98 in Appendix 2.

By far, checking financial account balances or transaction inquiries were the most common mobile banking activity, with 90 percent of mobile banking users having performed this function in the past 12 months (figure 2). Less prevalent activities were transferring money between accounts (42 percent) or receiving a text message alert from a bank (33 percent). Less frequently used mobile banking functions include making online bill payments from a bank account (26 percent), locating an in-network ATM (21 percent), and depositing a check by phone (11 percent). Lastly, mobile investment management is utilized by only 2 percent of mobile banking users. Many mobile banking users appear to be making use of their banks' mobile applications, as 48 percent have installed such an application on their phones.

Figure 2. Using your mobile phone, have you done any of the following in the past 12 months?



Accessible Version | Return to text

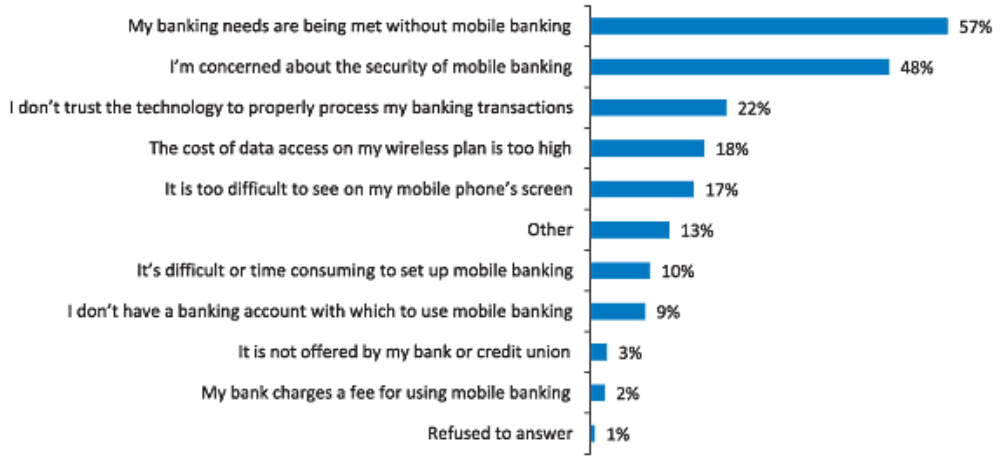
Note: This was question 25 in the survey (see Appendix 1); number of respondents was 372.

Consumers report using mobile banking up to 60 times per month; however, the median number of mobile banking transactions is four or five times in a typical month.

Of the consumers who use mobile banking, many appear to be quite satisfied with their experiences, as 62 percent report being "very satisfied" with their experiences, and another 32 percent report being "somewhat satisfied" with their experiences.

Among those consumers with mobile phones who do not currently use mobile banking, the top two reasons for not using the service are that they believe their banking needs are met without mobile banking (58 percent) and that they are concerned about security (48 percent) (figure 3). Less commonly cited reasons include a lack of trust in the technology to process transactions properly (22 percent), the high cost of data access on mobile phones (18 percent), and the small size of the mobile phone screen (17 percent).

Figure 3. What are the main reasons you have decided not to use mobile banking?



Accessible Version | Return to text

Note: This was question 36 in the survey (see Appendix 1); number of respondents was 1,626.

Consumers who express concerns about the security of mobile banking are concerned with hackers gaining access to their phone remotely (54 percent), losing their phone or having it stolen (19 percent), and experiencing data interception by a third party (18 percent). If these concerns were addressed, many non-users would be willing to adopt mobile banking.

Moreover, the potential uses of mobile banking by those who have yet to adopt it largely mirror those of current users. The majority is interested in checking financial account balances or recent transactions (55 percent), while fewer are interested in receiving text message alerts from their bank (30 percent), transferring money between accounts (25 percent), or making bill payments (24 percent).

Back to section top

Mobile Payments

The Federal Reserve survey defined mobile payments as "purchases, bill payments, charitable donations, payments to another person, or any other payments made using a mobile phone. Mobile payments can be used by accessing a web page through the web browser on your mobile device, by sending a text message (SMS), or by using a downloadable application on your mobile device. The amount of the payment may be applied to your phone bill (for example, Red Cross text message donation), charged to your credit card, or withdrawn directly from your bank account."

Consumers were less likely to adopt mobile payments than mobile banking, with only 12 percent of mobile phone users reporting that they made a mobile payment in the past 12 months. Mobile payment users also perform a narrower set of transactions than mobile banking users, with the most common activity being payment of bills (47 percent), followed by making online purchases (36 percent) and

transferring money directly to another person (21 percent). All other transactions (e.g., receiving a payment, texting to make a charitable donation) are used by less than 10 percent of those making mobile payments.

Mobile payments are disproportionately used by younger consumers (table 6). Individuals age 18 to 29 account for 37 percent of mobile payment users relative to 22 percent of all mobile phone users, while individuals age 30 to 44 account for a further 36 percent of mobile payment users relative to 27 percent of all mobile phone users. Hispanic consumers are active users of mobile payments, accounting for approximately 21 percent of all mobile payment users relative to 13 percent of all mobile phone users (table 7). In contrast, non-Hispanic whites are proportionally less likely to use mobile payments, as they make up 58 percent of mobile payment users but are 69 percent of mobile phone users. Almost 13 percent of non-Hispanic blacks use mobile payments, which is comparable to their 11 percent share of the mobile phone user population. Females are slightly more likely to use mobile payments than males, accounting for 55 percent of all users (table 8). Income does not play a role in mobile payment use, as each income group represents roughly the same percentage as it does in the overall mobile phone user sample (table 9). Similarly, mobile payment use by education level is roughly proportionate to its representation in the mobile phone user population (table 10).

Table 6. Use of mobile payments in the past 12 months by age
Percent, except as noted

Age categories	Yes	No	Total
18-29	37.3	20.3	22.4
30-44	35.9	25.6	26.9
45-59	16.9	28.5	27
60+	10	25.7	23.7
Number of respondents	**213**	**1,780**	**1,993**

Note: This is table B.90 in Appendix 2.

Table 7. Use of mobile payments in the past 12 months by race
Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	58.3	70.8	69.3
Black, Non-Hispanic	12.9	10.9	11.2
Other, Non-Hispanic	7.1	5.4	5.6
Hispanic	20.9	11.6	12.8
2+ Races, Non-Hispanic	0.9	1.2	1.2
Number of respondents	**213**	**1,780**	**1,993**

Note: This is table B.93 in Appendix 2.

Table 8. Use of mobile payments in the past 12 months by gender
Percent, except as noted

Sex	Yes	No	Total
Female	55	52.7	53
Male	45	47.3	47
Number of respondents	**213**	**1,780**	**1,993**

Note: This is table B.96 in Appendix 2.

Table 9. Use of mobile payments in the past 12 months by income group
Percent, except as noted

Income group	Yes	No	Total
Less than $25,000	19.1	18.5	18.5
$25,000-$39,999	20.6	16.7	17.2
$40,000-$74,999	23	27.2	26.7
$75,000-$99,999	11.7	14	13.7
$100,000 or greater	25.6	23.6	23.9
Number of respondents	**213**	**1,780**	**1,993**

Note: This is table B.102 in Appendix 2.

Table 10. Use of mobile payments in the past 12 months by education group
Percent, except as noted

Education (categorical)	Yes	No	Total
Less than high school	7.2	11.2	10.7
High school	27.9	29.9	29.7
Some college	37	28.7	29.7
Bachelor's degree or higher	27.9	30.1	29.9
Number of respondents	**213**	**1,780**	**1,993**

Note: This is table B.99 in Appendix 2.

Consumers use a variety of methods to make mobile payments, but the most common method is to input a credit card, debit card, or prepaid card number into a mobile phone (66 percent). Other mobile payment techniques used by consumers include making payments directly from a bank account (45 percent); using Google Wallet, Paypal, or iTunes (22 percent); or adding a payment to a mobile phone bill (8 percent).

Consumers use mobile payment services less frequently than they do mobile banking services. The median number of mobile payments in a typical month is one. Although some respondents reported making as many as 24 mobile payments per month, fewer than 7 percent of respondents make more than five payments in a typical month.

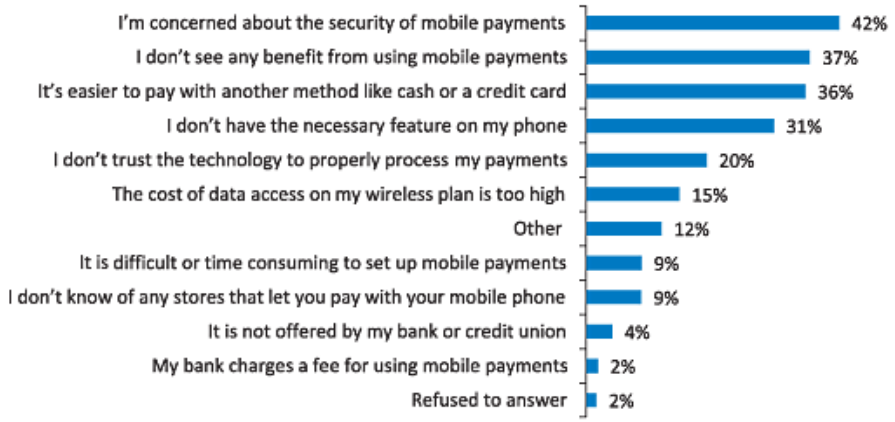
As with mobile banking, users of mobile payments appear to be quite satisfied with their experiences: 55 percent report being "very satisfied" with their experiences and 33 percent report being "somewhat satisfied" with their experiences.

Although security is the dominant reason why individuals do not use mobile payments (42 percent), there are many consumers who do not see any value in mobile payments; 36 percent report that it is easier to pay with other methods, and 37 percent report that they do not see any benefit from using mobile payments (figure 4). Other reasons for not using include the lack of necessary features on a phone (31 percent) and a lack of trust in the technology to properly process payments (20 percent).

If the concerns of non-users of mobile payments were addressed, those consumers express that they would have an interest in using mobile payments for a variety of activities. In particular, 34 percent report that they would pay bills online using their phone, 28 percent would receive coupons on their phone, and 22 percent say they would receive location-based offers or buy goods and services online. Making person-to-person payments is listed by 17 percent of respondents as a preferred mobile payment activity; the same percentage expresses a similar sentiment for using a mobile phone as the payment mechanism at a cash register or to use a phone as a "virtual wallet." Consumers also express some interest in using mobile payments to transfer money to friends or relatives in other countries (7 percent).

Figure 4. What are the main reasons why you have not used mobile payments?

Back to



Accessible Version | Return to text

Note: This was question 39 in the survey (see Appendix 1); number of respondents was 1,780.

section top

Mobile Security

Two major impediments to consumers' adoption of mobile banking and mobile payment technologies are (1) concerns about security and (2) the possibility of hackers remotely accessing consumers' phones. Consumers' beliefs about whether mobile banking or mobile payment technologies are secure is correlated with their use of these technologies. Consumers who use mobile banking or mobile payments are more likely to report that it is a secure process than those who do not use mobile banking or mobile payments. For example, when consumers were asked to rate the security of text messages for mobile banking, those who are mobile banking users rate the service "very safe" (18 percent) or "somewhat safe" (42 percent). In contrast, 38 percent of non-users of mobile banking report that they "don't know" whether or not text messages for mobile banking are safe, while only 6 percent rate the service "very safe" and 27 percent rate it "somewhat safe."

The dichotomy between users and non-users of mobile banking is even more pronounced when asked about the overall security of mobile banking for protecting personal information. Two-fifths of non-users report that they do not know if it is secure, while 13 percent of this group rate mobile banking "very unsecure" and 23 percent rate the service "somewhat unsecure." Mobile banking users, however, rate mobile banking as "very safe" (18 percent) or "somewhat safe" (56 percent) in maintaining their personal information.

References

8. There is a wide range of estimates of mobile banking adoption. comScore estimates that 13.9 percent of all mobile phone users had adopted mobile banking as of Q2 2011. Javelin estimated that 19 percent of mobile phone users had adopted mobile banking as of March 2011 (Smartphone Banking Security Report); however, the firm subsequently reports that mobile banking adoption jumped to 30 percent as of June 2011 (comScore, 2011, Mobile Banking Financial Institution Scorecard). Return to text

9. The denominator for each of the questions on mobile banking adoption varies, thus the potential adoption rate is less than the sum of the percentages of respondents who indicate that they have or will adopt mobile banking. There are a total of 2,002 mobile phone users in our survey: 418 are current users of mobile banking, 182 report that they are likely to use mobile banking in the next 12 months, and 246 report that they will likely use mobile banking at some point in the future (for a total of 846 potential users, or 42 percent of all 2,002 mobile phone users). Return to text

FEDERAL RESERVE
BANK OF BOSTON™

Meeting the Needs of Non-Traditional Consumers and Achieving Scale with Mobile Contactless Payments in the U.S.

Summary Report of November 13-14, 2013, Mobile Payments Industry Workgroup Meeting

by Susan Pandy, Director, Payment Strategies, Federal Reserve Bank of Boston and
Elisa Tavilla, Industry Specialist, Payment Strategies, Federal Reserve Bank of Boston

January 2014

In November 2013, the **Mobile Payments Industry Workgroup** (MPIW) met with academia, government, non-profits, card networks, mobile wallet providers, transit authorities, issuing banks, and retailers to gain a better understanding of fundamental consumer mobile payment adoption issues by exploring how mobile financial services and payments can meet the needs of nontraditional consumers and what is needed to achieve scale in the U.S. mobile payments market. The findings in this paper are based on the discussions at this meeting and include the panelists' views on mobile technology and financial access considerations for the underserved consumer, broader consumer market adoption for mobile retail payments, and the transformational role of mobile technology for financial services.

Full paper

EXHIBIT
K-7

Meeting the Needs of Non-Traditional Consumers and Achieving Scale with Mobile Contactless Payments in the U.S.

Summary Report of November 13-14, 2013 Mobile Payments Industry Workgroup Meeting

Susan Pandy
Director, Payment Strategies
Federal Reserve Bank of Boston

Elisa Tavilla
Industry Specialist, Payment Strategies
Federal Reserve Bank of Boston

January 30, 2014

Susan Pandy is a Director and Elisa Tavilla is a payments industry specialist in the Payment Strategies Group at the Federal Reserve Bank of Boston.

The authors would like to thank members of the MPIW and panelists for their thoughtful comments and review of the report.

The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Bank of Atlanta, the Federal Reserve Bank of Boston, or the Federal Reserve System.

Mention or display of a trademark, proprietary product or firm in this report does not constitute an endorsement or criticism by the Federal Reserve Bank of Atlanta, the Federal Reserve Bank of Boston, or the Federal Reserve System and does not imply approval to the exclusion of other suitable products or firms.

EXHIBIT
K-8

Introduction

In November 2013, the Federal Reserve Banks of Boston and Atlanta convened a meeting in Boston with the Mobile Payments Industry Workgroup (MPIW) and invited guests[1] to discuss the challenges underlying broad mobile payment adoption in the United States. The primary objective of the meeting was to gain a better understanding of fundamental consumer adoption issues by (a) exploring how mobile financial services and payments can meet the needs of nontraditional consumers, (b) and what is needed to achieve scale in the mobile payments market. Remarks focused particularly on how prepaid mobile products can address the needs of nontraditional consumers such as the underbanked and unbanked[2] (hereinafter referred to as "the underserved") and younger consumers (also known as Generation Y or millennials, born between the early 1980s to the early 2000s). Panelists also explored their different perspectives on how to achieve meaningful scale.

This report will summarize the discussions on (a) mobile technology and financial access considerations for the underserved consumer; (b) broader consumer market adoption for mobile retail payments; and (c) the transformational role of mobile technology for financial services.

I. Mobile Technology and Financial Access Considerations for the Underserved Consumer

Many underserved consumers experience pain points when transacting financial business (e.g., sending money, paying bills, accepting payments, and depositing/cashing checks). These might be addressed through the use of mobile technology solutions, namely mobile financial services and mobile wallets available through mobile phones and associated apps. Panelists characterized the underserved as the new middle class[3] rather than as low income consumers or those consumers likely to spend all or most of their income each month. Mobile phones present a great opportunity to provide the underserved with enhanced convenience and access to applications and tools to better manage their financial lives, encourage savings, and make real-time money decisions.

---

[1] Panelists represented academia, government, non-profits, card networks, mobile wallet providers, transit authorities, issuing banks, and retailers. For more information about the meeting panelists, see Appendix I.

[2] According to 2012 FDIC study, *2011 FDIC National Survey of Unbanked and Underbanked Households*, 8.2 percent or about 10 million U.S. households are "unbanked," meaning they do not have accounts with financial institutions. Another 20.1 percent have an account but are "underbanked," these are consumers who choose to use alternative financial services (e.g., money orders, check cashing services, payday loans, prepaid cards, and other financial services offered through outlets other than a traditional bank or credit union) at least once per year. Retrieved from http://www.fdic.gov/householdsurvey/2012_unbankedreport.pdf.

[3] Panelists characterized the underserved as the new middle class because they tend to rely on alternative financial services either because they no longer wish to have an account with a financial institution or other reasons such as budget and credit challenges. The U.S. Census Bureau does not have an official definition of the "middle class," and the term often means different things to different people. The Census splits the U.S. household population into five different groups based on income, each comprising 20 percent of the population. If the middle 20 percent is truly the "middle class," then middle class households make between $38,500 and $62,400 per year. However, in the 2012 U.S. Presidential election, the candidates defined the middle class as those making less than $250,000 per year. This number is different from the median – or middle – household income in America, reported by the Census to be about $50,000 in 2011. The top 5 percent of American households had incomes of $186,000 or more, meaning that many of them would still qualify as "middle class" under the candidates' definitions.

Dan Schulman, from American Express, explained how the less money that someone has, the more it costs that person to manage and move his money (e.g., time spent driving to a bank or business to pay bills or cash checks, paying check cashing fees, waiting in line, purchasing a money order, paying late fees for bills, etc.). In other words, "it's expensive to be poor." To the underserved, time spent managing one's money can be equivalent to a part-time job; therefore, time truly equates to money. By leveraging mobile technology, consumers can open and improve their regular access to financial accounts, freeing up valuable time and, hopefully, reducing fees.

Lew Goodwin, from Green Dot Bank, explained how his business is designed for the underserved consumer segment, including the digital natives–consumers who have grown up with mobile phones. Green Dot Bank offers both a prepaid card product as well as a mobile bank with a fully functioning Demand Deposit Account (DDA) (minus the paper checks) called GoBank.[4] GoBank offers several attractive features to customers such as allowing them to set their own monthly account fees based on what they believe to be the value of the account and not allowing overdrafts, thus avoiding overdraft fees. To minimize the possibility of a customer overdrawing his account, GoBank only supports online[5] transactions and requires a customer to replenish his GoBank account before using it. GoBank recognizes that the underserved consumer tends to live paycheck to paycheck and offers these features to help him better manage his funds and encourage savings.

Prepaid and the Underserved

The role of prepaid products in meeting the financial needs of the underserved was a prominent component of the morning panel discussion. One barrier raised was that prepaid cards/accounts are associated with disposability or the tendency for consumers to use a prepaid product one time or for one specific purpose and then discard it. Developing prepaid products for a mobile phone may enhance the value proposition and counteract the connection to disposability. While some prepaid products may offer the equivalent of a bank account with the broad range of functionalities, better consumer education is needed to show consumers the value beyond the one-time purpose.

---

[4] GoBank is a brand of Green Dot Bank, Member FDIC, which also operates under the brands Green Dot Bank and Bonneville Bank. Deposits under any of these trade names are deposits with a single FDIC-insured bank, Green Dot Bank, and are aggregated for deposit insurance coverage. For more information, see https://www.gobank.com/.

[5] While consumers may physically load money to their GoBank accounts at participating local retailers, GoBank is designed to support fully electronic/online payments. For example, a consumer who needs to pay a business that does not accept e-payments or that needs to give someone a check, can send those payments through GoBank by entering the necessary information and then GoBank sends a check free of charge.

The panel agreed that generally the value of using prepaid products for financial services is not well understood in the U.S. because they are complicated and have a reputation for charging high fees and offering few consumer protections.

II. Consumer Adoption Considerations for Mobile Retail Payments

The morning panel also discussed consumer adoption issues for mobile payments. According to Ed Ponte of Monitise, "Adoption can be understood based on *consumer awareness* and how that interest is translated into enrollment" for new mobile products and services. The business strategy for consumer adoption starts with a framework for *enrollment* and consumer *engagement*, followed by continual *adjustment* of the product. The product must be appealing to generate consumer awareness. It needs to have compelling features that drive both inbound and outbound consumer engagement (i.e., apps that create consumer interest and build sustainability), but consumers and merchants need to be comfortable with it. Once the product is available, it needs to be continually adjusted–features and functionality needs to be reassessed, particularly given the level and speed of innovation in the market. Adjustments are necessary to maintain competitive advantage and identify the compelling features/functionality that support continued investment. From a behavioral economics perspective, consumer marketing and decision-making related to mobile financial services are also critical considerations for generating and sustaining consumer awareness and adoption of mobile payments. Marketing strategies need to consider the specific needs and financial pain points of the consumer segments being targeted because low income and more affluent consumers have distinct financial needs, which result in very different financial decisions and spending behaviors.

Consumer Awareness and Adjustment

Lew Goodwin explained Green Dot's approach to building consumer awareness for its prepaid product. Because Green Dot did not start out as a bank, the company formed extensive partnerships with the retail community to have its prepaid cards displayed on J-hooks[6] in over 80,000 retail locations. Consumers could then load and reload the cards at the retail point of sale–the first touch-point with the consumer and a critical component to driving consumer awareness. Word of mouth has also factored strongly into building consumer awareness for its prepaid product.

[6] According to Management Ventures, Inc., *Retail Standards & Terms*, a J-hook is so-called because of its J shape. Usually it is placed on a shelf used for merchandising impulse products. Retrieved from www.kantarretailiq.com.

Once a customer activates their prepaid card online, Green Dot performs the Know Your Customer[7] verification which helps the company to understand how the consumer prefers to be contacted. The prepaid card is useable only upon a consumer passing the verification process and it then becomes a fully functional card.[8] Green Dot's prepaid also has a mobile account management component (e.g., balance alerts, transaction history, etc.). Customers can begin using the mobile and online features immediately upon registering their card. Green Dot sees this as an alternative option to having a consumer wait for a debit card to arrive in the mail from a branch bank and to begin using their card immediately and preferably from their phone.

Green Dot continually reevaluates the best ways to reach the customer and make the product features and fees fully transparent and easy to use, while GoBank continues to explore the most effective ways, to reach its target customer base (i.e., digital natives), including social media channels.

Jennifer Tescher, from the Center for Financial Services Innovation (CFSI), explained how TIO Networks[9] builds consumer awareness in the bill payment space. TIO works with a community of billers to spread the word about its kiosk-based network of bill payment machines for consumers who use cash to pay their bills. TIO recently transitioned to mobile bill pay and leveraged the biller community to generate awareness.

Dan Schulman, from American Express, emphasized the importance of packaging for consumer awareness, noting that if the product looks like a gift card, then it looks disposable. For Bluebird,® an alternative to checking and debit accounts, American Express created a box that resembles software packaging in order to position the product as an application rather than a plastic card.

Consumer Marketing and Decision-making

The panel moved on to discuss how mobile products are marketed to consumers and how the above factors may influence consumer decision-making.

Michael Norton, professor of business administration at Harvard University, noted that most consumer marketing efforts, particularly for financial services and/or products, differ between low income and more

---

[7] **Know Your Customer** (**KYC**) refers to due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. KYC rules are derived from the USA PATRIOT Act Customer Identification Program for financial institutions, which sets out rules and regulations requiring financial institutions to thoroughly and properly identify, verify, and authenticate new customers opening accounts, in order to better keep tabs on the money flowing in and out of America's banks and financial institutions.

[8] If the consumer does not pass the verification process or supply their Social Security Number, then the card becomes a spend down card with no reload ability or cash access.

[9] For more information, see http://www.tionetworks.com/.

affluent consumers. Marketing to low income consumers is often aimed at helping them avoid or manage bad events (e.g., debt, foreclosure, debt collection activities, and bankruptcy). Advertisements to more affluent consumers tend to encourage positive events, such as future planning for retirement and travel, replete with pleasant images of retirement homes, exotic locations, and time spent with grandchildren. In effect, advertisements that target low income consumers lack inspirational messaging and long-term opportunities. Norton recommended that advertising and marketing strategies directed at low income consumers shift their direction from fear-based messages to messages that balance the fear aspects with aspirational opportunities, including a longer-term vision beyond the immediate future.

The panelists also discussed how lower income consumers and the more affluent population, tend to make different decisions relative to payment choice (i.e., cash vs. credit vs. debit card). Without a good understanding of the consequences, a switch in behavior from cash to credit can cause more problems and make it more difficult to recover (i.e., debt). According to Norton, "We need to encourage consumers to make better decisions when we introduce new mediums/interventions, such as mobile, because the medium in which you make decisions impacts your decision-making process." If used appropriately, the mobile medium ultimately can help consumers maximize their preferences over time.

Tescher noted the importance of marketing products to the underserved for a specific purpose rather than general use. Consumers may be less likely to adopt a product that does not clearly address a particular pain point or solve real problems for them. Once consumers realize the value of a product for a specific purpose, or that it solves a particular problem, there are opportunities to expand its functionality, solve more problems, and deepen engagement.

Consumer awareness is essential in fostering adoption of new mobile products and services. Therefore, marketing messages, product packaging, and product positioning are critical elements to help consumers recognize the utility and relevance of the product features. However, to meet consumers' changing needs and remain relevant, products should be continually adjusted. While awareness can motivate consumers to try new mobile products once, creating long-term changes in behavior and building sustainability must be fostered through everyday use (habituation) and experiences associated with such products.

III. Achieving Scale in Mobile Payments Through Consumer Habituation and Experience

In the afternoon session, panelists shared their respective views on the importance of consumer spending habits and experiential contexts in achieving broad scale adoption of mobile payments. The panelists represented a mobile platform provider, a retailer, a mobile wallet provider, academia, and a transit authority.

Achieving scale for a new product is contingent on a number of factors, such as the intended consumer (e.g., coffee drinkers, transit riders, low income, Gen Y, etc.), the product value proposition, product positioning, ease of implementation, interoperability, and the level of scale desired by the stakeholder (e.g., micro vs. macro). Other critical factors that help increase adoption and achieve scale include consumer habituation and experience. The panelists referenced the Starbucks mobile payments app as an example of a mobile product that has successfully achieved scale, with mobile payments now representing approximately 10 percent of Starbucks' in-store payment transaction volume in the U.S.[10] Panelists cited Uber,[11] a mobile car service app, as an example of consumer habituation driven by consistent, positive experiences. Uber has leveraged habituation to drive scale and adoption by masking the payment aspect of the transaction for the consumer, as the service is prepaid automatically through the mobile app, and creates a convenient method to request the car service.

Andrew Boch, from LevelUp, explained how his company, a QR code-based mobile payments platform provider, views scale from a micro-level. The LevelUp business model is based on tying rewards to purchases made at small, local businesses. LevelUp customizes its platform for each business implementation. This customization underlies how it evaluates merchant success and scale. For each merchant, LevelUp measures how its mobile payment platform performs relative to other payment methods (e.g., Visa, MasterCard, and AmEx). Boch explained that for one of its customers, SweetGreen,[12] LevelUp represents 30 percent of total transaction volume, which is its measurement for gauging progress towards scale.

Each mobile payments stakeholder defines how it creates consumer spending habits differently. For example, Spencer White, from Isis,[13] an NFC-based mobile wallet provider, discussed the importance of driving habituation without ubiquity, or driving everyday habitual spends (e.g., public transit riders/fares). Once mobile payment adopters realize greater everyday habitual spends, they will be more likely to begin to use the payment method in other commerce venues, such as merchants.

---

[10] See http://www.finextra.com/blogs/fullblog.aspx?blogid=8245.

[11] Uber is a mobile taxi-hailing app (and mobile website) that connects passengers with vehicles for hire. Launched in 2010 in San Francisco, Uber enables smartphone users to locate and request taxis with GPS. Customers enroll in the service and link credit/debit cards to their Uber accounts. For more information, see https://www.uber.com/.

[12] SweetGreen is a restaurant that offers healthy, organic and locally grown food. For more information, see http://sweetgreen.com/.

[13] Isis is a joint-venture between AT&T, T-Mobile, Verizon with participation by Discover, Wells Fargo, Barclaycard, AmEx, and MasterCard that uses a SIM-based secure element in the mobile device for NFC contactless mobile payments. Isis allows consumers to pay for purchases or transit (in UT) by tapping their NFC-enabled phones at the POS terminal. The wallet holds credit and loyalty cards, organizes offers, deals, and promotions, and shows card balances and recent purchases. For more information, see https://www.paywithisis.com/.

Kate Jaspon, from Dunkin' Brands, added that for Dunkin' Donuts, "nothing is more habitual than coffee," and emphasized three factors that will drive consumers to use a mobile wallet: "convenience, the delivery of value (i.e., rewards), and speed." The Dunkin' Brands business model is based on loyalty and measures success in achieving scale in terms of how its mobile app drives increased sales and efficiencies in its franchises. Dunkin' tracks the number of downloads of its mobile app, which when used by its customers, also allows Dunkin' to gather valuable information about frequent users, such as the millennial segment. By better understanding its customers, Dunkin' can deliver better value and create goals for generating more growth.

David Leininger, from Dallas Area Rapid Transit (DART) Authority, explained how the DART mobile ticketing app provides consumers with a better experience for a habitual spend–paying for transit fare. Consumers seek easy access and minimization of pain points. DART's app responds to these needs by enabling customers to purchase tickets in advance for multiple modes of transportation, thereby avoiding lines at ticketing kiosks. For ease of access, the mobile app provides fare collection across all three regional transit agencies, creating interoperability efficiencies and convenience to both transit operators and consumers. The early success of the DART mobile app[14] can be partly attributed to awareness generated through print media (e.g., brochures, posters) and marketing events (e.g., state fairs, museums, and games) for consumers and transit operators. DART's long-term success hinges on its successful collaboration efforts, not only in working with other transit authorities, but also in partnering with businesses such as museums, zoos, and other local attractions to provide consumers with greater opportunities to use their mobile app and expand the mobile experience.

Meera Venkatraman, professor of marketing at Suffolk University, emphasized the importance of product positioning when considering scale. She explained the need for marketers to consider how consumers will react to change with the introduction of new products. Venkatraman underscored earlier comments about the need to "start small and start specific" because adoption can be hindered by complicated messaging and excessive marketing of benefits and lead to consumer confusion. Consumers are more likely to adopt new and radical products when they recognize a clear value proposition and purpose that is an improvement over the current product. Hence, marketers tend to be overly optimistic when launching a new product; whereas, consumers tend to overvalue existing products.

Several panelists agreed that it is critical for a new mobile product to make a positive first impression, and therefore, a product should be launched only after it has been fully developed. Jaspon explained, "If you

[14] DART's mobile ticketing app was launched in October 2013 and exceeded 50,000 downloads within the first two months of the launch and total sales of $235,000 in the first month. For more information, see http://www.dart.org/.

do something wrong, customers are not likely to forgive you." Leininger reiterated the importance of continually adjusting and improving a mobile payment app to ensure continued use by consumers. Once consumers realize the benefits and value of using mobile payments for everyday spends and enjoy a better commerce experience, they will be motivated to become more frequent users and expand their use to additional venues, according to the panelists.

IV. The Transformational Role of Mobile Technology for Financial Services

The next discussion underscored the opportunities that mobile technology presents for transforming financial services, beginning with the potential that digital wallets have for helping to solve larger societal problems such as financial inclusion, encouraging more saving among consumers, and providing enhanced security.

Initially conceived as a way to facilitate commerce and attract consumers to retail locations with customized offers and tailored marketing, the digital wallet has evolved to encompass a broad range of financial services based on multiple underlying technology platforms–NFC, cloud, or QR code-based. The general consensus is that this diverse set of digital wallet technology offerings will continue to co-exist until consumers and retailers decide which business model will dominate the market.

Schulman explained that the future of digital wallets will depend on the ability to solve real consumer pain points, not on the underlying technology. But industry stakeholders will need to work collaboratively to identify the pain points that digital wallets can solve. Schulman added that merchants need an agnostic POS platform to enable broad acceptance, and that a mobile app can offer a flexible solution because it requires minimal change to the POS infrastructure.

The customization and personalization that mobile technology affords has also led to the transformation of digital wallets into mobile money management tools that can enhance the range of financial services to consumers and influence better financial decisions and savings. For example, consumers can use their mobile phones to check their account balances multiple times per day to determine if they have sufficient funds to make a purchase. Mobile phone solutions can help improve access to bank accounts and other financial services products, as traditional bank accounts may not be suitable for every consumer. Mobile solutions can also help small businesses manage their finances and increase engagement with their customers through data analytics and two-way communications.

Mobile solutions are often discussed in the context of mobile payments without consideration for the opportunities they present for consumers to save, a capacity largely underutilized by the U.S. consumer

population and a huge priority for the U.S. Treasury. Schulman explained how the notion of software in the mobile phone offers the capability for consumers to automatically save money. For example, the Bluebird® product from American Express offers a Reserve account designed to encourage savings. Thirty-six percent of consumers who have created a Reserve account are putting money into it on a recurring basis. Green Dot's GoBank offers a similar aspirational savings tool that enables customers to set aside funds from their normal spending plan. Melissa Koide, from the U.S. Department of the Treasury, emphasized the need to show that U.S. consumers have an appetite for these types of services–prepaid accounts that have savings functionality–because from a regulatory perspective, it is difficult to recognize these savings functionalities in the context of traditional banking.

Norton added that "research shows that getting people to save is really difficult." However, on a local level small interventions can have a huge difference. Providing tools to consumers can show them how to spend less and/or divert some money for future benefits (e.g., tools that show consumers how much they typically spend on daily coffee and their annual spend and how that money could be better used). This is another area where software can be introduced to help consumers automatically assess spending habits and potentially influence their spending decisions and divert funds to savings.

Finally, mobile technology has a significant opportunity to increase trust and security in mobile financial services. Confidence in the security and fraud/risk management controls is crucial for the right consumer experience. Mobile offers a number of safeguards over the traditional payment card, such as location-based services, device ID, and other functionalities inherent in the phone that can enhance security. Panelists noted how banks and leading non-bank providers continue to be at the top of the consumer trust chain in various industry studies, yet in many surveys consumers continue to rank security as their top concern for using mobile for financial services.

V. Conclusions

Although mobile payments adoption in the U.S. remains slow, panelists were optimistic about the potential for growth among retailers and transit–where consumers regularly spend money. Incremental growth in mobile payment use, through mobile apps or mobile wallets, will eventually lead to greater use.

Stakeholders must recognize from the outset what makes mobile different for the consumer, such as the potential for customization and personalization. This approach has been relatively successful in beginning to address financial pain points of the underserved through various mobile offerings, including mobile prepaid products. However, prepaid products require further consumer education and understanding in the U.S., as they are currently associated with high fees, weak consumer protections, and

disposability (i.e., one-time use). Better consumer education could help to convey the broad range of prepaid purposes and benefits. How to provide education is also a challenge, since there is often little direct human interaction between the solution provider and the consumer when provisioning the financial services application.

Identifying financial pain points for the general population has been an even greater challenge, explaining why many in the industry believe mobile payments adoption has been slow. Realizing greater scale in mobile payment adoption in the U.S. will require a change in consumer behavior that will have to solve specific consumer pain points and offer enhanced convenience and speed over existing payment methods. Mobile stakeholders recognize that achieving scale is an incremental process, so they are focused on encouraging consumers to use their mobile phones to make every day, habitual spends to pay for typical daily, low value purchases like coffee, transit, or food. To enhance the consumer value proposition, mobile payments should aim to improve the experience connected to the purchase, whether that involves ordering ahead, confirming product availability, offering rewards and coupons, or personalizing the purchase event. The future of mobile payments adoption should also focus on building adoption with the digital native, or those consumers who have grown up with mobile (i.e., millennials).

Appendix I

Moderators and Panelists

MODERATORS

Cynthia Merritt Jenkins, Senior Director, National Automated Clearing House Association (NACHA)

NACHA manages the development, administration, and governance of the ACH Network. The ACH Network provides a safe, secure, and reliable network for direct account-to-account consumer, business, and government payments. Annually, it facilitates billions of Direct Deposit via ACH and Direct Payment via ACH transactions. Used by all types of financial institutions, the ACH Network is governed by the fair and equitable *NACHA Operating Rules*, which guide risk management and create payment certainty for all participants. As a not-for-profit association, NACHA represents more than 10,000 financial institutions via 17 regional payments associations and direct membership. Through its industry councils and forums, NACHA brings together payments system stakeholders to foster dialogue and innovation to strengthen the ACH Network. http://www.nacha.org.

Ed Ponte, Senior Vice President, Strategic Services & Technical Sales, Monitise

Monitise is a world leader in Mobile Money–banking, paying and buying with a mobile device. Leading banks, payments companies, retailers and mobile networks utilize Monitise's technology platforms and services to securely connect people with their money. Already over 24 million consumers benefit from our patented technology to 'bank anywhere', 'pay anyone' and 'buy anything' accounting for over $50 billion of payments, purchases and transfers annually. www.monitise.com.

PANELISTS

Melissa Koide, Deputy Assistant Secretary, Office of Consumer Policy, U.S. Department of the Treasury

Treasury's mission highlights its role as the steward of U.S. economic and financial systems, and as an influential participant in the world economy. The Treasury Department is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the U.S. The Department is responsible for a wide range of activities such as advising the President on economic and financial issues, encouraging sustainable economic growth, and fostering improved governance in financial institutions. The Treasury Department operates and maintains systems that are critical to the nation's financial infrastructure, such as the production of coin and currency, the disbursement of payments to the American public, revenue collection, and the borrowing of funds necessary to run the federal government. http://www.treasury.gov.

Michael Norton, Associate Professor of Business Administration, Harvard University

Michael Norton is an associate professor of business administration in the Marketing Unit and Marvin Bower Fellow at the Harvard Business School. He holds a B.A. in Psychology and English from Williams College and a Ph.D. in Psychology from Princeton University. Prior to joining HBS, Professor Norton was a Fellow at the MIT Media Lab and MIT's Sloan School of Management. He is the co-author–with Elizabeth Dunn–of the new book, *Happy Money: The Science of Smarter Spending* (Simon & Schuster).

Jennifer Tescher, President and Chief Executive Officer, Center for Financial Service Innovation

The Center for Financial Services Innovation (CFSI) is the nation's leading authority on financial services for underserved consumers. Through insights gained by producing original research; promoting cross-sector collaboration; advising organizations and companies by offering specialized consulting services; shaping public policy; and investing in nonprofit organizations and start-ups, CFSI delivers a deeply interconnected suite of services benefiting underserved consumers. Since 2004, CFSI has worked with leaders and innovators in the business, government and nonprofit sectors to transform the financial services landscape. http://www.cfsinnovation.com/.

Dan Schulman, Group President, Enterprise Growth, American Express

American Express is a global services company, providing customers with access to products, insights and experiences that enrich lives and build business success. www.americanexpress.com.

Lewis Goodwin, Chief Executive Officer, Green Dot Bank

Green Dot Corporation is a technology-centric, pro-consumer bank holding company with a mission to reinvent personal banking for the masses. The company is the largest provider of prepaid debit card products and prepaid card reloading services in the United States, as well as a leader in mobile banking with its GoBank mobile bank account offering. Green Dot Corporation products are available to consumers at more than 80,000 retailers nationwide, online and via the leading app stores. The company is headquartered in Pasadena, California with its bank subsidiary, Green Dot Bank, located in Provo, Utah. https://www.greendot.com/greendot.

Spencer White, General Manager, Isis

Isis is a joint venture between AT&T Mobility LLC, T-Mobile USA, Inc. and Verizon Wireless and is based in New York City. The venture is chartered with building Isis, a national mobile commerce venture that will fundamentally transform how people shop, pay and save. The Isis Mobile Commerce Platform™ is available to all merchants, banks, payment networks and mobile carriers. www.paywithisis.com.

David Leininger, Chief Financial Officer, Dallas Area Rapid Transit Authority

Dallas Area Rapid Transit (DART) transports passengers around Dallas and 12 surrounding cities with modern public transit services and customer facilities tailored to make their trip fast, comfortable and economical. Its extensive network of DART Rail, Trinity Railway Express and bus services moves more than 220,000 passengers per day across our 700-square-mile service area. http://www.dart.org.

Dr. Meera Venkatraman, Professor of Marketing, Sawyer Business School, Suffolk University

The Sawyer Business School at Suffolk University is located in the heart of Boston's financial, healthcare, government and business centers. Founded in 1937, it has a mission of preparing successful leaders of global business and public service. The following degrees are offered: Bachelors of Science in Business Administration, MBA, Global MBA, Executive MBA, Online MBA, MS in Finance, MS in Accounting, MS in Taxation, Master of Public Administration, Master of Health Administration are offered. With more than 27,000 alumni, the Sawyer Business School is a global network of industry leaders. Our alumni can be found working all over the world. http://www.suffolk.edu/business/.

Kate Jaspon, Vice President, Corporate Controller & Treasurer, Dunkin' Brands

With more than 17,000 points of distribution in nearly 60 countries worldwide, Dunkin' Brands Group, Inc. is one of the world's leading franchisers of quick service restaurants serving hot and cold coffee and baked goods, as well as hard-serve ice cream. At the end of 2011, Dunkin' Brands' nearly 100 percent franchised business model included more than 10,500 Dunkin' Donuts restaurants and more than 7,000 Baskin-Robbins restaurants. For the full-year 2012, the company had franchisee-reported sales of approximately $8.8 billion. Dunkin' Brands Group, Inc. is headquartered in Canton, Mass. http://news.dunkinbrands.com/.

Andrew Boch, Vice President, Operations, LevelUp

LevelUp is an American mobile payments platform created by Cambridge, Massachusetts-based start-up SCVNGR. The LevelUp mobile application uses QR code technology to allow for mobile transactions to be made at local businesses via iPhone and Android phone. LevelUp was initially launched in March 2011 and operated for its first 3 months as a daily deals platform. In July 2011, LevelUp shifted away from the daily deal space to focus exclusively on their mobile payments solution. https://www.thelevelup.com/.

Mobile Payments in the United States: Mapping Out the Road Ahead

by Darin Contini and Marianne Crowe, Federal Reserve Bank of Boston; Cynthia Merritt and Richard Oliver, Federal Reserve Bank of Atlanta; Steve Mott, BetterBuyDesign
March 25, 2011

Full paper

Updated report (May 2013): **U.S. Mobile Payments Landscape – Two Years Later**

Executive Summary

In January 2010, the Federal Reserve Banks of Atlanta and Boston, through their Retail Payments Risk Forum and Payments Research groups, convened a selected set of key players in this country's emerging mobile payments ecosystem. The goal of the meeting was to facilitate a discussion among all involved parties as to how a successful mobile payments (as opposed to mobile banking) regimen could evolve in the U.S.

Over the past 15 months, the self-named Mobile Payments Industry Workgroup (MPIW), met five times to share information and ideas, discuss the barriers and opportunities resident in mobile payments, and ultimately, to suggest a vision for the building blocks of an efficient and ubiquitous mobile payments environment. Ultimately, the discussions of this group, along with additional industry dialogue and literature research, constituted a body of input to the development of a research paper regarding the future for point-of-sale (POS) mobile payments in the United States.

This paper, drafted by the Boston and Atlanta Reserve Bank payments research teams, does not necessarily reflect the opinions of the Federal Reserve Banks, the opinion of the Federal Reserve Board of Governors, or the opinion of any individual member of the workgroup. Rather, the paper represents the collective views of the authors based on the inputs noted above. The paper depicts the current mobile payments ecosystem in the U.S.; discusses barriers, gaps, and opportunities; and sets forth a set of foundational elements that workgroup participants believe are fundamental to the development of a robust mobile payments environment. This "vision" for the future is built upon the recognition that the current environment faces many challenges and that success will require extensive collaboration between participants to ensure that consumers see a homogenous solution as they do today in other payment channels such as checks, ACH, and cards. Moreover, it must be a solution based on agreed upon standards, rules, and practices that ensure seamless interoperability regardless of the handset, mobile carrier, financial institution, payment network, or merchant location involved in any individual's desired transaction.

The foundational components of success suggested by the work group include:

1. The proposed environment is best defined by the concept of an "open mobile wallet."
2. The mobile infrastructure would likely be based on Near Field Communications (NFC) contactless technology resident in a smart phone and merchant terminals.
3. Ubiquitous platforms for mobile should leverage existing rails, including the ACH network for non-card payments, and support new payment types that meet emerging needs.
4. Some form of dynamic data authentication would be at the heart of a layered mobile payments security and fraud mitigation program.
5. Standards would be designed, adopted, and complied with through an industry certification program to ensure both domestic and global interoperability, including a standard to ensure that devices used to facilitate mobile payments do not create any electronic interference problems.
6. A better understanding of a regulatory oversight model should be developed in concert with bank and non-bank regulators early in the effort to clarify compliance responsibilities.
7. Trusted Service Managers should oversee the provision of interoperable and shared security elements used in the mobile phone.

During their discussions, the MPIW debated the need for a new entity in the ecosystem directed at assisting the various parties to resolve issues of mutual concern and codify solutions in such a way as to facilitate interoperability and ubiquity. While many members felt that such an entity may be useful in the future, the general

EXHIBIT
9

sense was that it was too early in the evolution to fully understand how such an entity might be constituted and what its role might be. In the meantime, the MPIW indicated a desire to meet again, perhaps with some additional attendees, to continue to discuss issues resident in the foundational components discussed above.

Additionally, the group discussed the need for an industry "roadmap" that could focus short term investment and accelerate progress. Once again, the general sense was that the complexity of the environment and diversity of participants would make this a daunting task. Efforts to specifically prescribe such a roadmap could create results that are inconsistent with the outcome eventually produced from natural market forces. Therefore, the group decided that defining such a roadmap this early in evolution of mobile payments in the U.S. might stifle innovation.

The benefits of this document and the underlying participative work effort will be revealed by what happens next. This paper is intended to be a vehicle for socializing a concept or model for an efficient, secure, ubiquitous, and convenient mobile payments evolution in this country to a much broader group of industry players. They, in turn, must ultimately agree to support or modify the ideas contained herein as a means of moving forward, recognizing that the opportunity to achieve maximum benefits may be best realized by acting sooner, rather than later.

The ability of the two convening Reserve Banks to organize and facilitate the discussions that led to the publication of this document, in addition to the ongoing and highly engaged participation of a diverse group of mobile ecosystem players, speaks to the potential success of idea-sharing and demonstrates that collaborative efforts could work. The authors would like to thank all the participants for their engagement and contributions to this work. A note of special thanks goes to Steve Mott of BetterBuyDesign, who contributed heavily to this effort.

Full paper

Updated report (May 2013): **U.S. Mobile Payments Landscape – Two Years Later**

Mobile Payments in the United States

Mapping Out the Road Ahead

Darin Contini and Marianne Crowe, Federal Reserve Bank of Boston,
Cynthia Merritt and Richard Oliver, Federal Reserve Bank of Atlanta,
and Steve Mott, BetterBuyDesign

March 25, 2011

==========
The authors would like to thank the members of the Mobile Payments Industry Workgroup for their valuable contributions to the work effort and insightful ideas and comments that are the foundation of this paper. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Banks of Atlanta or Boston or the Federal Reserve System.

EXHIBIT
K-10

I. Executive Summary

In January 2010, the Federal Reserve Banks of Atlanta and Boston, through their Retail Payments Risk Forum and Payments Research groups, convened a selected set of key players in this country's emerging mobile payments ecosystem. The goal of the meeting was to facilitate a discussion among all involved parties as to how a successful mobile payments (as opposed to mobile banking) regimen could evolve in the U.S.

Over the past 15 months, the self-named Mobile Payments Industry Workgroup (MPIW)[1] met five times to share information and ideas, discuss the barriers and opportunities resident in mobile payments, and ultimately, to suggest a vision for the building blocks of an efficient and ubiquitous mobile payments environment. Ultimately, the discussions of this group, along with additional industry dialogue and literature research, constituted a body of input to the development of a research paper regarding the future for point-of-sale (POS) mobile payments in the United States.

This paper, drafted by the Boston and Atlanta Reserve Bank payments research teams, does not necessarily reflect the opinions of the Federal Reserve Banks, the opinion of the Federal Reserve Board of Governors, or the opinion of any individual member of the workgroup. Rather, the paper represents the collective views of the authors based on the inputs noted above. The paper depicts the current mobile payments ecosystem in the U.S.; discusses barriers, gaps, and opportunities; and sets forth a set of foundational elements that workgroup participants believe are fundamental to the development of a robust mobile payments environment. This "vision" for the future is built upon the recognition that the current environment faces many challenges and that success will require extensive collaboration between participants to ensure that consumers see a homogenous solution as they do today in other payment channels such as checks, ACH, and cards. Moreover, it must be a solution based on agreed upon standards, rules, and practices that ensure seamless interoperability regardless of the handset, mobile carrier, financial institution, payment network, or merchant location involved in any individual's desired transaction.

The foundational components of success suggested by the work group include:

1. The proposed environment is best defined by the concept of an "open mobile wallet."
2. The mobile infrastructure would likely be based on Near Field Communications (NFC) contactless technology resident in a smart phone and merchant terminals.

[1] Use of the MPIW in this paper represents the existing workgroup or a modified version of the group in the future.

3. Ubiquitous platforms for mobile should leverage existing rails, including the ACH network for non-card payments, and support new payment types that meet emerging needs.
4. Some form of dynamic data authentication would be at the heart of a layered mobile payments security and fraud mitigation program.
5. Standards would be designed, adopted, and complied with through an industry certification program to ensure both domestic and global interoperability, including a standard to ensure that devices used to facilitate mobile payments do not create any electronic interference problems.
6. A better understanding of a regulatory oversight model should be developed in concert with bank and non-bank regulators early in the effort to clarify compliance responsibilities.
7. Trusted Service Managers should oversee the provision of interoperable and shared security elements used in the mobile phone.

During their discussions, the MPIW debated the need for a new entity in the ecosystem directed at assisting the various parties to resolve issues of mutual concern and codify solutions in such a way as to facilitate interoperability and ubiquity. While many members felt that such an entity may be useful in the future, the general sense was that it was too early in the evolution to fully understand how such an entity might be constituted and what its role might be. In the meantime, the MPIW indicated a desire to meet again, perhaps with some additional attendees, to continue to discuss issues resident in the foundational components discussed above.

Additionally, the group discussed the need for an industry "roadmap" that could focus short term investment and accelerate progress. Once again, the general sense was that the complexity of the environment and diversity of participants would make this a daunting task. Efforts to specifically prescribe such a roadmap could create results that are inconsistent with the outcome eventually produced from natural market forces. Therefore, the group decided that defining such a roadmap this early in evolution of mobile payments in the U.S. might stifle innovation.

The benefits of this document and the underlying participative work effort will be revealed by what happens next. This paper is intended to be a vehicle for socializing a concept or model for an efficient, secure, ubiquitous, and convenient mobile payments evolution in this country to a much broader group of industry players. They, in turn, must ultimately agree to support or modify the ideas contained herein as a means of moving forward, recognizing that the opportunity to achieve maximum benefits may be best realized by acting sooner, rather than later.

The ability of the two convening Reserve Banks to organize and facilitate the discussions that led to the publication of this document, in addition to the ongoing and highly engaged participation of a diverse group of mobile ecosystem players, speaks to the potential success of idea-sharing and demonstrates that

collaborative efforts could work. The authors would like to thank all the participants for their engagement and contributions to this work. A note of special thanks goes to Steve Mott of BetterBuyDesign, who contributed heavily to this effort.

II. Introduction

Almost daily a new mobile payments venture is announced that makes it possible for a consumer or business to use mobile phone technology to enable or enhance the payment process. Initially, the focus has been on enabling a mobile device to be used as a browser, accessing existing internet-based banking and retail systems. More recently, attention has turned to the use of an application-enabled mobile phone as a payment form factor, substituting for a check, cash or a card to eventually create a mobile virtual wallet. Financial institutions are testing these capabilities, as are numerous non-banks, including some who operate in the internet space.[2] In some cases, the phone is simply used to initiate a card payment, but in other cases it is used to create a direct transfer to another individual or business using an existing bank-centric clearing and settlement capability (e.g. ACH), or an online payment service provider. Another variation embraces the concept of sending SMS (text) messages via mobile phone carriers, who perform the clearing and settlement function, as experienced in the successful program to funnel aid to Haiti in the wake of its earthquake disaster.

The concept of mobile banking and payments has resonated in many developing countries where lack of a physical banking or payments infrastructure exists.[3] Mobile payments have enabled financial inclusion for individuals and small businesses that are more remote from banks to overcome the limitations of physical transportation and utility systems. Mobile payments have even created a new currency in the form of airtime minutes. The evolution of mobile payments in the U.S. has followed a different path because of the well-defined banking and payments infrastructure already in place in the U.S. As a result, U.S. mobile payments have advanced more slowly; and many pilots, while conceptually interesting and educational, have failed to produce evidence of a currently sustainable business case. U.S. consumers are fortunate to have many different payment methods available to them, so the need for a fully deployed mobile payments alternative is not as obvious. Additionally, the cost of deploying the physical software and hardware elements of a ubiquitous mobile infrastructure is significant and must be justified in the face of uncertain consumer demand.

Nevertheless, there is growing evidence that mobile payments will become a significant element in the U.S. payments landscape in the future. A recent government report estimated that 18 percent of U. S.

[2] For example, Google, Amazon and PayPal, all who accept payments for internet purchases, are involved in mobile payments.
[3] Merritt, Cindy. 2010. "Mobile Money Transfer," Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, September.

households do not have a bank account[4], a key variable in the attractiveness of mobile payments in countries where the majority of the population is unbanked. However, in the U.S. it is not anticipated that the unbanked will be the take-off point for mobile payments. It is likely to be the smart phone user. About 34 percent of U.S. consumers now own a smart phone and that number is growing at a compound annual growth rate of 17 percent[5]. Most large U.S banks offer customized banking applications for smart phones. Contactless mobile[6] technology provides additional capabilities resident in chips that can reduce payments fraud and potentially the cost that merchants bear to ensure their card brands are PCI compliant. Finally, the U.S. continues to become a more mobile society where consumers are motivated to use their time wisely. All of these factors point to the potential success of mobile-based payments and related activities in the future.

Most firms that would benefit from the long term deployment of mobile payments are eager to understand the details associated with successfully deploying a mobile payments infrastructure and accelerating progress wherever possible. Consequently, the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta[7] and the Payments Research Group at the Federal Reserve Bank of Boston[8] have collaborated to provide a setting for mobile industry participants to meet and discuss ways to move forward. This Mobile Payments Industry Workgroup (MPIW) is comprised of organizations representing the end-to-end mobile value chain. Since early 2010 they have met quarterly to discuss the reality of mobile payments and discern the way forward. Many of the discussions were first time events involving participants who had not previously engaged in face-to-face conversations, yet through this process some agreement has been reached on a number of key variables applicable to a perceived formula for mobile payments success in the U.S.

Present at the meetings were mobile carriers, issuing and acquiring banks, card brands, payments processors, credential manufacturers, trade associations (including merchants), mobile software solution vendors, handset makers, and large online payment service providers. To focus the discussion of "what is possible," the participants learned more about each other's business propositions, engaged in group activities aimed at understanding what cost and revenue factors were present, discussed various barriers to success, and contributed input to a basic set of characteristics that would be common to a successful mobile payments architecture.

---

[4] FDIC. 2009. "National Survey of Unbanked and Underbanked Households," December.
[5] Javelin Strategy & Research. 2011. "Mobile Wallets: With the New Mobile Network Operator Joint Venture Isis, Are Cards and Cash Ready to go Mobile in 2011?" January.
[6] Contactless mobile and mobile NFC will be used interchangeably throughout this paper.
[7] Hhttp://www.frbatlanta.org/rprf/
[8] Hhttp://www.bostonfed.org/economic/cprc/index.htm

These discussions occurred in a very dynamic U.S. payments environment. Even as the MPIW was meeting, new mobile pilot programs were announced (some involving workgroup participants), the Durbin Amendment to the Financial Reform Act was adopted, other new mobile technologies were launched, and an initial interchange price regimen was proposed by the Federal Reserve Board of Governors. Nevertheless, the focus of the group has been on long run success in the creation of a profitable and ubiquitous mobile payments infrastructure. The chicken and egg challenges of merchant deployment and consumer usage were debated, the roles of banks and telecoms clarified, and different infrastructure models were discussed. Ultimately, it became clear that significant success was likely to come as a result of collaboration directed at identifying necessary standards and encouraging efficient implementations, rather than independent action.

In essence, this paper is intended to be a framework for more widespread industry discussion and debate that could lead to more sustainable progress in improving overall U.S. payments system efficiency and integrity than might occur otherwise. In the sections that follow, we define the composition of the mobile ecosystem, describe a vision for a successful implementation, address the potential benefits and drawbacks of mobile deployment, outline the obstacles and barriers to be addressed, identify the components of an industry business case, set forth key standards issues for discussion, explore various use case scenarios, and propose possible directions moving forward.

Ultimately, the value of this work lies in its overall acceptance and use, recognizing that the payments system environment today, while stable and secure, may be affected by any number of factors, including the broad spate of legal/regulatory activity emanating from Congress, therefore making it difficult to move to a single agenda.

The MPIW realized that there are various terms used in the mobile ecosystem that need to be explained or clarified. Consequently, we have included a glossary of key terms in Appendix I.

III. U.S. Mobile Payments Infrastructure Today

While mobile payments, as opposed to mobile banking, applications have gained notable recent success in other parts of the world, they are just beginning to emerge in the U.S. Mobile payments for physical goods and services (e.g. POS and transit) imply the use of near field communications (NFC) contactless technologies that are not yet prevalent in the U.S., even in the card world. While NFC-like contactless technologies (e.g. barcodes, stickers, micro SD chips) have been appearing in the market recently, the emerging common standard for POS mobile transactions is near field communication (NFC). NFC enables a transmission using a very short-range wireless connectivity technology with the capacity to execute payment transactions, and a secure element that securely stores information such as identity

credentials and financial value. The appeal of NFC is that it is compatible and interoperable with other current systems, e.g. transit and security. In essence, it is not a new technology and works with existing hardware, secure elements and communication protocols.[9] NFC-enabled mobile payments have the potential to be the universal contactless payment technology if necessary stakeholders have the economic incentives to adopt it.

The slow evolution of contactless mobile payments in the U.S. is also indicative of a number of barriers that exist, as discussed in more detail later. As examples, the card networks, issuers, and acquirers have developed robust fraud analytics around mag-stripe technology and NACHA has developed monitoring processes which have mitigated ACH risk to a certain degree. Stakeholders are reluctant to invest in terminals and handsets in the absence of more certainty around changes to the infrastructure and the risk of making the wrong business decisions. The cost for merchants and issuers to invest in new device readers at the POS and for contactless chip-enabled payment devices, including cards, phones, and possibly other form factors, is significant.

Essentially, as discussed below, each primary stakeholder in the mobile payments ecosystem has its own ideas about how mobile payments should be developed and implemented, creating potential conflicts and barriers to development of a ubiquitous, interoperable solution for mobile payments. The market is moving quickly and there are still issues not fully resolved. So, there is benefit to convening the mobile stakeholders regularly to discuss the rules and framework of the mobile ecosystem as it evolves.

Mobile network operators (MNOs) own customer billing infrastructures that they can leverage to add value to existing voice and data services. While financial services such as mobile payments may represent an extension to existing customer relationships, the MNOs are new to financial services and have expressed concern about assuming material credit risk, based on their limited experience in providing consumer protections for financial services. However, the MNOs are experienced in providing subscriber acquisition and authentication, device provisioning, customer support and value added services, all necessary for increasing mobile payments. Additionally, they are a vital enabling technology channel for mobile payments**.**

U.S. financial institutions have not offered mobile financial payments because of a perceived lack of a good business case, although the growth in mobile banking implementations and recent mobile payment trials signal this may be changing. Financial institutions have the opportunity to add value to customer depository services with the addition of mobile technology and realize customer retention benefits as a result. With their long time experience handling payments, addressing customer authentication and authorization requirements, and enforcing Know Your Customer (KYC) rules,

[9] While there are other security options in addition to the secure element, e.g. cloud-based systems, this paper focuses on a secure element embedded in the phone.

financial institutions are well postured to settle payments to a consumer's account and to employ risk management programs that ensure regulatory compliance for money laundering, consumer protection, and other risks. Basically, financial institutions want to remain at the center of a customer's account relationship by issuing payment credentials and applications on the mobile device as they do in the physical payments world today.

Handset manufacturers must produce smart phones capable of including NFC technology and related security software and then pair with the MNOs to provide utility to the consumer. How to handle functionality around locked vs. unlocked phones, authentication, and the ability to use the mobile phone for NFC payments without the network all need to be addressed. Furthermore, technology needed on the handset to accommodate mobile payments is changing rapidly (e.g. SIM, micro SD, NFC sleeves) in order to address security challenges and compliance with MNO and payments certification. Yet, handset manufacturers around the world are beginning to issue standard handsets in volume that will embrace such technology in the next year or two.

Trusted Service Managers (TSMs), building on their role in the card world, have emerged as the entity responsible for provisioning credentials to secure elements in mobile phones as a necessary tool to provide the type of transaction security users will accept. Depending on the size and scope of a TSM, other functions may include provisioning/account set-up; ensuring compliance with security requirements for software, hardware, handsets, chips and applications; fraud and risk management; and customer service and support. Customer support might include handling device/service questions and resolution relating to secure element use; developing and maintaining user documentation for best practices; support and assistance for operating system and mobile application software upgrades and mobile vendor certification; lost/stolen/upgraded phone notification to customers; handling billing questions; and reporting fraudulent transactions.

Merchants are critical stakeholders in the chicken and egg equation of mobile payments adoption. Merchants are interested in secure payments at the point of sale, timely settlement, manageable investment in infrastructure, relief from costly data protection inspection obligations, and reasonable interchange for transactions. Without widespread merchant acceptance, it will be difficult for NFC mobile payments at POS to achieve mass adoption.[10] [11] Merchants must plan for and adopt the POS terminal technology necessary to work with wireless devices developed and deployed by the MNOs and handset makers. Depending on the application the merchant may need to interact with a particular bank. When the payments application used in a mobile transaction is a card application, the merchant must

[10] National Retail Federation. 2010. "Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape," version 1.0.0. White paper, May.

[11] Merchant Advisory Group. 2010. "Open the Curtains in the Payment System - Merchant Advisory Group Recommendations on the Mobile Transformation Opportunity."

work with an acquiring bank to begin the clearing and settlement process. For ACH at the point-of-sale, the merchant must integrate with an originating FI.

Intermediaries/third party processors and online payment service providers have emerged to provide the enabling technology for mobile financial services or to serve as intermediaries in the payments supply chain. These processors and online payment service providers, mobile software solution vendors, and application and hardware developers are partnering with financial institutions or MNOs for the provision of mobile proximity payments. The third party non-banks see mobile as a new market opportunity and must be included in any infrastructure plans for mobile payments. They may also consider the existing environment too constrained by regulation and entrenched providers and seek to disrupt the payments ecosystem with a new offering.

Consumer demand for mobile technology is very high, but their interest in mobile payments is uncertain due to their lack of experience using mobile devices for that purpose. Consumers have many safe and efficient payment choices in the U.S. so the case for shifting to mobile payments must include new features and value. The rapid advance of electronic payments in the United States is a testament to the fact that ultimately, consumers want payments that are convenient, inexpensive, and secure.

Payment Card and ACH Networks all play a key role in the mobile payments ecosystem, although at this stage of the evolution, each network has chosen a different path to implementation. Some are partnering with mobile carriers to develop new ventures, while others are working with banks and transit authorities to test different or new forms of mobile wallets. NACHA is analyzing its rules to properly route new mobile payment transactions. Regardless of the interim actions, credit and debit card accounts will be critical to the long term success of ubiquitous mobile payments, given their dominant base of customers.

Regulators must participate in the evolution of mobile as the regulatory framework for mobile payments is fragmented with respect to MNO and other third party participation in the provision of payment services. In business model examples where payment flows leverage existing value chains of networks and payment clearing and settlement systems such as the card brands and the ACH, existing regulatory oversight and consumer protections are expected to prevail. However, questions are arising about the legal liabilities and responsibilities of new parties to the payments transaction, which may be governed by agreements between the stakeholders in the value chain. Participants desire clarity of the new regulatory structure and want to know how to be proactive in addressing consumer protection issues such as identity management, cyber-security and prepaid mobile accounts. Dialogue between FI regulators, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and the Department of Commerce, *and* with mobile industry stakeholders is necessary to ensure that emerging

mobile payments services are conducted in a way that enhances safety and integrity in U.S. payment systems.

IV. Long-Term Vision For the Future Environment

As the MPIW discussed the future over a series of five meetings, a vision for the long-term mobile ecosystem emerged, in terms of successful business models and the important components of a mobile payments operating framework, such as standards and guidelines. While not all parties agreed in full, a decision was made to intentionally limit the scope of the effort to mobile payments at the point-of-sale. The group acknowledged that the mobile framework is not tied just to payments and that there is a need to look at opportunities to drive m-commerce, including value-added features such as coupons, rewards, clinical services, etc. The group further recognized that mobile has the potential to be a key component in making and/or securing remote payments and authenticating payments made via internet or card (i.e. card-not-present transactions). However, that possibility was viewed as something the group could discuss going forward.

The group opined that the potential societal benefits created by mobile-enabled payments technology, including the potential to reduce payments fraud and expand financial inclusion, portend a future where the mobile phone becomes the consumer's wallet and provides a seamless customer experience. This new mobile wallet will be enabled by NFC contactless technology embedded in the mobile handset so that it can store secure payment and identity information, as well as provide a secure access channel to payment services.

Ultimately, the successful mobile-enabled payments network will leverage a set of common standards and open platforms to ensure global interoperability. In a perfect world, mobile-enabled payments will be as interoperable as card payments are today, where consumers can use cards for payments anywhere in the world. Ubiquity will be achieved by creating a set of standards for payment applications that co-exist in a mobile wallet open to all card (credit, debit and prepaid) networks as well as ACH, that work across all carriers, and are accepted by all merchant POS terminals across all borders.

It is therefore critical for all participants in the future mobile payments environment to work together to design a model for interoperability that has the advantages of the card model and includes global industry standards. While the emergence of competing proprietary offerings encourages innovation, it also bears the risk of creating silos that may impede the development of critical mass needed to ensure a successful payments network. While workgroup participants were not in a position to establish consensus with respect to specific standards, all agree that the long-term vision of a successful mobile payments system in the United States will occur through the creation of mutually agreeable

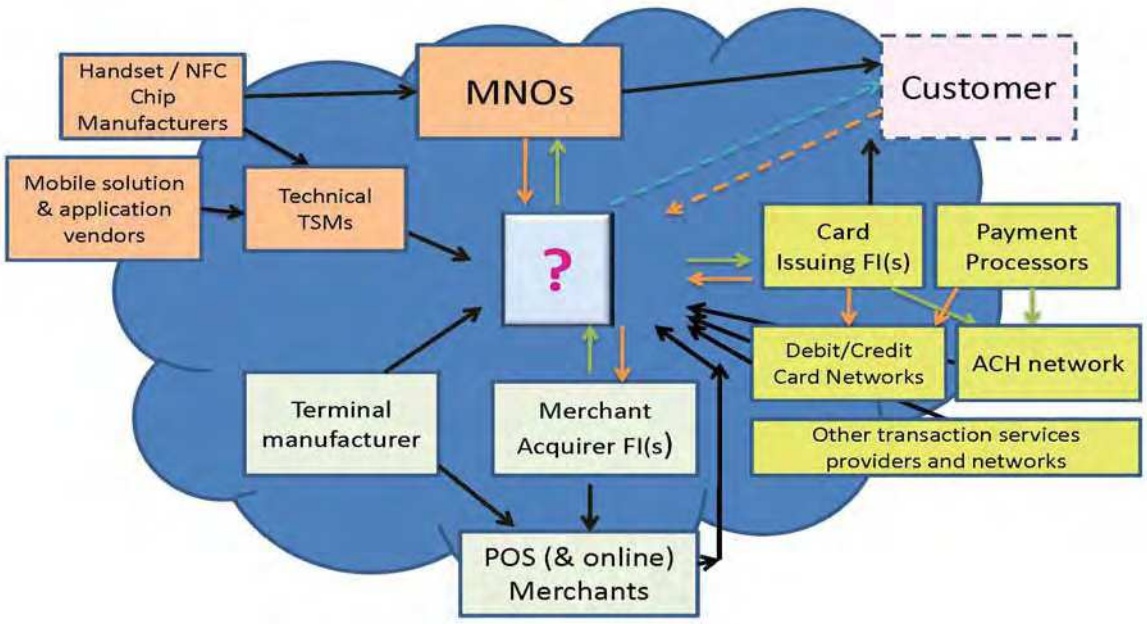
foundational principles. The goal of these principles will be to foster an interoperable mobile payments ecosystem; one that accommodates the customer of any financial institution or mobile carrier, thereby eliminating the need for compulsory customer movement between carrier or card brand (a common complaint today) and allows the customer to use multiple payment methods wherever merchants accept them. It is likely that a mutually agreed upon strategy will be necessary to provide the guidance and incentives to foster the evolution and migration to a ubiquitous mobile environment.

Business models

The major mobile stakeholders must determine the appropriate business model for the mobile payments infrastructure. The decision is complicated by the need to converge payments and mobile communications. The creation of a combined model requires the cooperation of multiple parties, including financial institutions, mobile operators, payment networks, technology service providers, chip and handset makers, and ultimately, merchants and consumers. While the MPIW did not discuss the different models at length, the consensus generally pointed to the possible co-existence of three basic business model scenarios within the mobile payments ecosystem (operator-centric, bank-centric and collaborative). In the operator-centric model the MNO owns the customer relationship for payments made using the mobile phone. In the bank-centric model banks own the customer relationship and mobile payments are processed over traditional payment networks (credit, debit or ACH). Each model could be utilized depending on the type and value of a purchase; the payment venue (e.g. physical POS, remote POS or internet); or other payment scenario.

The collaborative model (see Figure 1) emphasizes the need for an entity that would manage or work with all the parties in the mobile payment ecosystem to facilitate an efficient, holistic environment and provide oversight, business rules and standards for multiple service providers. This entity would serve as a neutral third party to assist other participants in creating a level playing field to facilitate faster and fuller market adoption. On behalf of all participants, it could tackle business issues of mutual need, such as determining the relative liabilities of each party, creating business standards and operating rules for handling customer problems, and leveraging the best practices and expertise of each individual mobile stakeholder.

Figure 1: Collaborative Model



The remainder of this section discusses how the different stakeholders might function with and without a collaborative framework in the mobile payments ecosystem.

Mobile Network Operators, working with partnered handset manufacturers, would continue to control access to the mobile channel and have secure elements configured into their offerings. However, they have limited experience with payment-related application or cryptographic data and while they have extensive account management experience, they have little experience dealing with banking and payment rules and regulations to protect consumers. Without collaboration of some sort, they would need to build new capabilities that go beyond their core business competencies to support mobile devices with broad mobile commerce capabilities; establish thousands of new relationships with financial account holders; and develop complex data centers that comply with industry security standards. Finally, MNOs would have to develop reciprocal agreements for commerce with each other so that account access could travel as easily from device to device as phone numbers do currently. In a collaborative model these elements could be managed by each party agreeing to a central set of guidelines.

Payment Card Networks have existing infrastructures for credit and debit contactless transactions and already perform a rules-making and fee-allocation capability related to card processing and

settlement. However, they lack access to the customer's DDA account and related data. Without collaboration they may not be able or willing to reach agreements about sharing data between competing entities.

Financial Institutions would continue to be at the center of their customers' financial activities, having a more trusted relationship and access to their own customer data, as well as secure data center capabilities that allow them to directly serve existing clients. Consequently, banks are well positioned to move consumers to new technology. However, banks will need the interoperability necessary to handle mobile payments involving other banks' customers and those customers who use different mobile carriers. Otherwise, without an open wallet, an FI would be able to work only with its own customers, unless it had bilateral agreements with other banks and carriers. Absent some scheme that facilitated multilateral relationships, having hundreds of bilateral agreements between banks and MNOs would be inefficient and fragmented, and not work well for mass adoption.[12]

Payment Transaction Processors and Online Payment Service Providers would continue to provide multiple-account payment processing services, perform credit and debit card provisioning and have existing extensive relationships with banks, merchants, credit card networks, pre-paid account service providers and technology providers. They would also have an extensive data support infrastructure to securely handle large amounts of financial and transactional data. While they might be able to provide more agnostic services for handling various credit and debit instruments, without collaboration they would need to establish multiple relationships with mobile carriers and expand relationships with banks to fully service consumer account management.

Mobile Technology Solution Providers, which include mobile payment application developers and TSMs, such as those who provision smartcards, secure elements and NFC chips, have the most experience and expertise with complex technology. While they may have collaborated on technical standards, such as ISO 14443, they have limited experience in dealing with payment rules and regulations to protect consumers. Technology providers would need to develop two-way relationships with carriers and banks, and with each other, since in some cases they are direct competitors.

A successful future mobile payments ecosystem requires an open payments system with interoperable services based on industry accepted formats, and technology standards that allow multiple parties to transact freely, but with some coordination and structure to ensure safety and efficiency within the mobile payments system. A collaborative model could provide stakeholders the opportunity to leverage their respective competencies for the collective good of the payments system overall. However, the number of stakeholders in the mobile ecosystem creates a more complex model that will require time

[12] For example, NACHA rules and ACH operator agreements create the effect of widespread multilateral agreements.

in which to establish industry norms for agreements and standards that will govern the interrelationships and their roles, responsibilities and liabilities. In addition, the MPIW was concerned that excessive coordination can sometimes stifle innovation.

Consequently, the MPIW felt that it was premature to consider such a model in the current market and it was decided to leave this discussion for a later time. Interestingly, a nascent version of the collaborative model was announced in November, 2010, by AT&T Mobility, T-Mobile US and Verizon Wireless, that includes a card network (Discover) and a bank issuer (Barclays Bank U.S.).[13] The joint venture, referred to as Isis™, is chartered to pilot a national mobile commerce network and an NFC mobile wallet. Isis will need to establish the rules of engagement, standards and customer needs within its collaborative effort and plans to have the scope and scale necessary to introduce mobile commerce on a broad basis, hoping to make it available to all interested merchants, banks and mobile carriers going forward.

V. Strategic Fundamentals of the Vision

The U.S. mobile payments market, particularly in the last year, has begun to move down what appears to be an obstacle filled path, absent any shared vision regarding key principles for success. All parties recognize at some level, however, that they share some common goals. Ideally, mobile commerce participants need to be able to flourish equally in the mobile ecosystem. FIs, merchants, payment networks and carriers need to be able to reach their own customers (and potential new customers) with innovative product offerings. Consumers should benefit from products and services that are standard and secure and that make purchase decisions easier for them, while a ubiquitous mobile commerce environment will provide the desired revenue opportunities. Further, through the implementation of common standards, costs can be reduced and integrity of the network increased.

As the MPIW met over the past year, the group's increasingly candid discussions led to a series of shared observations (or shared vision) about the nature of the necessary underpinnings of a successful

[13] On November 16, 2010, AT&T Mobility, T-Mobile USA and Verizon Wireless announced formation of a joint venture chartered with building Isis™, a national mobile commerce network to fundamentally transform how people shop, pay and save. With mobile payments at the core of their offering, they plan to create a mobile wallet that ultimately eliminates the need for consumers to carry cash, credit and debit cards, reward cards, coupons, tickets and transit passes. Isis expects to introduce its service in key geographic markets during the next 18 months. ATT, T-Mobile USA and Verizon Wireless collectively provide wireless services to more than 200 million consumers who will have access to the Isis service. Isis will utilize Discover's national payment network initially, which is currently accepted at over seven million merchant locations in the U.S., to develop an extensive mobile payment infrastructure for the joint venture, and Barclaycard US as the first issuer. See H**http://www.paywithisis.com/#/news/**

future move to mobile NFC payments in the U.S. What follows is the workgroup's assessment of a set of foundational principles necessary to achieve mass adoption of NFC mobile payments in the U.S. These principles will require stakeholders to tightly coordinate efforts to develop a fully integrated end-to-end mobile payments process and represent a set of fundamental "business requirements" for success. The more rapidly they are achieved, the sooner the benefits of mobile payments will be realized.

Foundation Principles

1. Open Mobile Wallet

A successful model for the future should be based on a standard definition of an ***open*** mobile wallet, one that carries broad payment and merchant/marketing value options for consumer choice. Such a platform would embrace a technical architecture that enables the wallet to support a wide range of payment methods and networks, would comply with agreed upon industry business rules and standards, would employ a secure element or container in the mobile phone to interface with the mobile payment applications, and would utilize appropriate wallet protocols and processes, such as the ability for multiple payment applications to share the wallet. The mobile wallet would exhibit all of the flexibility resident in a physical wallet today, including payment-related functions such as loyalty program applications.

Current and planned contactless card/mobile NFC (pilot) deployments are not true mobile wallets by this definition as they offer constrained payment options which limit consumer choice and utility. Since the MPIW views mobile marketing, advertising and promotions, as well as transit, as primary business case drivers for NFC payment deployment (i.e., payment capabilities are a 'qualifying' factor in the business case, but not a 'differentiating' factor), there will be a need to understand and perhaps provide input on or recommend standards for security (including accommodating multiple payment options and applications with multiple secure elements in the handset chip accessing multiple regulated banking networks), privacy, compatibility and interoperability.

2. *Implement a mobile NFC contactless scheme with a specific (embedded) hardware component that may or may not include a micro SD form factor.*

The NFC scheme should be based on an industry standard, capable of supporting all payment methods and networks, able to comply with business rules and standards and reside in a secure container in the mobile phone to interface with mobile payment applications. The contactless NFC solution developed must work globally and in all venues (retail, transportation, as well as ATMs). Contactless payments employing computer chip security and near field communications (NFC or radio wave) technology based on ISO 14443 via mobile devices represent a preferred embodiment of future payments

in the U.S. When used at the POS, the contactless form factor should follow established contactless standards as endorsed by ISO and NFC industry groups, such as SmartCard Alliance, NFC Forum, Mobey Forum, etc. Who would be responsible for designing and developing the solution needs to be determined. Minimum compliance requirements for adoption should include dynamic data authentication, m-wallet contactless functionality and a secure element in the mobile phone.

Utilizing NFC contactless technology for mobile payments assumes that handset manufacturers will commit to putting NFC chips on a large number of new smart phones by some future date. It also assumes that the majority of merchant terminals in the U.S. will simultaneously be upgraded to contactless/NFC. Having some idea of when NFC mobile will be implemented, even without a formal roadmap, would help the merchants plan their investments. Achieving such synchronization, however, will require an extraordinary amount of collaboration, absent a highly participative forum for such discussions.

3. *Establish a ubiquitous platform for mobile payments that uses existing clearing and settlement channels and rails (credit, debit, ACH, prepaid, carrier billing) but allows for new rails as they are developed.*

The existing clearing and settlement rails are the necessary foundation for the mobile payments platform in order to create opportunities for mass adoption and consumer choice. While new payment channels may be created in the future, the MPIW supported the use of existing clearing and settlement systems to exchange payment information and value. Given the ubiquity of the ACH network, and the growing modes and ease of access to it, the ACH option may be critical for supporting a customer's desire to use mobile payments to replace physical cash or check transactions (i.e. non-card transaction) by enabling funds to change hands between parties via direct debit and credit. In addition, merchants who are too small (in sales volume and/or revenue) to qualify for accepting credit/debit cards could use ACH on the mobile phone to accept electronic payments in place of cash or checks.

4. Adopt dynamic data authentication for long-term integrity and security in all card–based transactions and across all channels.

Dynamic data authentication protects cardholder and other payments data by making each mobile payment transaction unique. A valid cryptogram is generated for each transaction, which is then verified when the transaction is authorized. The cryptographic value, including transaction-specific data elements, is validated through the terminal with the network to protect against fraud. The chip device (card or phone) must be present to generate a valid cryptogram, which is verified online or offline when the transaction is authorized. Many issuers already are providing contactless payment cards with dynamic

cryptograms, which is how contactless transactions have improved payment security. Dynamic authentication technology on mobile phones would lower fraud because, absent the sequential codes on the embedded chips, stolen payment card information could not be used to make counterfeit cards or fraudulent online transactions. In addition, the group noted the possibility that this technology could, over time, be applied to the card-not-present venue.

5. *Develop and adopt a global interoperable platform in the U.S. for standards and certification of payment methods for an open mobile wallet, applications, NFC, etc. Leverage existing standards where possible.*[14]

Using a special carrier-issued chip in the phone, consumers currently enjoy the ability to use their mobile phones on a global basis. Adding payment functionality to the phone, however, presents a number of challenges, particularly in the area of compatible standards. There are several existing mobile standards bodies such as GSMA, GlobalPlatform, ETSI (European Telecommunications Standards Institute) and the NFC Forum. Differences in what each standards body addresses and gaps in coverage for mobile payments will need to be identified and resolved, particularly where there is no overarching standard today, as is the case for a TSM in the U.S. Standards for implementing a secure element structure and technology must also be developed to ensure that a secure platform is open and works with multiple applications in the mobile wallet.

Absent a coordinating body, the industry will be hard pressed to analyze applicable global standards and the impacts to the different industry stakeholder groups, determine if changes to the standards are needed to accommodate contactless/NFC mobile payments and what the timeline and resource requirements would be. For the near-term (3-5 years) there is likely to be a wide array of initiatives to be aware of, provide input to, and consider incorporation of for deployment and operation in the U.S.

Full-NFC deployment will involve several infrastructure elements (e.g., a variety of secure elements in handset chips; multiple payment options with separate regulatory requirements in open wallets; management of security and operational services; etc.).

The industry will also need to consider how to address configurations other than full-NFC, such as micro SD cards or NFC stickers that perform lightweight implementations of NFC transacting. Some view these 'NFC-lite' deployments as preceding full-NFC in the U.S., and there are notable pilots involving banks underway and planned. Others view NFC-lite deployments as more likely to continue to occur after full-NFC attains critical-mass adoption, filling in with limited functionality, but sufficient security for users of less-advanced handsets, (i.e. backwards compatibility for awhile). The former view might relieve the industry from expending efforts that distract or dilute mapping out the infrastructure

[14] See Appendix IV for a discussion on current standards activities.

requirements for full-NFC, but the latter view raises the perennial need for the industry to figure out how to accommodate users who lag behind the technology adoption curve.

Finally, additional standards may need to be developed or modified to ensure that the NFC RFID chip communication does not interfere with other wireless network communication. The CTIA can potentially conduct tests to address this issue within its existing device certification initiatives; and improve clarity of member-driven initiatives for device certification. Working with CTIA members, terminal vendors, financial services providers and regulators, such as the FCC, the MPIW could assist in development of a comprehensive consumer, merchant and ecosystem-wide education and monitoring program.

6. Regulatory Clarity

Mobile transacting will cross over domains covered by multiple regulatory agencies—the Fed/FDIC/OCC/NCUA for banks, the Department of Commerce for identity protection, the FCC for wireless carriers, and the FTC for consumer product protection.[15] The MPIW wants to understand sooner rather than later the regulatory focus and oversight regimen of each agency in the mobile payments world, as well as the applicability of current regulations and laws to the mobile environment, in order to avoid potential missteps as they proceed to develop mobile payments solutions. This was viewed by all parties in the MPIW as a key priority for the Fed to initiate and initial steps have been taken to begin dialogues with these agencies. A workgroup assigned to identify regulatory gaps, with supporting resources beyond the original MPIW membership, would assist in such an effort.

7. Trusted Service Managers should oversee the provision of shared security elements used in the mobile phone.

There are several companies that manufacture secure elements. The TSM role would be to manage and control the provision of the secure elements in the mobile phones. The TSM may also perform other account management functions as discussed earlier.

Focusing on the core principles discussed above, the MPIW indicated a desire to continue meeting following a period of broader review of these principles by all stakeholders in the industry. The sense was, that absent any other inclusive industry forum, the continuation of the MPIW, perhaps in some expanded form, would benefit the stakeholders in the mobile ecosystem by providing a venue for the group to begin resolving some of the barriers and issues related to the list of foundational elements in order to successfully incorporate them into a mature system. For example, obstacles that need to be

[15] The new Consumer Finance Protection Bureau (CFPB) may ultimately weigh in on consumer protections for mobile payments.

resolved over the next 3-5 years to achieve true commercial adoption of NFC payments at retail POS may include commercial availability and widespread adoption of smart phones containing NFC chips; secure element resolution (ownership, standards, etc.) and implementation; identification and resolution of technical and business risk and security issues; agreement on the best business models; implementation of contactless readers at an acceptable number of merchant locations; agreement between regulatory agencies on regulatory requirements, assignment and changes (even if the regulatory changes have not yet been legislated); consumer and merchant education plans; etc. Many of these activities will likely need to be completed in overlapping periods, with some dependencies.

The MPIW also discussed the concept of developing an industry roadmap for moving forward, perhaps as a vehicle to clarify direction and encourage faster adoption of necessary change. Typically, such a roadmap might document a detailed explanation of the potential barriers to mobile payment adoption and recommend approaches (with cost/benefit analysis) to address them. A roadmap might also include best practices for the technology (hardware, software, terminals, chips); security (EMV[16] or something similar), dynamic data authentication, secure element (what is in the secure element and how is information involving payment credentials protected, etc.); interoperability; vendor/application management, vetting and certification; consumer relationship management (including enrollment, service and support for phone usage, recovery if lost or stolen, problems if bad applications downloaded); liabilities (who is responsible for exception handling and problem rectification); fraud and risk management practices to address consumer and merchant security; and regulatory protection and education.

In its fullest form, a roadmap could also discuss consumer use from an academic, non-competitive basis. It could identify the consumer value proposition, which is critical for achieving broad adoption. It could address ways to understand what motivates consumers and how to convince them of the benefits of switching payment methods. The roadmap could highlight ways to develop a viral marketing program to build mass adoption. Obtaining a better sense of consumer and merchant preferences and concerns would enhance the roadmap. In other industries, as well as payment associations such as NACHA, roadmaps are augmented by shared surveys directed at various stakeholders, which in this case would be consumers and merchants.

Ultimately, the workgroup felt that it would be premature to try to develop a roadmap that would influence the broad range of mobile payment stakeholders. The mobile payments industry is in its early stages of development in the U.S. and is characterized by experimentation and pilots which typically inform longer term thinking. Moving too early to determine common ground, establish standards, and

[16] EMV is used today in other countries for card payments. The MPIW discussed briefly the possible intersection of EMV with mobile payments in the U.S. For a more detailed discussion, see Appendix II.

develop rules of exchange could stifle innovation and reduce consumer choice. Further, certain key elements of the mobile payments infrastructure are still in pilot phase globally, implying that the adoption of standards (such as NFC standards) may, in some cases, still be a work in progress. In essence, the group felt that attention would be better focused on some selective barriers and issues in the short term and that an industry roadmap might better be approached in the longer term, if market forces produce inefficient outcomes.

Finally, the workgroup touched on another key issue - the role of the consumer helping to secure the future mobile environment. The group felt that future discussions should also include a plan to get consumer buy-in on shared responsibility for risk management. Unlike what unfolded with e-Commerce, where "zero liability" policies by the primary card brands produced a flood of repudiated transactions and so-called 'friendly-fraud' (along with a black market in stolen mag-stripe card credentials often fed by irresponsible cardholder behavior), the mobile venue needs to be *better*. That is, consumers need to buy-in to their role in ensuring a secure, private and efficient payments system and correct the bad habits they developed online. Consumer education related to security is critical for them to understand and know how to identify fraud risks on their end, assist in fraud prevention, and use the security tools that will be available to them in the mature mobile environment. Collaborating in some form to provide such education is a topic that needs to be addressed. Ultimately, the educational process must be coordinated, supported and, potentially enforced within the mobile ecosystem with a goal of helping consumers understand why they should upgrade to more secure handsets and employ best practices for usage in order to protect themselves and the entire mobile payments ecosystem from harm.

VI. Potential benefits of contactless mobile payments ecosystem

The creation of a contactless mobile payments infrastructure in the U.S. would provide a number of definable benefits, including improved fraud reduction capabilities, improved cost efficiencies for merchants and issuers, better data privacy, international compatibility, and reduced risk of settlement.

Fraud reduction

The contactless mobile platform, replete with chip capabilities, can take advantage of the intelligence of the chip and the resultant layering of security tools to provide security features not present in today's mag-stripe environment where skimming and counterfeit production are prevalent. The contactless mobile solution provides the framework for the enhanced security present in the EMV chip+PIN card environment, while also introducing new security layers unique to the mobile phone, including password protection to operate the mobile phone and access applications securely embedded in

the phone. Once at the mobile menu, access to individual mobile banking and payment applications can be further password protected. The EMV chip-based card, which can be replicated in the mobile chip, (although standards for contactless EMV must still be developed), contains individual account credentials, which can remain encrypted to the reader while an authorization is in progress (in some robust implementations). The PIN is also encrypted between the card and the reader, adding a second authentication factor dynamically to the transaction authorization.

Adding mobile data, such as location awareness, phone numbers or carrier accessed device IDs (e.g. MSISDNs or MDNs), can enhance account data, which banks use for risk management and the passing of encrypted tokens and PINs. Among cooperating stakeholders in the mobile ecosystem, utilizing all the data fields and information available with the mobile transaction end-to-end can logically and technically make the mobile transaction even more secure.

The mobile phone can also be used as a security tool for financial payments made at the physical POS and over the internet. The customer is always available, real-time, during a mobile payment transaction. If a network or issuer wished to authenticate customers with a real-time SMS challenge question, application or phone call, it could do so.

Furthermore, in addition to dynamic data for authentication, the mobile channel can support the other big fraud reduction initiative in the U.S.: preventing fraudulent transaction accounts from being set-up using credentials that might have been exposed (credit card numbers, demand deposit accounts, social security numbers, etc.). Better account set-up requires improved registration and enrollment processes, with higher levels of identity verification accessibility and utilization. The enrollment process for mobile banking and payments applications, including NFC provisioning and set-up with device-internal protections, could materially improve the registration and verification process. The additional enrollment process supplements the FI's own account-sign-up mechanisms and enables a much broader set of data about the enrollee to be collected.

It will be important to measure fraud reduction resulting from the use of a mobile phone vs. other payment methods to see how much mobile helped to reduce fraud. This may be difficult to do if companies are not willing to be transparent and share their fraud numbers and costs. Bank and other trade associations such as the ABA and AFP collect fraud data from surveys. The CTIA has a voluntary requirement for its members to complete an annual survey and report anonymously so perhaps they could help collect mobile fraud data through a survey.

With proper changes in regulations, this broader set of data has the potential to be shared within the mobile ecosystem. Full NFC implementations, augmented by encryption that works with the secure elements embedded in the phone, make superior payment account and user ID protections readily available. Ultimately, this benefit can result in both lower PCI compliance costs and lower fraud losses.

The MPIW can help maximize the opportunities for overall fraud reduction by working with the players to develop and implement fraud reduction standards for the entire environment that avoid the possibility of the network safety relying on the lowest common denominator. In addition, the group can work with the other parties to enforce standards and pursue bad actors.

Merchant cost efficiency

The one-time cost of conversion to mobile payments may be viewed as a barrier (as described in the next section), but the ongoing and future benefits may be substantial. For example, mobile may provide an opportunity for merchants to reduce PCI inspection costs over time,[17] and reduce the costs and risks of storing sensitive data, as mag-stripe data exposure is eliminated. Short-term or one-time costs, including costs arising from merchant liability to issuers for accounts compromised from data breaches (in a mag-stripe/open-credential paradigm), are projected by some merchants to exceed the actual costs of fraud in the future if the industry stays with a mag-stripe standard. Many large merchants acting unilaterally are adamant about ensuring consumer payment choice, and appear to be prepared to support a number of alternative payment systems that take advantage of mobile and contactless capabilities. This includes advanced commitments and investments by merchants in chip+PIN for both offline and online transacting, which signals a growing understanding of the long-term business requirements.

Lower issuer costs

In the mobile payments environment, card issuance costs can be reduced by electronic downloads replacing expensive physical card distribution programs over the long-term. However, plastic cards are expected to co-exist with mobile phone payment options for several years, which will impact cost savings. And, current VISA and MasterCard rules require issuing of cards along with mobile accounts, so customers will carry cards and phones for a few more years. Costs to access TSMs and secure elements, uncertain at this time, must also be factored in. However, customer validation and activation can be simplified through more efficient, fully digital, and more secure (through the Global Platform standard) payment account provisioning, set-up and maintenance via the mobile channel. This would, in time, offset costs associated with phasing out mag-stripe cards. Loading cards to the mobile wallet will be less risky. Lost phones can be secured and remotely deactivated in ways that cards, wallets and purses cannot be, and there is evidence that consumers are much more attentive to the status of their phones. (Industry research states that it takes a consumer 4-8 hours to realize he lost his wallet, but only one hour to realize his phone is lost.) This can reduce fraud from lost payment accounts and make restoration of payment capabilities much faster and easier.

[17] See Visa Europe announcement at 'Hhttp://usa.visa.com/download/merchants/bulletin-tip-020911.pdfH.'

Data privacy

The mobile channel can give a consumer the ability to opt-in or -out of applications and services offered by sellers and advertisers on a timely, case-by-case basis to control and limit access to private information. This requires the mobile channel to have effective and efficient regulatory check-points and roadmaps to ensure that the consumer has sufficient protections. Mobile can also have the broader benefit of triggering a proactive national agenda to drive toward consumer protections that lend themselves to individual preferences, versus universal blocks or hurdles that waste expense and effort to disable when circumstances warrant. Once again, standards developed collaboratively and orchestrated by a central party can enhance the data privacy process.

International compatibility with a chip+PIN standard

Implementing the international chip+PIN standard (or some yet to be defined alternative) generates additional benefits for the NFC mobile phone by making mobile transactions more fraud resistant. Ongoing mobile EMV pilots in Europe demonstrate continued evolution toward that end. Considering a near-term deployment of contactless chip+PIN mobile in the U.S. allows us to anticipate change and move in lock step with the rest of the world.

Economies of scale and cross selling

Mobile NFC technology is also being considered in non-payment and non-banking venues, such as transit and health care. As a result, investments in mobile payment technology may be shared over time, creating better economies of scale that will drive down the cost of future mobile solutions. The convenience and efficiency of the tap-and-go format can support many other applications that provide value-added services. Examples include high volume, high speed ticketing in transit venues; tap-and-go for parking meters, parking lots, and vending machines, and a variety of health care applications (e.g. making integrated, approved and authenticated purchases of medical products and services for insurance-defined accounts like Flexible Spending and Health Saving Accounts). Integrating rewards programs (from banks, merchants and third parties) can efficiently and effectively be orchestrated via mobile NFC wallets and applications as well—potentially increasing ROI for those programs.

Consumer convenience, security and efficiency

Surveys continue to show that consumers want to save time. Tap-and-go payment schemes can overcome the limitations and inefficiencies of 'self-checkout' and turn it into a sought-after mode of transacting, particularly when coupled with emerging shopping applications where the phone is used as a scanning device and barcode reader. Education programs can help consumers and small businesses understand that mobile technology has the potential to provide an even safer environment than exists today if implemented correctly. Consumers also want payment choice, and if possible, ways to consolidate all the cards in their physical wallets.

Increased relevance of marketing, promotions and advertising

The current one-way, one-size fits all broadcast-mode of buyer-seller interaction can be replaced with one-to-one, integrated communications and location-aware, real-time capabilities of mobile transacting. Services will need to be somewhat customized to reach different consumer demographics, since digitally oriented younger adults are more willing to opt-in to highly personalized services and commercial interactions, while older adults may avoid them. Recognizing that there are existing marketing regulations, use of the mobile channel for more extensive marketing may create gaps. Therefore, developing a regulatory roadmap will ensure that the industry invests wisely and appropriately to develop services that work in the interests of buyers and sellers without jeopardizing consumer protections. A properly guided mobile marketing, promotion, and advertising environment may create efficiencies and improvement in relevance, and convert wasted costs and investments into profitable new transaction streams that benefit participants in the mobile ecosystem.

VII. Obstacles to Implementation[18]

Despite the exciting business prospects and other benefits of transacting payments by mobile phone, there remains a significant amount of skepticism about how necessary, and how affordable, the transition to mobile NFC payments and, logically, their extension to EMV or similar standards, will actually be. The convergence of several major changes in the payments environment might finally be wearing down this traditional reluctance to change the status quo. Ironically, the unexpected attraction to mobile NFC increasingly appears to be the catalyst to finally moving from the mag-stripe paradigm to a payment system more fitting to today's digital economy and lifestyle. How and why this is happening makes a great study in consumer preferences and technology transformations.

At least four obstacles to implementation of a mobile NFC payment option with the breadth of impact thought by some to change the entire payments paradigm must be addressed and resolved:

- Cost of deployment
- Lack of adoption for contactless with cards
- Disruptive changes in the status quo for existing payments parties
- New revenue models and how to fund the changes necessary to create the mobile ecosystem

[18] See *Appendix III* for Steve Mott's perspective of contrasting views on what motivates participants in the U.S. mobile payment ecosystem.

Cost of deployment

The biggest obstacle to any transformation is the cost of the change. Upgrading the existing payments infrastructure from mag-stripe to smart cards and PINs has long been resisted by both FIs and merchants due to the apparent lack of a business case for the necessary investment. However, there is a growing sentiment that the conventional 'wisdom' about chip+PIN might have changed due to the need for global interoperability, as well as increased interest in moving to contactless payments on mobile phones.

One key factor about the lack of justification for shifting to chip+PIN might be the realization that the costs of PCI compliance (and clinging to mag-stripe) could soon exceed the costs of actual fraud. Ironically, merchants, who bear most of the costs of attempting to comply with these card credential protections, and who are increasingly exposed to financial liabilities to compensate issuers for mag-stripe fraud from data breaches, would pay more to avert mag-stripe fraud than issuers experience from the fraud itself. So, *any* substantive innovation in payments seems likely to devolve quickly from whether to replace mag-stripe to what technology to replace it with and how fast. Mobile NFC advocates make the case that their technology can facilitate this transition in a number of ways, and may prevent the need for a substantial build-out for chip+PIN contact cards in the process for the U.S.

Contactless advocates, including most big merchants, some of whom have already deployed terminal systems capable of supporting contactless chip+PIN technology, argue that the rest of the world is making steady progress moving to contactless. However, because of the overlap between the card world and mobile payments, some mobile stakeholders believe that it will be necessary to support both contact and contactless options in cards for some time, which if the market proceeds in that direction, will be more expensive.

Slow market adoption of contactless to-date

Why should the U.S. also consider moving to NFC on mobile phones when the first generation of contactless has by some accounts been a disappointment?[19] Three reasons stand out for the apparent slowness in consumer adoption. First, consumers don't really have an incentive to try or use contactless, vis-à-vis their other, familiar payment modes. With respect to more than half the cards issued, consumers aren't aware they can *do* contactless. Additionally, it is difficult for consumers to figure out which merchants accept this format. Finally, banks have done little in the way of promotion, and have done a poor job of explaining to consumers that they will be *safer* with contactless.

[19] In the marketplace since 2004 with an estimated 70 million cards and fobs available for use in 150,000 merchant locations, but too few transactions to report so far.

The concept of mobile NFC is thought by many to address these constraints to consumer adoption by being fun to use, accessible to almost anyone with a mobile phone, and supportive (if the payment 'wallet' is open) of a multitude of payment choices, including prepaid for the un- or under-banked. Mobile devices can offer *added* security by providing more information to augment verification and integration of 'full' NFC, where the radio-wave chip and antenna enable the NFC application to interface with the secure element in the device's chipset. Two-way NFC capabilities may also offer another way for consumers to receive and redeem offers, promotions and coupons from merchants and third-parties—including many innovative exchanges based on location-awareness of mobile devices.[20]

The card networks primed the pump for merchant adoption of first-generation contactless payments, subsidizing the costs and deployment of several hundred thousand terminals, largely in the expectation that contactless would prove faster at checkout, cleaner to handle and therefore a good alternative to cash payments at the counter. But for the most part, the only payment options available are signature-based credit and/or debit, replacing cash transactions that typically cost less than a nickel to process with a signature-card transaction that costs $.15 to $.75 or more. This has not incented merchant support (such as prompting and assisting consumers to try the mechanism out). Additionally, merchants want to see equipment that looks the same and doesn't require retraining staff. Mobile stakeholders must work harder to identify a compelling need for merchants to accept contactless payments.

It is worth noting that as of February, 2011, industry estimates indicated there were 70 million contactless devices (mostly cards) and 150,000 contactless merchant terminals in the U.S. Despite the obstacles, this evolution of contactless cards at POS has been valuable, preparing and providing the industry with the experience needed to move to the next phase of contactless payments with mobile phones.

Merchants, from a variety of recent reports and publications, appear to have high expectations for the coming transformation in the payments environment. In particular, they are pushing for more payment choices with contactless, and pricing that better reflects the common view that mobile contactless—by virtue of being capable of greater safety and efficiency—should cost less than problem-prone mag-stripe payments. In the new consciousness of the raft of recent consumer-protection and merchant-assisting legislation, lower costs should be reflected in more advantageous pricing to merchants and lower purchase prices to consumers.

The NFC deployment configuration supports this new perspective by making an open payment wallet possible; even merchant-provided payment options (e.g., private label, store-card based, stored value) could be offered. That gives the consumer a full set of payment choices, and the possibility of enjoying automated rewards and loyalty benefits managed by the NFC/chip interaction.

[20] It is expected that offers, promotions, and coupons will also be distributed over mobile data channels.

The big inducement for merchants with mobile NFC contactless goes beyond the basic payment transaction. Two-way communications between the customer and the merchant enable more value-added innovations such as location-aware prompting to visit a store; identification of the consumer upon entering the store (to receive customized offers and promotions); facilitation of product promotions and coupon exchanges while shopping; and even a faster and more convenient self-checkout. And while it is fair to speculate that the mobile NFC version of contactless will engender much more merchant support, it is not possible at this time to estimate the revenue benefits associated with this concept.

Mobile NFC also enables the marketplace to bypass an aging, interim technology deployment (EMV contact cards) and focus investment resources on where the market appears to be headed in the future. This opportunity to save money and time should enable the new, mobile payments 'ecosystem' to build out a robust and efficient infrastructure that can benefit all parties.

Ingrained Consumer and Merchant Payment Habits

Perhaps the greatest barrier to change in the U.S. payments system over the past thirty years has been the consumer's comfort with the status quo. Check usage has just begun to decline over the past decade and even then at a reluctant pace. It took a decade to get consumers to utilize ATMs in meaningful numbers. POS systems were technically feasible in the early 1970s, but did not come into meaningful use for two decades. A significant number of beneficiaries still do not select direct deposit of government benefit payments and legislation may be required to achieve the last mile of change.

Merchants have understandably geared their changes to respond to consumer demand, not lead it. The cost of investments in new technology at the point-of-sale and the need to retrain staff to use new technology are clear deterrents to unnecessary change. These forces also tend to maintain the status quo.

Further, in the face of stiff competition, the banking industry has moved over the years to giving away most services (with the exception of credit carrying fees), offering them free of charge to the consumer; and focusing instead on charging for exceptions. Such practices have become a comfortable norm, making it difficult to use pricing as an incentive or disincentive to evoke change.

Finally, over the last fifty years, new payments options have been developed, but virtually no options have been eliminated. The consequence of this approach is inefficiency as a wide range of payment solutions continue to be supported, and even enhanced at the margin, despite apparent inefficiency.

Faced with these existing norms, consumers and businesses don't have a compelling need for changes in payment methods. Similarly, financial institutions faced with many competing investment opportunities in the wake of the economic crisis are not actively pushing change. As a result, progress in realizing a ubiquitous mobile payments ecosystem in the U.S. is likely to be relatively slow unless a

paradigm shift occurs in a key variable, such as fraud experience or regulatory change, or development of a truly new functionality that does not exist in current payment methods.

Revenue Uncertainties

Regulatory impacts are cutting away at many sources of card revenue and the market practices that make this revenue possible. Therefore, it is natural for the conventional payment industry providers to be concerned about the need to make incremental investments in a market in which timing of benefits is unknown, and about the uncertainty over whether they will be able to achieve the same position in the new payments paradigm that they had in the old, given the pressure on fees and the onslaught of new, non-bank competition.

Convergence of the wireless and banking sectors creates another perceived threat to revenue stability. It is assumed that both carriers and banks believe they own the mobile payments customer, provide the bulk of the value for mobile payments, and are attracted by the possibilities of increasing revenues related to transacting over phones. There is, at least, the potential for rivalries between the two powerful industries and many calls for cooperation in order to produce an efficient payment capability with fair compensation and return on investment for building out the necessary infrastructure.

Merchants, however, appear to be adamant about not wanting *two* big contenders in the payments 'food chain.' Instead, they point out that mobile payments ought to be safer and more efficient with the combination of both sources of data and network security from both industries, and that this lower risk and cost should be reflected in more attractive pricing *for the merchants.* Merchants propose a shift from the prevailing view that payment fees should constitute the financial foundation for a mobile transaction system, to a new perspective that payment capabilities might establish the *basis* for a new payment paradigm infrastructure, but not be the primary revenue model per se.[21]

Many of the participants in the old and the new payments ecosystem have expressed support for the development of a visionary infrastructure and a regulatory roadmap to help chart out what infrastructure, market practices and technology requirements can be expected and approved so that they can make the incremental investments needed that will be justified by viable business cases that are exposed to no surprises or undue risks.

Reaching such collaborative and enlightened cooperation will be a substantial challenge and might require a steady, sure hand from regulators from both the banking and the wireless industries to ensure an even playing field. Moreover, it is important to reach a quick consensus on what is required, and what

[21] National Retail Federation. 2011. "Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape," January. The blueprint describes new ways for buyers and sellers to interact more efficiently and more gratifyingly with mobile NFC—setting the stage for revenue models based on mobile marketing, promotions, and advertising.

should be shared and non-competitive in the infrastructure, in order to develop and approve cross-industry standards to make certain the new, mobile digital payment system for the 21st century is even more reliable, ubiquitous, and robust than the one it will be replacing.

VIII. Conclusion

This document is a work product stemming from the discussions of a Mobile Payments Industry Workgroup that was organized and convened by the payments research teams at the Federal Reserve Banks of Boston and Atlanta. While the ideas expressed in this document about a future success path for mobile payments in the U.S. are not directly attributable to any single member, they do represent a shared view of the participants about a way forward. Yet, even as the group met over a fifteen month period, many participants engaged in formative, independent partnership efforts to announce pilot initiatives to begin the exploration of mobile payments opportunities in this country. In many cases, the underlying concepts of these pilots are consistent with the vision expressed in Sections IV and V of this document; in other cases they are not. But, in all cases these independent efforts signal an appetite to pursue mobile payments as an important future strategy for payments efficiency, security, and convenience.

In essence, the concepts expressed in this paper represent a good entry point into the evolving mobile space that could create a more sustainable and efficient ecosystem through collaboration and sharing wherever possible. Group members ultimately thought that this could be a better way of doing business- agreeing early in the process on ways to build a highly ubiquitous and interoperable ecosystem model, while still competing fiercely on customer facing products and services. Moreover, by collaborating on key issues such as standards and rules of engagement, the sense was that the U.S. would be better positioned to be a part of a global mobile payments system that recognizes the flexibility and mobility of the phone as a payments instrument.

In other countries where mobile has emerged more rapidly, a central body from government, or one sponsored collectively by key private sector stakeholders, has helped organize and direct collaborative solutions. In some small way, the facilitating efforts of the two Reserve Banks noted above represents a microcosm of the benefits of having a central entity with no apparent “skin in the game” work with industry leaders to advance discussions. By providing administrative and thought leadership, the convening Reserve Banks were able to maintain a level of momentum that has resulted in this work product being developed in what, by industry standards, is a relatively short period of time. More importantly, though, the organizations that participated as members of this work group remained engaged throughout, while clearly expressing their independent views on very difficult key issues. Many of the

participants were meeting face to face for the first time and consequently the group went through a "getting to know you" period that eventually led to a willingness to share more openly for the benefit of a long term outcome desired by all. The need to establish a more enduring collaborative industry body is a decision that lies ahead, following a period of industry experimentation. Similarly, the benefits of establishing a cohesive industry roadmap for the future are yet to be determined, based upon the future identification of meaningful barriers to progress.

Ultimately, the value of this workgroup's efforts will be measured by what happens next. Clearly, there are many more parties who will need to support the ideas set forth in this document, including the benefits of a central coordinating entity to work on behalf of all parties to create a roadmap for the future. Forums for engaging these parties may need to be established. This can only be achieved through broad circulation of the ideas in this paper and a decision by significant market leaders to foster further collaborative work. Existing industry trade groups and membership organizations will need to be an important part of this process. While there are notable precedents of success with such collaborative endeavors in the U.S. and overseas, there is also a long list of initiatives that ultimately failed because parties did not see the tradeoffs of independence and collaboration as beneficial. In many of these occasions, the underlying concepts never came to market or never achieved maturity because the obstacles to success could not be removed through independent efforts.

Yet, the opportunities and benefits of doing business differently with mobile payments in this country seem significant and the obstacles to success do seem daunting. Working together to pursue a common high level vision does appear to promise lesser investments over time by all parties and more rapid accrual of benefits than other options. Moreover, through enlightened collaboration, we all might benefit from the perceived view that if we get mobile payments right, it can be the entrée point to making other financial transaction services safer and more efficient. Beyond that, figuring out how to master fully flexible, digital and real-time transacting in payments and banking services might generate ways to bring more security and efficiency to other transactional domains, such as health care, government licensing, and even voting.

APPENDICES

I. Glossary of Mobile Terms

II. Cost of Converting to EMV in the U.S.

III. Elements of a Mobile Payments Business Case

IV. Mobile Payments Standards in the U.S.

APPENDIX I - Glossary of Mobile Terms

Term	Description
APRU (Average Revenue per User)	• Commonly used financial benchmark measuring the average monthly revenue per mobile subscriber
CDMA (Code Division Multiple Access)	• Technology for digital transmission in which multiple frequencies are used simultaneously with each user having a unique code • Each group of users has a shared code and only users associated with that code can understand each other • Used to send voice, data, and signaling data (such as dialed telephone number) between mobile phones and cell sites • Used in several countries including the U.S. and S. Korea
Contactless Card/Device	• Use of either radio frequency (RF) or infrared technology to allow a payment card or mobile device and the POS terminal to communicate or transact without physical contact • Contactless technology is popular with mass transit, road toll and physical security access applications which require fast transaction speeds. • Consumer holds the contactless card, device or mobile phone in close proximity (2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly via radio frequency (RF)
Cryptogram	• A numeric value that is the result of data elements entered into an algorithm and then encrypted; commonly used to validate data integrity.
DDA (Dynamic Data Authentication)	• Protects cardholder and other payments data by making each mobile payment transaction unique. A valid cryptogram is generated for each transaction, which is then verified when the transaction is authorized. The cryptographic value, including transaction-specific data elements, is validated through the terminal with the network to protect against fraud and skimming. The chip device (card or phone) must be present to generate a valid cryptogram, which is verified online or offline when the transaction is authorized.
Downloadable Mobile	• Program residing on a mobile device

Application	• May be pre-installed by the MNO or handset manufacture but usually downloaded by the end-user, either via MNO or FI, or directly from the mobile phone store
EMV – Europay, MasterCard, Visa Specifications (EMV)	• Technical specifications and standards developed jointly by Europay International, MasterCard International and Visa International outlining the interaction between IC (integrated circuit) chip cards and terminals to ensure global interoperability • Standard for interoperation of IC (chip) cards and IC capable POS terminals and ATMs to authenticate credit and debit card payments • Purpose of EMV standard is to allow secure interoperation between EMV compliant IC cards and EMV compliant credit card payment terminals globally • EMV based credit card payment systems improve security (with associated fraud reduction), and the possibility for better control of 'offline' credit card transaction approvals • IC card systems based on EMV are known also as chip and pin
GSM (Global System for Mobile Communication)	• The most widely used digital standard for mobile or telephony • Open, digital cellular technology used to transmit mobile voice and data services • Has international roaming capability, allowing users to access the same services when travelling abroad as at home in over 210 countries
ISO 7816	• ISO standard for chip cards with contacts. The EMV standards are built on ISO 7816.
ISO 14443	• ISO standard for contactless chip cards • ISO 14443 defines two types of contactless standards: Type A (Philips Mifare) and Type B (Motorola) • Type C (Sony) is also widely used in Asia Pacific, but not yet formally adopted by ISO
ISO 18092	• ISO standard for NFC
MMS (Multimedia Messaging Service)	• Standard for mobile messaging systems that enables message to include multimedia objects such as images, audio, video, and rich text as well as plain text in SMS
Mobile Banking	• Access to bank information such as account balances and recent transactions via a mobile device

	• Includes informational and transactional services, including bill pay, funds transfers, alerts
Mobile Bill Pay	• Ability to set up and pay for various bills via a mobile device • Mobile bills could be paid through mobile banking or through a third party or mobile operator
Mobile Ecosystem	• A complex set of interconnected entities and relationships which interact to form a stable functioning payments system • Ecosystem includes all payment system participants in the mobile payments environment, including financial institutions, money service providers, handset makers, technology service providers, mobile network operators, merchants and consumers, etc.
Mobile Marketing	• Provision of advertising for mobile transaction services
Mobile Payment	• Payment initiated from a mobile device. Mobile phone is involved in the initiation and/or confirmation of the payment • Payer may or may not be 'mobile' or 'on the move' • Mobile phone facilitates payment between the two entities in a C2B payment
Mobile Parking (m-parking)	• Type of m-payment • Ability to pay for car parking using a mobile device, typically via text messaging or possibly with a downloadable application
Mobile Commerce	• Purchase of digital content such as ringtones and music, or physical goods in the same way a consumer would purchase over the internet • Analogous to an e-commerce transaction
Mobile Coupon	• Token, typically issued as a marketing or sales promotion, that can be redeemed at a participating physical or digital merchant • Typically an incentive in the form of a discount on purchase goods • Can be considered a subset of m-marketing, although the coupon itself may represent a cash value and may therefore be more directly transactional
Mobile RDC	• Use of camera-equipped mobile phones for check image capture as a stand-alone application or as part of a broader mobile banking solution

Mobile Remittances	• P2P mobile transaction that crosses national borders
Mobile P2P	• Person-to-person mobile payments • Transfer of funds from one individual to another via a mobile device within the borders of a specific country • Uses SMS to send text messages with payment instructions to third parties, such as the bank accounts of customers, suppliers, or family members • P2P payments very popular in developing countries through service providers such as M-Pesa in Kenya and Smart Communications in the Philippines
Mobile Ticketing	• Ability to pay for , load and store mass transit tickets electronically on a mobile device
Mobile Top-up	• Transferring funds from a funding source (bank account, credit card, etc.) to top-up minutes on a prepaid mobile account • Minutes may be used as an equivalent for cash, allowing the mobile account to become a stored value 'wallet'
Mobile Wallet	• Software application loaded onto a mobile phone to manage payments made from the mobile phone • Can centrally and simultaneously store multiple applications managing customer account/transaction information with financial providers, public transit agencies, or third part entities such as health clubs, schools, and office or apartment buildings • Can also be used to hold and control a number of other applications (for example, payment and loyalty), in much the same way as a physical wallet holds a collection of physical cards • On-device storage technology allowing for the controlled and secure partitioning of information such as payment cards, coupons, mass transit tickets and medical information
Mobile Web	• Version of internet created to be accessed on mobile phones. Also know as mobile internet.
MNO (Mobile Network Operator	• Also known as mobile carrier, the telecommunications business that provides mobile phone service to end-users • Has its own frequency allocation of the radio spectrum • Has the required infrastructure required to provide mobile phone service
MVNO (Mobile Virtual Network Operator)	• Business that provides mobile phone service but does not have its own frequency allocation of radio spectrum or all of the infrastructure required to provide mobile phone service
Mobile originated SMS billing	• Payment method via SMS where the payee originates the payment by sending an SMS text message to the customer

Mobile terminated SMS billing	• Payment method via SMS where the intended payee closes the payment by receiving one or more SMS messages
NFC (Near Field Communications)	• Wireless technology enabling communication between devices over a short distance • Used in mobile POS payments solutions • Short range, high frequency, standards based wireless communication technology which enables the exchange of data between devices in close proximity (less than two to four inches distance) • An extension of ISO 14443 RFID proximity-card standard that combines the interface of a smartcard and a reader into a single device • Communication occurs when two NFC-compatible devices are brought within four centimeters of one another • NFC can operate in one of two modes: passive or active • NFC contactless transactions clear over existing credit card or bank payment networks, not over wireless networks • Because transmission range is so short, NFC-enabled transactions are inherently secure
NFC Sticker	• A token containing RFID technology, allowing for the transfer of information between the token/sticker and the reciprocal contactless reader (e.g. mass transit access gate, contactless POS terminal, etc.)
OTA (Over-the-air provisioning)	• Transportation of messages wirelessly and without landline • Method of distributing new software updates to mobile phones or provisioning handsets with the necessary settings with which to access services such as MMS or WAP
POS (Point of Sale)	• Location where a transaction occurs, which is usually a retail store or similar venue, including public transportation, taxi cabs, restaurants, etc. • Equipment used by the merchant to complete the payment transaction
Premium SMS	• An SMS message for which the sender pays a higher fee than normal to cover the expenses for a good or service delivered
Proximity mobile payment	• Payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity to the merchant's POS equipment

Remote mobile payment	• Payment initiated from a mobile phone to a recipient (person or device) where the recipient is not in the immediate area
RFID (Radio Frequency Identification)	• Automatic identification method that relies on storing and remotely retrieving data using devices call RFID tags or transponders • An RFID tag can be attached to or incorporated into an object to identify using radio waves • RFID tag contains an IC (integrated circuit) to store and process information and an antenna to receive and transmit the RF signal between devices (e.g. mobile device and a POS reader)
SD Memory Card /micro SD chip	• Secure digital memory card for removable memory in mobile devices • Used as a means of adding additional memory • Micro SD chip is a much smaller version of the SD memory card, which is now being used as a bridge to add contactless memory to mobile devices not equipped with means to interface with contactless POS terminals via RFIC and perform lightweight implementations of NFC transactions
Secure Element	• Platform where applications can be installed, personalized and managed, preferably over-the-air • Combination of hardware, software, interfaces and protocols that enable secure storage and use of credentials for payment, authentication and other services • Location of the security components, including confidential information, within the mobile phone • Location can be the SIM, a separate secure chip in the phone, or an external plug-in card
Short code	• Special shortened telephone numbers used mainly to address SMS and MMS messages from mobile phones • Widely used for such things as TV voting, ordering ringtones, charity donations, requesting product information, and mobile services such as SMS search services • Also known as short numbers or Common Short Codes (CSC)
SIM (Subscriber Identity Module)	• Removable smart card within a GSM mobile phone • Securely stores the service-subscriber key (mobile user account) used to identify a mobile phone to the network • Configured with information essential to authenticating a GSM mobile phone, allowing a phone to receive service whenever the phone is within coverage of a suitable network • SIM card allows users to change phones by removing the SIM card from one mobile phone and inserting it into another mobile

	phone • SIM card can be partitioned to store multiple forms of data • Can be used to host applications such as mobile banking applications
SMS (Short Message Service)	• Service for sending messages of up to 160 characters to mobile phones • Communications protocol allowing the interchange of short text messages between mobile phone devices
TSM (Trusted Service Manager)	• Neutral trusted third party intermediary or service provider that manages downloads of applications to mobile wallets • Securely distributes and manages contactless services for the application service providers' customers using the MNO networks • Provides a single integration point to all mobile operators for financial institutions, transit authorities and retailers that want to provide a payment, ticketing or loyalty application to their customers with NFC-enabled mobile phones • Owner/manager of the master key that controls the Secure Element platform. This allows the TSM to control and authorize service providers to install applications on the SE • Provides services to manage the secure download and life-cycle management of the mobile NFC applications for the FIs, transit authorities and retailers • Does not participate in any contactless transactions using NFC devices • Key functions include interconnecting with MNOs and application service providers; enrolling new customers; updating user interfaces; managing customer databases; managing application lifecycles; managing value-added service such as ticket reloading; and guaranteeing end-to-end security
2D Barcode	A 2D (two-dimensional) barcode is a graphical image that stores information both horizontally -- as one-dimensional bar codes do -- and vertically. As a result, 2D codes can store up to 7,089 characters, significantly more than the 20-character capacity of a one-dimensional barcode. 2D barcodes enable fast data access and often used in conjunction with smart phones. The user photographs a 2D barcode with the camera on a phone equipped with a barcode reader. The reader interprets the encoded URL, which directs the browser to the relevant information on a Web site. This capability has made 2D barcodes useful for mobile marketing.

UICC (Universal Integrated Circuit Card)	• Chip card used in mobile terminals in GSM and UMTS networks • Ensures the integrity and security of all kinds of personal data • Typically holds a few hundred kilobytes
UMTS (Universal Mobile Telecommunications System)	• A third generation (3G) cell phone technology using CDMA as its underlying air interface
USSD (Unstructured Supplementary Service Data)	• Messaging technology unique to GSM phones • In contrast to SMS, which is a store-and-forward delivery system, USSD provides a continuous online session • Associated with a real-time or instant messaging type phone service • Response times are generally quicker than those used for SMS • It is a popular platform for mobile banking in South Africa
WAP (Wireless Application Protocol)	• Open international standard for applications that use wireless communication • Principal application is to enable access to the internet from a mobile device
WAP Browser	• Provides the basic services of a computer based web browser but simplified to operate within the limitations of the mobile phone • Program on mobile device that facilitates access to the mobile or 'real' internet from the mobile device • Commonly used web browser for small mobile devices such as cell phones.

APPENDIX II - Cost of Converting to EMV in the U.S.

In 1998, the Tower Group conducted a detailed study of the cost of converting to EMV *contact* cards.[22] The total costs—most of which would have to occur at and with the POS systems—were calculated to be $12.8 billion. That year, total bankcard fraud, as affecting the banks, was estimated to be less than $1 billion—about a nickel per $100. So it was difficult to make a business case on those numbers.

Yet the rest of the world was proceeding apace with planning deployment of EMV chip+PIN specs, which Europay (now a part of MasterCard), MasterCard, and Visa had developed and contributed as a global standard just a few years before. The specification provided for interoperability and synonymous security for encrypted chip card and PIN credit, debit and stored value payments.

Europe was experiencing much higher rates of fraud than the U.S. due to the lack of ubiquitous and cost-effective telecommunications infrastructure needed to conduct reliable and fast real-time authorizations. The U.S., on the other hand, enjoyed the world's best communications infrastructure. But there was still a lingering realization that eventually, if the rest of the world went to EMV chip+PIN, and the U.S. stayed with mag-stripe, payments fraud would migrate to the U.S., and U.S. travelers and merchants would be disadvantaged by not being able to transact with smart cards. At one point, Visa and MasterCard even proposed mandating the use of chip cards by 2005; that mandate never materialized.

By 2001, Tower Group re-checked its study on switchover costs to chip+PIN.[23] This time the total was $13.4 billion. Merchant costs—adding in the need to accommodate the fast-growing online market—were projected to be three-fourths of the costs (bank authorization system upgrades accounted for 17% and bank network upgrades another 8%). Once again, there was no compelling business case.

Fast-forward to late 2009, when the Smart Card Alliance estimated total U.S. card fraud losses in 2007 at a still-modest $1.7 billion, but indicated that total fraud was dramatically underreported, citing an estimate by the Mercator Advisory Group that adding in all merchant costs and the associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses, the total cost might be more like $16 billion, much of which was borne by merchants.[24] A Kansas City Federal Reserve paper, written by Rick Sullivan in 2010, estimated payment card fraud of about $3.7 billion (using 2006 data), adding in the often unreported merchant costs![25]

---

[22] Tower Group. 1998. "Smart Cards in the U.S.: An Infrastructure Cost Analysis," June.
[23] Iacobuzio, Theodore. 2001. "Smart Cards in the U.S.: An Infrastructure Cost Analysis (Redux)," Tower Group, February.
[24] SmartCard Alliance. 2009. "Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud," October.
[25] Sullivan, Richard J. 2010. "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Federal Reserve Bank of Kansas City, *Economic Review*, Second Quarter, pp. 101-132.

Importantly, the Alliance warned that retention of the mag-stripe on cards and POS readers would begin to dilute the fraud reduction benefits for countries that deployed EMV chip+PIN. Moreover, the growing dangers of data breaches, with big surges in compromised mag-stripe credentialed accounts, would inevitably require something other than a 'do-nothing' response.

In 2010, Javelin Strategy & Research echoed these concerns with their updated estimate of the cost of converting to chip-based contact cards (perhaps EMV, perhaps not) at $8.6 billion.[26] One of the lingering deployment cost factors remains deployment of PIN-pads and terminals to cover the estimated 60-70% of retail, card-accepting locations that don't have them yet. In the Javelin report, part of the motivation for moving to chip cards has now become the need for a true end-to-end encryption solution to data breach generated fraud and the growing costs and specter of PCI compliance. For example, by mid-2010, estimates to upgrade existing merchant locations that already process PIN-debit to comply with new PCI requirements might cost upwards of $20,000 per store.

The most important argument for EMV contactless is that it could be materially cheaper to implement than contact cards. For example, in the convenience store industry, two-thirds of the outlets pump gas. The average store incurs an average of $700 of card fraud per year. PCI compliance costs $1600 annually—making that a stretch for business case justification all by itself. Outfitting the pumps with remote smart-card/PIN readers would cost an estimated $50-60,000 per store/gas station.[27] With some 8% of retail sales in this retail vertical, EMV contact cards represent a huge hurdle. But contactless phones, communicating to inside the store via a Wi-Fi hotspot, could wind up costing less than $5000 per store.

Some estimates suggest that EMV contactless could cost merchants as little as half the expense of deploying contact card readers (although banks and networks would likely experience little change in their conversion costs). However, to accommodate foreign travelers coming to the U.S. with EMV contact cards, a reasonable number of ATMs, travel venues, entertainment centers and food service facilities likely would need to accept the contact version, and U.S. issuers would still have to issue contact cards to U.S. travelers abroad.

[26] Javelin Strategy & Research. 2010. "End-to-end Encryption, Tokenization and EMV in the U.S.," January.
[27] National Association of Convenience Stores estimate. 2010.

APPENDIX III - Elements of a Mobile Payments Business Case, *by Steve Mott*[28]

Changing the way people pay is difficult enough in any era, given the stability, predictability and fiercely preserved status quo the U.S. card payments system has achieved over the past half-century. By introducing technology (two-way NFC mobile handsets with chip-based security) that departs from the plastic card paradigm and can simultaneously become a catalyst for elimination of the magnetic-stripe infrastructure, the embryonic mobile 'ecosystem' discussed here is propelling an unprecedented disruption in business models—one that has old and new payments providers scrambling to come up with viable business cases.

The contention between old and new, legacy and future, and conventional versus value-added depicts the divergent interests of the mobile ecosystem as the participants jockey for position. Fundamentally, this is a $300 billion industry[29] in which many established companies such as Visa, MasterCard, their big bank members, Amex, Discover, processors like First Data, Global Payments and TSYS, equipment manufacturers, and thousands of Independent Sales Organizations (ISOs), and many others (including consulting companies, law firms, and industry organizations) have profited substantially for decades.

New entrants, which include non-traditional payments companies with considerable presence such as PayPal, Intuit, Apple, and Google in addition to the giant wireless carriers (ATT, Verizon, T-Mobile and Sprint) and the handset manufacturers and application providers, are moving concertedly into the space with new technology innovations and business models. Consumers—especially smart phone users—appear to have put themselves up for grabs, constantly pushing and testing the borders of the walled garden of payments. And merchants, which have moved to the forefront of the discussion due to their singular role in deciding which of these innovations for mobile checkout at POS to embrace, are wielding unprecedented influence in both political and economic elements of this transformation.

Such robust participation suggests the dawning of a new 'payments' ecosystem, from which many more 'parties' will contend for portions of the emerging new revenue models for mobile transacting. If the new paradigm is chip-based contact cards, as many expect, the infrastructure replacement cost could easily be in the $8-12 billion range—75% of which would logically be borne by merchants in terminal upgrades.[30]

One of the lingering deployment cost factors remains deployment of PIN-pads and terminals to cover the estimated 60-70% of retail, card-accepting locations that don't have them yet. Online deployment of PINs is viewed as much easier, with most of the EFT networks and several of the big

[28] This section is adapted from a series of articles written by Steve Mott, Principal, BetterBuyDesign, 2009-2010.
[29] McKinsey & Co. 2009. "Payments Industry Roadmap."
[30] Javelin Strategy & Research, 2010.

processors now adopting software-encrypted PIN-debit capabilities. No additional infrastructure is needed by consumers, merchants or issuers in order to process these transactions over the internet.

Perhaps for the first time in this country's conversion to electronic payments, the sustaining business case appears unlikely to be made principally on garnering new transaction fees or reducing payment processing costs. Rather, it will likely be made by wholly different cost avoidance and revenue drivers altogether. And several external influences are converging to suggest that the new ecosystem will be driven far more by new revenue drivers than 'tolls' for doing payments.

What follows is a general discussion of the elements to a business case, as well as an assessment of the potentially important business case ingredients for the major players in the ecosystem. At this time, it is very difficult to place meaningful estimates on the potential value of each business case element. This will become more possible over time as various pilots are performed, new regulations are finalized, and new technology is unveiled. However, it is important to recognize that the factors discussed below be evaluated as part of a holistic business case assessment both by individual firms and, perhaps, by industry overseers as part of an effort to understand any public policy issues that may emerge. It is also important to note that while few have demonstrated a clear business case for the full adoption of a mobile NFC payment infrastructure in the U.S. to date, the vast range of announced pilots are evidence of widespread interest and anecdotally, many key players are sensing that the time is near.

External Influences on the Business Case

There are a number of disruptive changes occurring in the world of payments today that are upsetting the status quo, and continuing to push conversations about new payments technology, such as incorporation of mobile phone payments, to the over-arching issue of the need to overhaul/replace the existing mag-stripe infrastructure:

1. <u>Security issues with mag-stripe/stolen credentials</u>

Funding terrorist operations with stolen credit card and debit card credentials—which can be easily obtained from hundreds of black market websites for often less than a dollar—raises questions about how long the U.S. can persist in supporting current mag-stripe technology, when chip-based security for credentials is the standard for every other developed country in the world.

NFC payments, using a contactless chip in the handset that houses secure elements that protect account credentials, and communicates them securely through the NFC chip and antenna to the terminal, represents a new payments paradigm. Current and future cost avoidance opportunities and future reputational risk costs stemming from a move from mag-stripe to a mobile

based NFC world should become part of any business case analysis. Data associated with this move can be gleaned from current and proposed initiatives in other countries.

2. PCI compliance requirements and costs

Recent merchant association estimates (most recently from a survey by the Merchant Advisory Group in October 2010) project the amount of money merchants have spent to-date on trying to comply with PCI data protection requirements to be $20 billion or more, with annual costs expected to exceed $2.5 billion by 2014—more than the reported bank cost of payment card fraud itself. If accurate, such an investment would have easily paid for conversion to chip and pin technology. Merchants are uncharacteristically motivated to abandon the mag-stripe paradigm in order to rid themselves of this burden alone.

NFC payments securing account credentials from the handset chip to issuer authentication in a widespread deployment has the potential to greatly reduce merchant PCI issues. Those aspects of PCI compliance that can be satisfied by a robust mobile implementation should be factored into a business case assessment.

3. Endemic Fraud

Most payment card fraud containment activities in the past five years have related to PCI compliance, rather than attacking the sources of fraud,[31] leaving the industry with an ambient issuer fraud rate about $.05 on $100 in spend. That means absolute fraud losses continue to grow with volume, and if merchant and third party fraud losses are counted in the conventional estimate of about $2 billion in ambient card fraud (U.S. issuers only), future fraud losses could be 5-10 times that amount with all parties' losses counted in.

It is getting more difficult to justify continued investments in tweaking the mag-stripe infrastructure—versus investing in stronger, more digitally capable technologies—such as full NFC payments using secure elements and electronic wallet functionality. Future estimates of growth in fraud losses need to be a part of the business case, as opposed to historic costs[32].

4. Exported fraud

[31] VISA submission to the Federal Reserve in anticipation of the proposed rulemakings regarding the Durbin Amendment to the Dodd-Frank Financial Reform Act, fall, 2010.

[32] In late 2009, when the Smart Card Alliance estimated 2007 total U.S. card issuer fraud losses at about $1.7 billion, but indicated that total fraud was dramatically underreported, citing an estimate by Mercator that adding in all merchant and associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses, the total cost was closer to $16 billion --much of which was borne by merchants.

By clinging to mag-stripe, the U.S. also forces overseas deployers of chip+PIN cards to retain the mag-stripe on the cards they issue so that their customers can use them when in this country. Similarly, merchants overseas must prolong use of mag-stripe terminals to accept cards from U.S. customers. In effect, the U.S. is 'exporting' fraud to overseas issuers and merchants; yet few U.S. issuers are converting to EMV so far, and Visa and MasterCard are still non-committal on how fast they might support a conversion to EMV.

EMVCO has completed its initial contactless specification but needs to ensure that it conforms to generic use and interoperability, while Visa and MasterCard state their conversion plans and aim for the same kind of compatibility.

5. Regulatory impacts on signature-based card rates and pricing practices

The Durbin Amendment to the Dodd-Frank Financial Reform Act could result in outcomes that reshape debit card economics and competitive practices. For example, some suggest that in aggregate, the prospects for continued use of signature debit will dim in favor of PIN-debit. An estimated cut of 75% of interchange rates, to a cap of $.12 per transaction, may challenge existing business models for alternative payments in place today. Also, the current regulatory impetus seeks more competitive debit network access choices for consumers and merchants.

In open wallet configurations, where multiple payment types and networks can be accommodated, NFC payments can satisfy emerging requirements for broader payment choice. Final regulations on interchange and options will create a new business case environment for some of the critical parties that may carry over to the mobile environment.

6. Technology shift in consumer behavior

A persistent move is underway to on-the-go, real-time, mobile transacting as part of a versatile digital lifestyle for the young, including a new cohort of mobile bankers. Downloading of applications on increasingly sophisticated smart phones, coupled with the opening up of payment networks (e.g., PayPal, Visa, Intuit, MasterCard, etc.) for applications development, portends unprecedented opening of access for payment transactions. Mobile handsets have begun replacing wallets and pocketbooks with younger and tech-savvy consumers, and offering break-through utility and innovations in lifestyle.

While NFC-'lite' architectures (e.g., micro SD) may satisfy some of the utility of these innovations today, there is growing evidence of a concerted move to full, two-way NFC-enabled handsets—which will both accommodate digital lifestyle enhancing applications and support the commercial innovations discussed below. Use of mobile NFC solutions in symbiotic non-payments

areas will have an "improved economy of scale" effect on payments applications that could bring about improved unit costs.

7. Technology cost improvements.

In growing technology markets, prices characteristically improve over time as sales volume grows and standards are adopted. Because of the state of the mobile evolution in Europe and elsewhere, NFC standards are emerging and terminal manufacturers are deploying systems that already contain elements to support various types of non-mag-stripe card offerings, as well as mobile NFC. In fact, some U.S. merchants have already deployed such capture devices, while others have such plans, and still others are positioned to add on new technology.

This implies that the business case for merchants may not be as daunting as predicted in the whole. If so, the chicken and egg problem of customer demand and ecosystem ubiquity may diminish.

8. Improved buyer-seller interactions at POS

A slower growing economy overall, with little opportunity to raise prices when so many consumers (and businesses) are struggling financially, has propelled merchants to pursue new business models that improve on the poor historical results they have experienced with 'broadcast-mode' advertising, marketing and promotions, such as free standing coupon inserts in newspapers or store circulars. Instead, they are determined to use mobile technology to influence new customers to sample their stores, spend once they get in stores, try products the merchants (and manufacturers) are pushing, and exchange information that helps attract, grow and retain the relationship over time.

Two-way NFC enables real-time, location-aware interactions that combine shopper behavior and history with tailored, one-to-one promotions and integrated loyalty programs. As a result, some merchant groups are advocating a concerted move to contactless technology—bypassing the costs of deploying contact cards where possible. Moreover, the merchant business case for mobile is significantly enriched, if not substantially justified, by the marketing opportunities resident in mobile payment alternatives.

These influences taken together will shape which business models will survive or get traction in the decade ahead for the key participants in the evolving mobile payments ecosystem. In particular, if the U.S. payments market is indeed beginning to migrate to chip secured account credentials and PIN verification of cards at merchant terminals/network interconnections (whether based on the EMV standard

or something perhaps better), there will be many doubts about what interim technologies to invest in until or unless a new payment paradigm takes hold.

But there are fundamental conflicts that exist at the level of basic business interests of many participants in the new ecosystem that further complicate the decision on whether and to what extent to cooperate in a symbiotic sharing of new, non-competitive infrastructure. The differences in the business case pros and cons for the major participants are themselves revealing of the complexities inherent in transitioning a previously isolated business model to a more holistic one that can support the need to scale to huge volumes, provide security in ubiquitous retail environments, and interoperate in a seamless and transparent fashion. Replicating those attributes will be a daunting task.

Conventional Payments Stakeholder Business Challenges

Starting with the existing, conventional payment card transaction providers—banks, bankcard associations/networks, processors, and terminal providers—for whom the status quo—recent regulatory changes in interchange and banking fees notwithstanding—has produced a sustaining and substantive business opportunity, participating in the emerging mobile ecosystem presents unusual business case challenges.

Banks

Twenty years ago, banks depended primarily on interest rate arbitrage for the bulk of their earnings. Today, more than two-thirds (cite?) of bank revenues come from an assortment of fees, charges, and other pricing for services. Tomorrow, banks will earn billions less from consumer fees and pricing (e.g., on checking account overdrafts), and an estimated 75% reduction of interchange revenue on debit cards. Pressures are expected to mount to lower merchant costs for credit cards as well. For the top 10 banks, which control over 90% of credit card revenues, and get 20-30% of overall payment revenues from credit cards, the economics of the signature-based payment cards status quo is declining dramatically. So a lot is riding on making sure that bankcard payment options make it into new venues like mobile.

Implementing EMV contactless could be materially cheaper to implement than contact cards in some retail sectors that have resisted any wholesale change at POS. For example, in the convenience store industry, two-thirds of the outlets pump gas. The average store incurs an average of $700 of card fraud per year. PCI compliance costs them $1600—making that a stretch for business case justification all by itself. Outfitting pumps with remote smart-card/PIN readers would cost an estimated $50-60,000 per station (according to the National Association of Convenience Stores). With some 8% of retail sales in this retail vertical, EMV contact cards represent a huge hurdle. But contactless phones able to communicate into the store via a Wi-Fi hotspot could cost less than $5000 per store.

The banks, and their card payment associations, argue that they already provide consumer access through hundreds of millions of existing payment accounts, and merchant acceptance at 8 million locations. Moreover, they have global networks that already scale to huge volumes and generations of risk management experience. So the business case for their participation in mobile NFC payments is: 'use what's already there' and adapt the existing infrastructure to evolving needs. The question, of course, is at what level of economics for what participants? And whether they will manage a chip+PIN paradigm with more flexibility and balancing of compensation than exists with the mag-stripe model.

Bigger banks experience an intensity of reactions from these influences, owing to both the considerable money they have historically made on signature-based, mag-stripe cards—at least until the coming year—and the investments made in both online and mobile banking and card use. Smaller FIs face a quandary of their own, contrasting a keen and growing desire to be relevant to the digital savvy, under-35 cohort of financial services customers, and the need to find a way to obtain infrastructure services to allow them to do mobile banking, mobile payments, mobile marketing, and—prospectively—chip and pin. Those are daunting choices and investments to make at a time in which industry wide debit card revenues might drop by $15 billion or more.

Payment Networks

While fundamentally aligned with their bigger banking members, Visa and MasterCard as public companies are increasingly driven by the mandate to drive more transactions across their networks—even if they come from non-banks/non-members. Step-by-step, these publicly traded payment networks have pushed into prepaid, contactless, P2P payments and more recently, versions of NFC-based payments, doing pilots with both bank members and non-banks. And, they are not as impacted financially by the regulatory changes sweeping the current payment card business. So, it is logical to expect them to be at the table for any consideration of mobile payments infrastructure and business opportunities.

What is not so certain is the business case for the ecosystem's use of their networks, and ascribing to their network rules and requirements. After decades of exerting material influence over industry pricing, the mobile payments paradigm in the new regulatory environment appears to be seeking different revenue models going forward—particularly those where the mobile handset interaction in merchant locations fosters real-time, location- and customer-aware decisions on purchases, and where big and powerful non-banks (e.g., wireless carriers) are key players.

Closed-loop charge card companies like American Express and Discover stand to play intermediary roles in architecting new variations of mobile payments, as recent market initiatives indicate. Because they have nearly the same merchant acceptance 'pipes' as the credit card payment networks, and can offer national access for tens of millions of consumers with their payment cards, they can be a factor in any new business calculation. For them, the business case is new transaction volumes from potentially new

customers who utilize them for mobile applications, with merchants still willing to pay prevalent credit card transaction fees.

Non-profit payment networks such as the ACH network and other PIN debit networks also provide payment utilities for their financial institution members of all sizes. Volume is also important to these networks as they develop rules to balance the appropriate amount of innovation with risk management for the benefit of their FI members, which enable valuable solutions for their clients.

Processors

Payment card processors are a lynchpin to the existing infrastructure, but will be called upon to make major changes to their network configurations—particularly to accommodate passing encrypted account credentials through their terminals and networks straight through to chip and pin implementing issuers. This is not a trivial task. For example, in order to minimize the deployment changes required in processor environments overseas when EMV was implemented, Visa and MasterCard have temporarily permitted use of static authentication of chip card transactions (rather than dynamically generating unique data) and decrypting the account credentials at the merchant terminal so they could pass through the processor network to the issuers. Similarly, processors were given two-and-a-half years longer to become PCI compliant than their big merchants were, meeting these requirements only by mid-year 2010 as mandates.

Like the payment card associations, the key economic driver is the *volume* of the transactions, versus the interchange fee rate. So as long as processors can derive a business case for making the infrastructure changes, they would be largely indifferent as to what type of payment was being generated. Moreover the liability shift that accompanies robust implementation of chip and pin would largely make processors' lives easier, and perhaps lower cost due to the reduction in charge-back and other exception handling costs.

But, with some exceptions, many processors have remained silent on the much-discussed mobile 'transformation', and have focused on preserving the funding levels that the payment card industry has historically generated, for as long as possible. That is perhaps understandable in a part of the business that has borne the brunt of price compression from both merchant discount fees and the associations' pass-through of acquirer fees for many years. Their clear concern: how many of which alternative payment types and technologies must they tool-up to support?

Terminal Manufacturers

For several years now, higher end POS terminals have spawned a rich array of functionality to support PIN-debit, prepaid, ACH, barcode, and even biometrically authenticated applications. A standard terminal now contains hundreds of potential applications that need only simple downloads or on-site programming to activate. Such application-migration now extends to EMV contact card reading

capabilities, as well as vanilla contactless tap-and-go radio signaling. Attaching a full-NFC reader to these terminals is fairly straightforward, and can cost about $300. Some recent quotes for both EMV contact card and contactless combination readers are around $400 per terminal, if deployed together. For these participants of the ecosystem, change is usually a good (and profitable) occurrence.

Such forward-thinking infrastructure planning has been embraced by some of the nation's biggest merchants. For example, Wal-Mart, BestBuy and HomeDepot—among others—are currently able to accept EMV contact cards around the world, and Wal-Mart has publicly predicted EMV transactions in the near-term (BestBuy and HomeDepot were also early adopters of contactless tap-and-go). Meanwhile, hundreds of smaller merchants in U.S. states along the Canadian border are already accepting EMV card payments from their foreign shoppers using cards issued by Canadian banks.

The sticky problem with terminals, however, is the business case for getting the millions of smaller merchants to upgrade their terminals. For example, there are roughly 400,000 merchants still using Verifone Tranz330 terminals which were first introduced in the mid-1990s. These terminals have limited applications for largely mag-stripe only transactions, and subject the system to much inefficiency—like the ability to commit rudimentary fraud (e.g., with forced draft capture). Many of these merchants are likely to protest even POS upgrades that cost them only a few hundred dollars—just as they have resisted PIN-debit pads over the years, even though the additional monthly cost is typically less than a dollar.

Merchant Requirements

A primary but until recently reticent player in any payment ecosystem is the merchant base. Perhaps emboldened by a recent surge of support from Congress, regulatory agencies and the courts and with an unusual sense of unanimity, U.S. retailers have largely embraced the mobile transformation—partly as a way forward from a payments business model largely unchanged over decades, but mostly as an opportunity to gain one-to-one relationship connections with customers, and truly drive incremental, competitive sales.

To that end the National Retail Federation introduced a report in mid-2010 (updated in January 2011) called the *Mobile Retailing Blueprint*, containing an extensive list of innovations that NFC-enabled and other mobile payments could bring to the retail sector.[33] At the end of 2010 the Merchant Advisory Group published a set of policy and infrastructure recommendations to put their spin on what should be done implement the Blueprint as soon as possible.[34] Among the suggestions: focus deployment on EMV contactless, bypassing EMV contact card deployment where possible, to avoid transitional investments in technologies that will not be essential in the future.

[33] National Retail Federation. 2011.
[34] Merchant Advisory Group. 2010.

Most importantly, though, the merchants active in contactless and NFC mobile payments implementation seek an 'open wallet' configuration, where consumers can load as many payment choices as they want, and merchants can search for the payment options they prefer in the transaction session. Such choices would include standard credit and debit account options, but would not be restricted—as they are today for the most part—from doing PIN-debit, prepaid, merchant private label, or even ACH transactions. Transactions from third parties—PayPal, BlingNation, Obopay, Western Union—could co-exist with those from the traditional payment brands. There is even talk of cross-merchant acceptance of closed-loop, private label, merchant-provided credit and prepaid options

Such new requirements from such an important part of the mobile payment ecosystem foretell a much more competitive environment for transacting than has ever existed before, and makes the notion that both banks and carriers could build their business cases mainly on joint assessments of payment fees a much less likely route for tomorrow's revenue model. In other words, the business case for NFC payments must go beyond the payments component.

Other Ecosystem Participants

New participants in the mobile payment ecosystem (e.g. wireless carriers, application providers/markets, handset makers, security providers, system integrators, trusted service managers, etc.) all have their own revenue and profitability objectives. Until very recently, they expected some portion of payment fees to drive the business case for their participation. While much of the arms-length jockeying between banks and carriers for ecosystem support over the past two to three years concerned which industry would charge the fees (to merchants) and how those fees might be divided up, the recent merchant 'activism' (and apparent exploration of market alternatives) has changed the nature of the 'conversation' toward who provides what value, and what is fair compensation for that value.

Wireless Carriers

Three of the big carriers announced a joint NFC initiative (called Isis) in conjunction with Discover and BarclaysCard in November 2010. Details were sparse, but the idea was that the built-in NFC wallet would be restricted to carrier-specified payments, and the carriers—rather than banks—would earn the interchange portion of merchant fees. Several reports on Isis concluded that besides aversion to any restrictions on payment choice, some merchants were disappointed that a new revenue model that improved on the interchange convention had not materialized.

If nothing else, this announcement put the payments world on notice that some big players with deep pockets wanted to participate. The carriers' ability to package and bundle services built around heavily marketed handsets demonstrates their ability to steer consumers to more and more advanced services. Whatever the fate of Isis might prove to be, carriers appear likely to be important for the front-

end outreach necessary to spur consumer adoption. Moreover, Isis fueled consideration that, while carriers were clearly seeking new sources of stable revenue for a wireless business that underwent constant price compression, the other assets they brought to the mobile table were very important to factor in to the ultimate business case. Certainly their ability to operate huge networks undergoing rapid change, and their ability to incorporate relentlessly evolving technology with persistent risk management challenges made them a worthy partner for mobile commerce.

The biggest revelation was the possibility that carriers, who collect unique handset identification numbers, the cell phone number associated with a registered account, a location over a specific network, and other verifying data, could become valuable fraud mitigation partners with banks, which know a purchaser's registered account number, associated authenticating information, bank account history and behavior, and usage patterns. In combination, mobile payments could be materially safer than any other payment mechanism, and the properties of end-to-end digital transmission and authentication points could make mobile payments more efficient as well. Regardless of all the above motivations, carriers stand to handle and charge for more traffic across their networks than experienced in traditional non-mobile payments systems.

Application Providers/Marketers

Any observer of the explosive phenomenon of Apple iPhones and their cavalcade of applications (including dozens of payment utilities for both consumers and merchants) can see where the mobile payments market is headed. While Apple itself operates as a walled garden (including a set of NFC patents), the application provision market for open Google Android, Blackberry and other handset operating systems ensures that complete payment choice—and self-sufficiency—is a safe bet among smart phone users (28% of the marketplace at year-end 2010).[35]

For some of these companies (e.g., PayPal, BlingNation, Obopay, and Western Union), capturing incremental payments *is* the business model, and garnering payment fees drives the business case. For the most part, these companies gain merchant and bank acceptance at slightly lower fee levels than standard signature-based cards. In a post-Durbin world, however, there is no certainty that these base-level rates will prove sustainable. So even they will need to find other sources of revenue in the value they add.

For online marketers morphing to the mobile environment, such as Google, marketing sources of revenue—i.e., paid searches, lead generation fees, linked advertising, etc.—promise to be as rich as on the internet. In fact, in their previous payments foray for the online market (Google Checkout), the search goliath attempted to make payments transparent to the advertising and marketing propositions—a useful analogy for mobile, perhaps.

[35] Composite estimates of CTIA, ABI Research and other industry research firms.

Moreover, the ability to add real-time, location-aware, one-to-one granularity to essentially 'blind' online interactions offers the potential for much higher fees and profits from results superior to those online. Such optimism is borne out by the surging number of mobile coupon tests being conducted in the marketplace. Initial results of user take-up appear very encouraging for all participants—including merchants which appear willing to pay high rates for consummated purchases than can be demonstrated as incremental and/or taken from competitors.

Technology Providers

Most of the other components of the mobile payments ecosystem sell infrastructure and/or related services to the others. Such technology includes handsets, security components, communications and systems integration, and even shared-services configurations such as Trusted Services Managers (TSMs). Most of these participants are dependent upon a fully secure, two-way NFC paradigm becoming commonplace in the next 2-3 years. Accommodating secure payments is viewed as an essential baseline service that will attract the consumer to other high-value activities, and that, in turn, will further increase demand for their products and services.

To some degree, these participants can 'prime-the-pump' for new infrastructure. For example, Nokia's announcement in late 2010 that all of its smart phones from 2011 forward would be full NFC-enabled help dilute skepticism that an NFC critical mass would ever appear. Google's recent announcement that Android 2.3 would support NFC payments, coupled with reports that millions of NFC-enabled phones were already in the Android pipeline, further buoyed confidence and expectations in this ultimate baseline configuration for mobile payments.

To-date, mobile technology providers tend to embed their products and services in packages crafted by the carriers, and more recently by Apple, Google, and Microsoft—as these computing companies expand their presence into the mobile marketplace. The real costs of this technology (e.g., full NFC components for GSM handsets is believed to cost an incremental $5-$10) is often not visible to the public, but must be accounted for in a business case for *some* member of the mobile payments ecosystem. But that business case does *not* have to be based on payments functionality alone.

Regulatory Road Map/Shared Infrastructure Decisions

All of these uncertainties make business planning precarious, and companies hesitant to invest. So representative constituencies of *all* of these participant groups have asked the Fed to coordinate with other regulatory agencies (such as the FCC and FTC) and provide a 'regulatory road-map' of what functions, activities, and implementations would be viewed as permissible over the next three to five years. These mobile payments ecosystem players are also asking for clarity on what infrastructure can/should be shared on a non-competitive basis.

For example, security is certainly a foundation for market cooperation, as evidenced in TSMs for smart cards worldwide. But other business services that might be critical to market adoption in the U.S., such as standardized contracting among 16,550 banks and credit unions, 5,000 wireless carriers, and millions of merchants, notification services for lost handsets and even (perhaps especially) coordinated risk management are all under consideration.

So the foundational notion that has emerged is to compete on the marketing and personal service value propositions—but not on generalized transaction capabilities. In this sense, payments become a *qualifying* factor for standardized applications and components of shared infrastructure that protect everyone, but the mobile marketing, advertising and promotional components become the bases for *differentiation* (and therefore competition). As such, mobile marketing services become the heart of the business case for NFC payments. (Note: This is really a good point. Let's see if we can incorporate it in the new vision part of the document also.)

Thus, the mobile marketing business case drivers—mostly still to be determined in an empirical way—should be viewed, and researched, as part of a brand new theoretical construct. Under this construct, payment choice, with open and/or interoperable mobile wallets, will enable the market to set its own prices—in all likelihood as a function of actual costs. And superior customer value in facilitating efficient and effective transacting should engender contributions (financial or otherwise) from both buyers and sellers for the new value they receive. Whether that value materializes as purchase commitments from consumers, or incremental purchase bounties from merchants, the specific mechanism is less important than the concept that real value provided will find a path to fair compensation.

APPENDIX IV – Mobile Payments Standards in the U.S.[36]

Mobile payments require multiple industry participants to work together. If collaboration is difficult, adoption will be delayed. Difficulty may arise because the industry is made up of many small participants who are heterogeneous and have very different preferences, because there is a culture of distrust, or because of legal restrictions. All of these issues play a role in the evolution of mobile payments.

Because there are over 16,000 banks and credit unions but just four major mobile carriers (who account for nearly 90% of the handsets used) in the U.S., industry-wide agreements on technology standards and business policies are very difficult to coordinate and negotiate to reach consensus. Bilateral negotiations between a single bank and a single carrier are much easier, but the market share of customers having accounts with both the bank and the carrier for any given pair of institutions is likely to be small, lowering the value of any resulting agreement. The number of parties involved in each transaction: a mobile carrier, a handset manufacturer, a payment network, a mobile software vendor, a bank, a merchant, and a consumer also make it more difficult. The parties must agree on who is responsible for verifying the consumer's identity, resolving disputes, handling customer service, etc.

Coordination problems may be exacerbated by the possibility that the significant players (banks and mobile carriers) both consider the users to be their customers and therefore may want to "own" the relationship with the customer and the rich set of information that mobile payment services yield.[37] And even though four mobile carriers dominate the wireless market, there are 5,000 wireless carriers in the U.S. in total. Nearly all are small, localized carriers that serve customers in rural areas of the country. The FCC does not want those rural carriers to disappear as the industry evolves, so it will be important to integrate them into the mobile ecosystem.

Open industry-wide standards, involving all stakeholders, are necessary to achieve mass adoption of mobile payments. The alternatives are not simple. For instance, mobile carriers could offer payment services without the involvement of banks, perhaps by limiting consumers to pre-pay accounts or by offering consumer credit themselves. Alternatively, a single carrier could contract with a single bank to offer payments services. These types of approaches are feasible, but they face serious hurdles. Limiting consumers to pre-pay accounts reduces the attractiveness of the product, and offering credit services brings carriers into an unfamiliar industry at a large scale, with important regulatory obligations. To succeed on a large scale by contracting with a single bank, consumers must agree to transfer their financial relationship across institutions, something they are often hesitant to do.

[36] Excerpts from Crowe, M., M. Rysman and J. Stavins. 2010. "Mobile Payments in the U.S. at Retail Point of Sale: Current Market and Future Prospects." Federal Reserve Bank of Boston Public Policy Discussion Paper, No. 10-2.
[37] McCarthy, B. 2008. "Mobile Payments: The Linchpin of the Mobile Commerce Economy," White Paper, First Data.

The U.S. is making important progress in developing an industry standard for the technical details for how mobile payments might work, thus overcoming substantial negotiation costs in this regard.

Current Mobile Standards Efforts

The development of open industry-wide standards through collaboration of industry stakeholders may be the best path towards successful adoption of mobile payments. Importantly, an open standard for mobile payments is under development currently. The financial industry standard-setting group ASC X9 is developing U.S. standards, and ISO is developing an international version of the standards. [38] The X9 and ISO standards will specify how a mobile phone securely formats messaging and data elements and delivers that information over payment rails. Any bank, mobile carrier, or other vendor that develops its service in compliance with the standards would be able to participate in the mobile payments market. At this stage, prospects for the ultimate development of mobile payment standards appear to be strong, although their readiness is at least 18 months away. However, developing a standard does not ensure that it will be adopted.

Although standards are currently in place for the transmission of data either remotely or by proximity from a mobile device to allow for mobile commerce, gaps exist and need to be addressed in order to provide an efficient and secure mobile commerce environment. While ISO 14443 describes the physical characteristics of proximity hardware and NFC standards enable the exchange of data wirelessly, the following work efforts are underway to address the gaps.

ISO TC68/SC7/WG10 Mobile Banking / Payments (International)

The ISO study group, convened by the U.S., has identified areas for development of an international standard and will be formally developing standards for the following areas:

- Mobile person-to-person payments, involving a financial institution intermediary
- Life cycle management of banking/payment applications
- Banking alerts
- Banking account Inquiries
- Banking solicitations and offers
- Payer to the secure element authentication
- Discovery of device capabilities
- Technical report on business oriented security requirements

[38] ASC X9 (Accredited Standards Committee X9) is an industry nonprofit association composed of members of the financial services industry. ISO (International Organization for Standardization) is a network of national standards institutes of 162 countries, one member per country. It is the world's largest developer and publisher of international standards.

For the new work item, the group recognized that Payments break down into two broad areas, proximity and remote. There is a consensus that models for point-of-sale payments will heavily leverage the standards in place for NFC contactless payments. The workgroup will set new standards for "Life Cycle Management of Banking/Payment Applications" as well as "Person to Person" payments, including remittances, focusing on mechanisms that leverage clearing and settlement through established banking channels. These standards will include messaging between parties as well as bill and invoice payments.

For banking the workgroup will focus on three areas: "Alerts," "Inquiries" and "Solicitations/Bank Offers." Each will leverage existing standardized technologies, e.g. Short Message Services (SMS), Instant Messaging (IM) and Really Simple Syndication (RSS). For authentication, the workgroup will develop standard interaction models for "Payer to the Secure Element," standard means for the identification of "device capabilities", and document "business oriented security requirements" for sound banking practices.

X9.112-3 - Mobile Commerce (Domestic)

The mobile environment accumulates numerous risk factors, such as: unattended terminals, card-not-present transactions, untrustworthy platforms, and persistent wireless connections. Further, the mobile network operator (MNO) infrastructure may not provide sufficient security that can be relied upon by the financial services industry. From a security perspective mobile commerce suffers all of the same vulnerabilities as the internet and wireless environments combined; and from a business perspective it encompasses three disparate industries: financial services, mobile telecommunications, and manufacturing mobile platforms.

Areas within scope of this standard include but are not limited to the following:

- Mobile transactions, including sending and receiving messages for payments, banking, and commerce
- Mobile payments for person to person (P2P), person to business (P2B), and small business to business (SB2B), including credit card, debit card, and electronic funds transfer (EFT) transactions

Areas not in scope because they are addressed by other ANSI or ISO standards include: PIN Management and Security; Biometric Information Management and Security; Key Management and Security; and mobile marketing (e.g. advertisements, coupons, loyalty programs, catalogs).

Stored Value Cards: An Alternative for the Unbanked?

July 2004

Printer version

Stored value cards are one of the most dynamic and fastest growing products in the financial industry. Anyone who makes purchases with a merchant gift card, places phone calls with a prepaid telephone card, or buys goods or services with a prepaid debit card is using a stored value card. Certain types of these cards are being heavily marketed to lower-income consumers, especially the unbanked or underbanked. Although these cards may provide consumers with a more effective means of accessing funds and making financial transactions than cash, consumers need to be aware that these cards come with a vast array of features, fee structures and levels of consumer protections. This article highlights many of the principal features of these financial innovations and identifies important aspects of these cards that consumers must be aware of in order to make informed decisions about the products that best meet their financial needs.

Stored value cards provide a way to make financial transactions. Stored value cards use magnetic stripe technology to store information about funds that have been prepaid to the card. Payroll cards, government benefit cards, prepaid debit cards, gift cards, and telephone cards are examples of stored value cards. There are two main categories of stored value cards in the marketplace. The first prepaid cards made available to the marketplace were single-purpose or 'closed-loop' cards. Gift cards, which can only be used to purchase goods at particular retailers, and prepaid telephone cards, which can only be used to make telephone calls, are examples of single-purpose cards. The second type of card to emerge was a multipurpose or 'open-loop' card, which can be used to make debit transactions at a wide variety of retail locations, as well as for other purposes, such as receiving direct deposits and withdrawing cash from ATMs. Some multipurpose cards are branded by Visa or MasterCard and can be used wherever those brands are accepted.

Consumers obtain stored value cards in a variety of ways. They may obtain a payroll card from an employer, an electronic benefit card from a government agency, or a gift card from a retail store. Typically, a consumer would apply for a general spending multipurpose card by telephone or online, although these cards may be increasingly offered at check-cashing outlets, money transfer company locations, and retail stores.

The stored value card market is growing and evolving rapidly. According to industry estimates, more than 2,000 stored value programs are available, with roughly 7 million Visa- or MasterCard-branded stored value cards in the marketplace. There are approximately 20 million users and that figure is expected to more than double to 49 million users by 2008. In 2003, stored value cards were used to make $42 billion in transactions. By 2006 over $72 billion in stored value transactions are expected. Experts put this industry in the introductory or early growth stage of the product life cycle, suggesting that there is substantial growth potential in the years ahead[1]. These industry figures include all stored value cards, such as multipurpose general spending cards, payroll cards, government benefit cards, child support payment cards, merchant gift cards, and telephone cards.

Reloadable multipurpose cards are often viewed as alternatives to checking accounts. Among stored value cards, reloadable multipurpose cards most closely resemble traditional deposit account debit cards in functionality and are thus most likely to meet the needs of the unbanked or underbanked. Consumers not only can use these cards to make payments to a wide variety of merchants and service providers but also can reload them with additional funds. The ways in which cards can be reloaded vary but may include direct deposit, money wire transfer, money order, or cash presentment at designated retail locations such as convenience stores.

Reloadable multipurpose cards are offered by a variety of firms and have an assortment of features. Some cards are both issued and distributed by banks, while others are issued by banks but distributed to customers by nonbank firms. Nonbank firms may also play roles in processing card transactions. Some cards are Visa- or MasterCard-branded, allowing them to be used wherever these bank association cards are accepted.

Cards may offer any or all of the following functions: direct deposits of payroll checks, withdrawals of cash at ATMs, payments for retail purchases, bill payments, and money transfers. Some cards require the cardholder to enter a PIN (personal identification number) at the point of sale, whereas others require the cardholder's signature. Credit-building features, in which accounts in good standing are reported to one of the credit bureaus, are offered by a few card issuers, although the degree to which such features actually influence a customer's credit score is still unclear. There is some preliminary discussion among industry representatives about the feasibility of adding overdraft protection or payday advance features; for example, cardholders would pay a fee to receive a loan advance from their next payroll deposit. Here, again, the net benefit to cardholders is unclear.[2]

Consumers need to be aware of how these cards work and the fees they will incur. Given the wide range and complexity of card types and features, consumers must weigh the benefits of these features against the additional costs incurred. Below are some of the primary categories of fees and the ranges of fees that may be charged[3]. Cards that have relatively high fees in one category often tend to have relatively low fees in another category; for example, higher monthly fees are often associated with lower or no transaction fees.

Table 1: Basic Fee Categories

FEE TYPE	FEE RANGE
Entrance/Activation	$0 to $39.95
Maintenance	

EXHIBIT
K-11

Annual	$0 to $99.95
Monthly	$0 to $9.95
Point of Sale	$0 to $2.00[4]
Domestic ATM Transaction (within network)	$0 to $2.50

Other potential fees to look for include:

- Transaction limit fee
- Bill payment fee
- Phone or online transaction fee
- Reload fee
- Money transfer fee
- Out-of-network domestic ATM transaction fee
- International ATM transaction fee
- Inactivity fee
- Overdraft fee
- Overdraft protection fee
- Payday advance fee
- Credit-reporting fee
- Dispute fee

Consumers should also pay attention to whether or not their financial transactions generate dual fees. For example, while the company offering the card may not charge a fee to the consumer for reloading the card, there may be a charge from a third-party, such as a retail store or a check cashing business, that accepts and loads these funds.

Whether a stored value card makes financial sense for a consumer depends on how the consumer expects to use the card. Consumers should carefully examine the fee structure of different stored value card products and calculate the expected monthly costs for each card based on the kind and number of transactions they foresee making. They should also compare the costs and benefits of using a stored value card in lieu of holding a checking account or using alternative financial service providers such as check-cashing businesses. The table below shows average fees nationwide for various types of non-interest-bearing checking accounts.[5]

Table 2: Minimum Balances and Fees for Non-Interest-Bearing Checking Accounts

TYPE OF ACCOUNT	MINIMUM BALANCE TO OPEN	AVERAGE MINIMUM BALANCE	AVERAGE MONTHLY FEE	AVERAGE PER-CHECK FEE
Single-Balance, Single-Fee*	$159.21	$591.46	$7.35	$0
Fee-Only**	$78.41	$0	$5.27	$0.22
Free	$73.82	$0	$0	$0

**The monthly fee is not charged if accountholder maintains the minimum balance.*

***The monthly fee is charged regardless of balance; per-check fees are not always charged.*

Consumers should be aware that some states, including New York, require banks to provide low-cost checking accounts. Even so, consumers should verify whether monthly, per check, or other fees (e.g., out-of-network domestic or foreign ATM fees, overdraft fees, debit-card transaction fees, and transaction limit fees) are charged against these types of checking accounts.

Consumers may also wish to compare the costs of using a stored value card with those of using a check-cashing business or other alternative financial service provider. Fees at check-cashing businesses vary widely because they are determined at the state regulatory level. Fee limits in New York, New Jersey, and Connecticut, are among the lowest in the nation, ranging from 1.4% to 2.0% for most checks. As of 2003, eighteen states had no limits whatsoever.[6] Check-cashing customers will also pay fees for bill payment services, money orders, and money transfer services.

Stored value cards may not offer all of the consumer protections that come with traditional checking accounts. Although a reloadable multipurpose card may provide a level of functionality equal to or better than a traditional checking account, not all cards offer the consumer protections enjoyed when holding a traditional checking account. Specifically, consumers should be aware that some cards do not currently provide federal deposit insurance to protect the cardholders' funds in the event that the issuing bank fails.[7] In addition, some cards do not provide protections under Regulation E which covers debit cards linked to traditional checking accounts. Regulation E has several requirements, the most important of which are provisions for fund replacement in the event of lost or stolen cards.[8] Visa- or MasterCard-branded cards offer zero-liability policies, although consumers should be aware that these association and/or firm-specific policies are not the same as Regulation E protections.[9]

Regulatory changes and new product innovations may benefit consumers. On the regulatory side, it remains uncertain whether federal regulations that govern deposit accounts and debit cards will be expanded to apply to stored value cards. Several regulators, however, are presently looking into the issue. For example, the Federal Deposit Insurance Corporation (FDIC) is currently evaluating comments on whether stored value card funds should qualify as deposits that must be insured.[10] The Federal Reserve Board is considering whether stored value payroll cards should be covered by Regulation E. The Office of the Comptroller of the Currency (OCC) issued an advisory letter in May 2004 offering guidance to national banks engaged in payroll card systems regarding appropriate disclosures, error resolution procedures, liability limits for unauthorized use, and other issues.[11] States, too, may initiate consumer protection requirements for stored value cards, such as caps on certain kinds of fees.

Industry innovations may also benefit consumers' interests in asset-building and credit-building functionality.[2] Some card providers have begun to look at ways to add interest-bearing accounts to card products. Others are testing ways to report cardholder transaction

activity to credit bureaus. The Office of Regional and Community Affairs of the Federal Reserve Bank of New York and the Center for Financial Services Innovation at Shorebank Advisory Services are working together to examine industry trends and innovations in these areas.

Top

[1]*See Ted Dargan, "A Stored Value Update" and Karen Larsen, "Closed Systems: Strategies for Capitalizing on Gift/Convenience/Loyalty Cards", Stored Value: Challenging the Credit Card Paradigm, Conference Proceedings, Pelorus Group, March 2004.*

[2]*These card features and others are described in greater detail in "Stored Value Cards: A Scan of Current Trends and Future Opportunities", Katy Jacob, Center for Financial Services Innovation, 2004 (**http://www.cfsinnovation.com/managed_documents/storedvaluecard_report.pdf**).*

[3]*Fee ranges are taken from "Stored Value Cards: A Scan of Current Trends and Future Opportunities", Katy Jacob, Center for Financial Services Innovation, 2004.*

[4]*Pin-based transactions tend to have higher fees than signature-based transactions.*

[5]*Board of Governors of the Federal Reserve System, "Annual Report to the Congress on Retail Fees and Services of Depository Institutions", June 2003.*

[6] *Financial Service Centers of America, "Check Casher Fee Schedule: Regulated States", 2003. See **http://www.fisca.org/FeeSchedulenew.pdf***

[7]*For more information on FDIC coverage, see **http://www.fdic.gov/regulations/laws/rules/1000-100.html***

[8]*For more information on Regulation E requirements, see **http://www.fdic.gov/regulations/laws/rules/6500-3100.html***

[9]*For more information on Visa and MasterCard zero-liability policies, see **http://www.usa.visa.com/personal/secure_with_visa/zero_liability.html?it=il_/personal/secure_with_visa/index.html** and **http://www.mastercard.com/general/zero_liability.html***

[10]*See **http://www.fdic.gov/news/news/financial/2004/fil4404a.html**; comments were due July 15, 2004.*

[11]*See **http://www.occ.treas.gov/ftp/advisory/2004-6.doc***

[12]*These innovations are described in greater detail in "Stored Value Cards: A Scan of Current Trends and Future Opportunities", Katy Jacob, Center for Financial Services Innovation, 2004.*

Top

FEDERAL RESERVE BANK OF BOSTON™

U.S. Mobile Payments Landscape – Two Years Later

by Marianne Crowe, Susan Pandy, and Elisa Tavilla, Federal Reserve Bank of Boston; Cynthia Jenkins, NACHA
May 2013

The Federal Reserve Banks of Boston and Atlanta through their Payment Strategies and Retail Payments Risk Forum Groups have released a paper based on several meetings of the Mobile Payments Industry Workgroup over the last two years. This paper updates **the original version** issued in 2011 and reflects on the evolution of the mobile retail payments industry over the last two years, which has witnessed considerable changes including collaborative efforts across a diverse set of industry stakeholders despite a market still characterized by considerable fragmentation, increased channel and technology convergence, participation by new non-bank entrants, and continuous technological innovation and experimentation. The paper concludes that while the market is still nascent, progress is being made towards achieving benefits within this ecosystem such as improved security and fraud reduction, cost efficiencies, value-added services, revenue and monetization opportunities, and data privacy. As a result of changes in the mobile payments landscape, the MPIW has updated its original strategic principles and has carved out a long-term vision that embraces technological disruption and is committed to interoperability and ubiquity but realizes the need for a concerted effort to develop industry guidance and standards to ensure a secure and cost-efficient ecosystem.

Full paper

EXHIBIT K-12

U.S. MOBILE PAYMENTS LANDSCAPE – TWO YEARS LATER

Marianne Crowe, Susan Pandy, and Elisa Tavilla, Federal Reserve Bank of Boston

Cynthia Jenkins, NACHA[1]

May 2, 2013

[1] At the time the white paper was written, Cynthia (Merritt) Jenkins was employed at the Federal Reserve Bank of Atlanta.

The authors would like to thank the members of the Mobile Payments Industry Workgroup for their valuable contributions to the work effort and insightful ideas and comments that are the foundation of this paper. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Banks of Atlanta or Boston, the Federal Reserve System or NACHA.

EXHIBIT
K-13

Table of Contents

I. Executive Summary 3

II. Changes in the U.S. Mobile Payments Ecosystem: 1Q2011 to 4Q2012 4

Mobile Network Operators (MNOs) 5
Smartphone/Terminal Manufacturers and Mobile Operating System Providers 5
Payment Processors and Alternative Payment Service Providers 6
Payment Cards and ACH Networks 7
Financial Institutions 8
Merchants 9
Consumers 11
Regulators 11
Summary 13

III. Progress Towards Achieving Benefits 13

Improved Security and Fraud Reduction 13
Merchant Cost Efficiency 15
Competitive Technologies 16
Value-Added Services 17
Revenue and Monetization Opportunities 18
Data Privacy 18

IV. Update of Original Strategic Principles 19

Open wallet concept has evolved to include both mobile and digital wallets 20
Convergence of multiple technology platforms for mobile payments 20
Establish a ubiquitous platform for existing and new clearing and settlement rails 21
Dynamic data authentication provides long-term integrity and security for transactions across all channels 21
Develop and adopt a global interoperable platform in the U.S. for mobile payment standards and certification of payment methods 22
Neutral Trusted Service Managers (TSMs) to oversee the provision of shared security elements used in the mobile phone 23
Regulatory Clarity 24
Understanding the Role of Nonbanks in the Mobile Payments Ecosystem 24
Summary of Principles 25

V. Long-term Vision 25

Ongoing Technology Advancements will Alter the Mobile Payments Landscape 25
Mobile and Digital Wallets will Co-Exist 26
Increasing Channel Convergence 26
Big Data Monetization withRisk Management Oversight 26

VI. Conclusion 27

Next Steps for the MPIW 27

Appendix: MPIW Activity 2011-2012 28

I. Executive Summary

In 2010, the Federal Reserve Banks of Boston and Atlanta (FRB), through their Payment Strategies and Retail Payments Risk Forum groups, convened the first Mobile Payments Industry Workgroup (MPIW)[2] to discuss the benefits and obstacles to developing a successful U.S. retail mobile payments system. The MPIW meets with the FRB three to four times per year to discuss mobile industry developments and related issues. In response to expanded use of mobile payments and increasing interest among mobile stakeholders, the FRB expanded the MPIW's scope in 2012 to enable broader participation from groups with a specific interest in mobile payments adoption such as merchants, vendors, start-ups and regulators. The FRB will maintain this approach to ensure ongoing comprehensive discussion within the MPIW that encompasses prospective issues of collective concern.

After multiple meetings during 2010 and 2011, the group dialogues were captured in a white paper published in March 2011, *Mobile Payments in the United States: Mapping out the Road Ahead*.[3] Since the first paper was published, the mobile payments industry has undergone considerable changes. Notable changes include increasing convergence of channels that has blurred the lines between online and physical commerce. A broad range of technology developments are accelerating this convergence, including mobility, analytics, cloud, broadband and social networks.

The mobile device has become a pivotal driver in creating a dynamic marketplace that is bringing diverse companies and sectors together, both as competitors and collaborators and across traditional boundaries of industry and technology. Such changes have expanded the possibilities for new products, services and types of companies in this emergent commerce environment. The mobile device has introduced unique qualities such as the portability of the technology and additional factors inherent to the mobile device, including multimedia services, GPS, Internet access, mobile telephony, camera, and social media, which could all impact the payments environment.

In the retail payments space, these dynamic changes have created a market that offers digital and mobile wallets, near field communication (NFC) and cloud-based point-of-sale (POS) solutions, mobile apps, and Quick Response (QR) barcodes. The merging of these technologies with platforms (POS, online, other remote), uses (consumer-to-business (C2B), person-to-person (P2P)), new payment methods (virtual prepaid, direct carrier billing (DCB)), and many cross-industry players further changes the market for

---

[2] Use of the MPIW in this paper represents the existing workgroup or a modified version of the group in the future. The original MPIW included 22 members, representing various mobile payments industry sectors, and now has 42 members, including several merchants. MPIW member information can be found at http://www.bostonfed.org/bankinfo/payment-strategies/mpiw/index.htm.

[3] http://www.bostonfed.org/bankinfo/payment-strategies/publications/2011/mobile-payments-mapping.htm.

mobile payments. Large banks are collaborating through joint ventures, partnerships, consortiums, and bilateral relationships with mobile network operators (MNOs), card networks, retailers, mobile solution providers, and well-funded innovative start-ups to implement numerous mobile payment solutions. In some instances, stakeholders are experimenting with multiple approaches to see what consumers will use, and what merchants will accept.

These rapidly developing innovations in the mobile payments landscape created the need for the FRB and MPIW to update the original white paper to inform the payments industry concerning the evolution of a ubiquitous mobile payments system. The new report reflects what the FRB has learned from the MPIW, with the intent that it could inform policymakers and regulators, as well as the mobile payments industry.[4] The key findings note that while the mobile landscape remains characterized by fragmentation, various developments have gained importance. These include the convergence of channels, the role of nonbanks, the formation of new relationships, the unresolved security and privacy issues, and the increasing role of data monetization. As this ecosystem matures it will challenge new entrants in their ability to achieve scale and sustainability, while technology will continue to proliferate and drive improved efficiencies and innovation. The need for interoperability, industry guidance, and standards will become even more critical to ensure a secure and cost-efficient ecosystem. Creation of an open model could become a means to a secure an interoperable mobile payment system capable of building scale through consumer and merchant adoption. However, in this competitive and rapidly innovating market, new solutions have not waited for a uniform open model to become available.

Based on these findings, the MPIW updated the original strategic principles and introduced new themes. The paper expands on the benefits and challenges marking the landscape in light of recent developments and examines earlier considerations to determine if they are still relevant based on the many changes in the mobile payments marketplace. Finally, the paper revisits the long-term vision for POS mobile payments, including risk and regulatory concerns, along with implications for all stakeholders.

II. Changes in the U.S. Mobile Payments Ecosystem: 1Q2011 to 4Q2012

This section provides an overview of the accomplishments and challenges faced by primary mobile stakeholders over the last two years and outlines new infrastructures and capabilities offered in this span of time. The discussion includes the following stakeholders: MNOs, smartphone/terminal manufacturers,

[4] This paper provides the MPIW's assessment of the state of the U.S. mobile payments industry, but does not reflect any agreement among the MPIW members as to the manner in which mobile payments may be transacted.

mobile operating system providers, payment processors, alternative payment service providers, card and ACH networks, financial institutions (FIs), merchants, regulators and consumers.

MNOs

In the last two years, MNOs have partnered with banks, card networks and technology companies to pilot mobile payment solutions. New business models have emerged more quickly than some MPIW members had originally expected. For example, three of the largest MNOs formed an NFC mobile wallet joint venture (Isis) with several FIs and a card network. Sprint partnered with Google and Citi to launch Google Wallet.[5] Because MNOs typically subsidize and certify handsets on their networks, they have maintained control over which service providers can access the secure element[6] on mobile phones in their networks, although not without consequences to mobile service providers and ultimately to consumers by limiting their access in some cases.[7]

The mobile carrier's approach has some historical context. Before Apple and Google introduced their smartphone platforms and app stores, mobile subscribers were limited by their MNO in terms of applications that could be downloaded to their mobile phones and how the apps could be purchased (a.k.a. the "walled garden"). The introduction of app stores managed by Apple and Google, and the quick consumer acceptance of these app stores changed this mobile app dynamic. These factors reduced the MNOs' leverage and control of software on the handsets and gave customers options and capabilities that were unavailable through the MNO ecosystem.

Smaller mobile carriers have yet to engage in POS mobile payments, but some are exploring opportunities to address the needs of the unbanked and underbanked consumer markets with prepaid phones, mobile financial services, and other innovative use cases.

Smartphone/Terminal Manufacturers and Mobile Operating System Providers

The Google Android and Apple iOS mobile operating systems continue to have the largest share of smartphone subscribers, with 52.3 percent and 37.8 percent respectively.[8] While few mobile phones are currently enabled for use with either SIM or embedded NFC secure elements, more handset manufacturers are including these capabilities as a basic component. At the end of 2011, 45 global

---

[5] Google Wallet is a partnership between Sprint, Google, Citibank and MasterCard. Isis Wallet is a consortium comprising AT&T, Verizon, T-Mobile, Chase, Capital One, Discover, Barclaycard, Visa, MasterCard and American Express.

[6] A secure element is an encrypted smart card chip embedded in a mobile phone that safely stores and executes mobile payment applications and stores associated payment credentials and financial data.

[7] At this time, only selected Android phones work with the two wallets. The Apple iPhone is not NFC-enabled.

[8] As of the date of this publication. See http://gigaom.com/2013/03/06/comscore-android-still-top-us-smartphone-os-but-iphone-top-smartphone-and-ios-gaining/.

handset manufacturers announced plans to add NFC/SIM cards to their mobile phones,[9] and Isis planned to have up to 20 NFC-enabled mobile phones available by the end of 2012.[10] Assuming that MNOs activate NFC in the handsets, these efforts could begin to alleviate some barriers to adoption of NFC mobile payments.

Early industry expectations assumed that the majority of POS terminals would have been upgraded to accept contactless NFC payments by 2013. For several reasons this has not been the case. The three big terminal manufacturers, Verifone, Ingenico, and Equinox, have incorporated NFC functionality into their new POS terminals, but merchant implementation has been slow.[11] Rolling out new hardware to enable NFC on every POS terminal, changing POS software, and upgrading POS terminals to support NFC is not only costly, but also an operational challenge. While implementation of the Google and Isis NFC mobile wallets may have helped gain traction with some merchants, many others still must decide if and when to invest in upgrading their POS terminals to NFC.

Payment Processors and Alternative Payment Service Providers

Payment processors, online payment service providers, mobile software solution vendors, and application and hardware developers are exploring new market opportunities and innovations in the mobile payments space, ranging from digital wallets to dongle plug-in smartphone card readers. They continue to provide the enabling technology for mobile payments or to serve as intermediaries in the payments supply chain.

Google's first mobile wallet stored payment credentials issued by Citi MasterCard in a secure element embedded in the mobile phone. Google adapted its business model in response to limited transaction volume and introduced a hybrid mobile/digital wallet that stored a virtual MasterCard number associated with the mobile phone in the secure element. The virtual card does not correspond to any specific payment card account, but is a proxy for the real account credentials stored in the cloud and is used for NFC transactions at the POS. This change enabled Google Wallet customers to store and pay with credit and debit card credentials issued by any FI. It also demonstrated Google's flexibility and capacity to adapt quickly to overcome barriers in the market. In contrast, FIs cannot adapt as quickly to market changes because of competing needs for resources and funding within their organizations, impacts to legacy systems, financial impacts to their interchange revenue, and regulatory requirements.

---

[9] GSMA announced at its Mobile Asia Congress that it has commitments from 45 MNOs worldwide to implement SIM-based NFC. See http://www.nfcworld.com/2011/11/16/311363/45-mobile-operators-commit-to-nfc/.

[10] See http://www.wired.com/gadgetlab/2012/10/isis-sets-oct-22-launch-date/. The Isis Wallet uses a SIM-based secure element; Google Wallet uses an embedded secure element.

[11] See http://gigaom.com/2011/03/04/verifone-all-new-point-of-sale-terminals-will-get-nfc/ and http://www.finextra.com/news/fullstory.aspx?newsitemid=23494.

Apple took a different approach and chose not to deploy NFC for the iPhone. Instead, Apple created a non-payment app-based mobile wallet called Passbook that serves as a repository for boarding passes, movie tickets, retail coupons, and loyalty cards. Passbook provides a platform that supports third-party integrations, including digital wallet providers, for a closed-loop network of merchants. It enables customers to select, download and store QR codes from registered merchants' apps and access them as needed to pay at the POS or at a barcode scanner. By storing non-payment accounts on their mobile phones consumers can reduce the need to carry paper or plastic.

The convergence of online, mobile, and physical POS channels has provided alternative payment providers with the opportunity to develop solutions and applications that leverage a range of technologies, such as cloud, QR codes, and geo-fencing.[12] Unlike NFC, cloud-based and QR code technologies are less dependent on mobile carriers because they rely on software that does not store payment information on the mobile device, and therefore does not require access to the mobile network. However, Internet access is typically necessary to complete a transaction.

Payment Cards and ACH Networks

Credit: The major U.S. credit card networks face growing competition from other mobile stakeholders. They continue to actively pursue multiple mobile payment efforts to gain market share. In recent years, the card networks have introduced a variety of strategic initiatives and acquisitions that demonstrate the importance they place on mobile in both developed and developing countries. They have leveraged their ability to connect services through their standardized global networks. They have formed strategic partnerships with MNOs, issuers, merchants and mobile payment technology vendors, as well as investing in mobile start-ups. They have been complementing plastic cards with mobile payments at the POS, with prepaid, transit, and P2P. A notable change over the past two years is their new focus on cloud-based digital wallets and merchant loyalty programs. And, while following different strategic paths to implementation of mobile payments, the card networks continue to promote and support NFC, approving more NFC mobile phones for their services globally, participating in the Google and Isis mobile wallet programs in the U.S., and engaging in NFC initiatives in Europe and Asia.[13]

---

[12] In the cloud model, payment credentials are stored in a remote file server (cloud), not in the secure element in the mobile phone. In one use case, a consumer registers and then pays for purchases by entering his mobile phone number and PIN at the merchant POS terminal. Some cloud-based digital wallets use location-based technology in the mobile phone. Geo-fencing leverages location-based services (such as GPS and RFID) to create a virtual perimeter in which a mobile device can be recognized and a notification generated. For example, Square uses geo-fencing to notify a merchant when a customer has entered the store.

[13] According to one mobile payments stakeholder, "NFC is still the fastest, quickest and best user experience. It is the least clunky and works in different environments with no connectivity. NFC is fit for the purpose, which is NFC payments." James Anderson, SVP Mobile, MasterCard, *NFC Times*, November 7, 2012.

Debit/Prepaid: Debit card networks are experiencing growth in mobile payment transactions processed through virtual prepaid access accounts, prepaid card systems and online payment providers. Online and mobile prepaid options offer the unbanked and underbanked access to financial services without requiring a traditional bank account. Two recent major prepaid initiatives include Green Dot, which in 2012 purchased a bank and introduced its GoBank account,[14] and Bluebird, a digital/mobile prepaid account offered by American Express and distributed through Walmart.[15] As prepaid products grow, the Consumer Financial Protection Bureau (CFPB) and other regulators will continue to monitor their progress because of concerns about excessive fees and lack of transparency for consumers regarding such fees and other card usage terms and conditions. Any potential regulatory actions should be evaluated to determine their impact to the growth of prepaid debit accounts and the prepaid debit model for mobile payments.

ACH: ACH is a major payment network that competes with card networks in the United States. Only recently have mobile ecosystem stakeholders begun to actively consider ACH as a viable alternative in the mobile/digital wallet evolution. Use of the ACH network for mobile payments continues to grow as a segment of online ACH payments. Currently, the majority of these transactions are comprised of bill payments. FIs and non-bank payment providers are developing Internet and mobile applications to implement P2P payment products that are processed via the ACH network, creating opportunity for future growth as more consumers use their smartphone apps and browsers for mobile P2P and Internet purchases. Several companies in the mobile payments ecosystem are pursuing solutions that leverage the ACH network to clear and settle mobile payments and offer ACH to consumers as an alternative payment method for retail purchases. This use of the ACH at the POS also responds to merchant demands for less costly alternatives to credit and debit. Ultimately, the ACH will be another component for expanding consumer choice in the future, particularly for recipients of electronic benefits and transfers (EBT) and other government benefit payments.

Financial Institutions

FIs face many competitive pressures from other banks and nonbanks, particularly as the banking industry tries to determine its role in the fast-paced mobile payments environment. FIs' current moderate

---

[14] GoBank is an FDIC-insured mobile-only bank that is accessible using a mobile app. It includes a Visa debit card linked to a traditional checking account, but it does not issue checks. GoBank has been available in limited launch since January 2013. See www.gobank.com.

[15] Bluebird is an FDIC-insured alternative to debit and checking accounts that can be linked to a mobile app which allows consumers to make mobile deposits to their prepaid account, make mobile bill payments, or send P2P payments. See www.bluebird.com.

approach to implementing mobile payment solutions stems from the economic consequences, uncertainty, and risk aversion created by the recent financial crisis and in response to broad financial regulatory reform. The largest FIs have taken different, but overlapping, strategic directions and approaches to building their business models. A few have participated in NFC wallet initiatives through collaboration with card networks and MNOs. Beyond NFC, FIs have also formed relationships with start-ups to test other mobile payment solutions such as cloud-based digital wallets, QR codes and mobile device card acceptance applications for small businesses. Financial institutions are simultaneously expanding their mobile banking platforms to include mobile remote deposit capture (mRDC), P2P payments, and corporate mobile banking services. P2P payments have helped FIs expand their role as a facilitator of mobile commerce by enabling money transfers between FIs or through retail payment networks.[16]

Financial institutions have the chance to leverage their reputation as trusted payment providers and effective risk managers to strengthen their role in the mobile payments ecosystem. Various studies have shown that consumers have more trust in mobile payment solutions driven by FIs and/or credit card companies than alternative providers.[17] Financial institutions have broad experience that puts them at an advantage to drive and shape consumer acceptance – from due diligence, know your customer, authentication and authorization, corporate security, fraud monitoring and prevention tools, risk management policies and systems, to anti-money laundering tools. Partnering with viable nonbank mobile ventures can complement the FIs' strengths and generate innovation, technology and a better understanding of the market dynamics. Strong customer marketing and communication efforts can also help FIs succeed in the mobile space. However, if FIs cannot leverage their unique advantage as the trusted entity for consumer mobile payments, they risk being viewed by other participants simply as a utility that provides the transactions.

Merchants

Since the inception of the MPIW, merchants have expressed concerns related to the overall business case for mobile payments. Their concerns stem from the expanse of costs in comparison to the benefits of rolling out mobile contactless payments. These costs include, but are not limited to, processing, investment in terminal upgrades, chargebacks from card payments, security (including PCI compliance),

---

[16] Examples include clearXchange, a network between Bank of America, Wells Fargo and Citi that allows customers to send and receive P2P payments electronically, and Fiserv's PopMoney.

[17] Javelin Strategy & Research (March 2012). *Gang of Four (and Possibly Five) Apple, Google, Facebook, Amazon – and PayPal: Positioning for Payments in the New Mobile-Social Technology Era* and 2011 Fiserv Consumer Trends Survey. *Beyond Mobile Banking: It's Time to Stake the Claim for Mobile Payments*. Retrieved from http://www.flickr.com/photos/fiserv/6153751056/in/photostream.

and EMV implementation. [18] [19] In addition to cost considerations, merchants are concerned about rules and liability shifts that vary depending on how a payment is handled, for example, whether a transaction will be processed as card-present (CP) or card-not-present (CNP). As such, merchants of all sizes (e.g., big box retailer, quick-service restaurants (QSRs), small and micro-businesses), and across various segments, are experimenting with different mobile payment technologies to build cost-efficient POS solutions that enhance customer experience and lower costs.

Several retailers are offering closed-loop prepaid account solutions using QR code applications to make mobile payments. QR codes are non-proprietary and relatively quick and easy to implement. However, a customer still needs a custom app and QR code for each merchant or group of merchants, who must agree to a common set of technology standards and/or a common app. Recently, over 30 of the leading U.S. merchants formed the Merchant Customer Exchange (MCX)[20] to create a secure mobile platform with a common set of standards to reduce costs in the payments system, keep merchants' customer data securely with merchants, and provide their customers with a better shopping experience. According to public statements, the MCX solution will utilize barcode technology (i.e. QR codes) for mobile proximity payments.

Many QSRs are heavily franchised making it difficult for them to implement uniform payment solutions. However, several chain QSRs and drug stores that initially deployed NFC terminals to accept contactless cards are now leveraging those terminals to accept NFC mobile payments.
Merchants are generally positive about the business case for mobile, but regard it as a more holistic development of which payments is a small piece. Merchants see mobile as an opportunity to introduce competition and innovation in the payments market.

---

[18] EMV is a global specification for credit and debit payment cards based on chip card technology that defines requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities. The EMV specification encompasses credit, debit and contactless (card and mobile) payment transactions. The primary use for these chip-based cards is to perform payment transactions that store encryption data for authentication. As part of the transaction authorization, the card uses the data to prove it is authentic, thus preventing the use of stolen or cloned cards. For more information on EMVCo see http://www.emvco.com.

[19] U.S. EMV migration plans accelerated between mid-2011 and early 2012 when all four major card networks announced plans to migrate U.S. merchants and issuers to a more secure EMV chip payment environment – merchant acquirers must be ready by April 2013, liability shift for POS as of April 2015 and for automated fuel dispensers as of October 2017

[20] At the time of publication, MCX included the following merchants: 7-Eleven, Alon Brands, Bed Bath & Beyond, Best Buy, CVS/pharmacy, Darden Restaurants, DICK's Sporting Goods, Dillard', Dunkin' Brands, Gap, HMSHost, Hobby Lobby Stores, Hy-Vee, Lowe's, Meijer, Michaels Store., Publix Super Markets, QuikTrip, Sears, Sheetz, Shell Oil US, Sunoco, Target, Wakefern Food, Wal-Mart and Wawa.

Consumers

Growing smartphone ownership will influence stronger adoption of mobile banking and payments.[21] As consumers become increasingly adept at using smartphones (e.g., through downloading and using applications), this will likely lead to an increase in consumer mobile commerce activities, (e.g., using mobile phones to search the Internet for product reviews and comparing prices) and mobile banking. Use of mobile banking and related mobile financial services products builds trust and awareness, and contributes to the willingness of consumers to try emerging mobile payment offerings.[22]

Mobile payment services can also help unbanked and underbanked consumers who have access to mobile phones. Fifty-nine percent of individuals who are unbanked have access to mobile phones, and 50 percent of these phones are smartphones. Notably, 90 percent of the underbanked have mobile phones, 56 percent of which are smartphones. Both of these groups have a higher percentage of smartphone ownership than the general population.[23] For many of these users, their smartphones represent their primary connection to the Internet. They can use their smartphones to reload their mobile accounts, make purchases, deposit checks, and pay bills, alleviating expensive check cashing services and ATM fees.

The growing ubiquity of mobile commerce, coupled with the expanded functionality and greater convenience of smartphones, provide the framework for driving consumer mobile payment behavior. However, the primary barriers to adoption remain the limited availability of some technologies (e.g., NFC) and concerns with security and privacy. Substantial educational outreach and awareness by the industry is required because consumers will play a critical role in driving mass adoption of mobile payments and will likely dictate the sustainability of mobile solutions in the long-term.[24]

Regulators

Mobile payment instruments use the existing payments infrastructure in different ways. Some mobile payment solutions clearly fall under the scope of existing regulations, while other alternatives using new

---

[21] Pew Research reports that smartphone ownership in the United States is at approximately 46% and growing, while feature phone ownership is at about 41 percent.

[22] Javelin Strategy & Research (2012, September). *Battle for Control of Mobile Wallet* estimates that over 60% of consumers using mobile banking are likely to adopt a mobile wallet in the next 12 months. Forrester (2012). *State of Mobile Banking 2012*, forecasts that the number of mobile bankers in the U.S. is expected to double by 2017.

[23] Gross, M. B., Rock, A.M., and Schmeiser, M.D. (2013, March). *Consumers and Mobile Financial Services 2013*. Board of Governors of the Federal Reserve System. According to the FDIC's *2011 National Survey of Unbanked and Underbanked Households*, 8.2 percent (almost 10 million) of U.S. households are unbanked and 20.1 percent (24 million) are underbanked.

[24] For more information on consumer adoption of mobile payments, see Elisa Tavilla. (July 2012). *Opportunities and Challenges to Broad Acceptance of Mobile Payments in the United States*. Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/opportunities-and-challanges-to-broad-acceptance-of-mobile-payments.htm.

technologies (e.g., NFC, QR code) may not have an obvious fit and require a better understanding before regulations might be prescribed. Mobile payment stakeholders perceive that regulators have not kept pace with mobile payment innovation and that the industry would benefit from more specific guidance and a legal framework for mobile payment providers. While industry participants acknowledge the applicability of current regulations and laws to underlying payment methods (credit, debit, prepaid, and ACH) that govern mobile payments today, they are concerned over the uncertainty related to coverage and liability responsibilities and a need for enhanced coordination among regulatory bodies. Financial institutions and related organizations also express concern for participation by nonbanks, including MNOs and alternative payment providers which may be less familiar with payment banking laws (e.g., BSA/AML, KYC, state money transmission licensing, risk compliance, and consumer protection).

The MPIW and representatives from several regulatory agencies[25] met in April 2012 to discuss issues, concerns, and potential gaps in regulatory coverage. The primary concerns they raised were focused on consumer protection, privacy, and data security; however, neither the regulatory agencies nor industry stakeholders concluded that there was an immediate need for additional regulation. Rather, they expressed support for clarification of existing regulations and their applicability to mobile payment service providers in order to increase understanding at the policy level, dispel misperceptions, and focus collective energies on potential risk vulnerabilities in the mobile channel. It was suggested that stakeholders focus on education and communication between the industry and the agencies, while regulators ensure that industry stakeholders are informed if and when the need for mobile regulation arises.

Given Congress's high level of interest in mobile payments and attention to the MPIW's initial white paper and ongoing work, several Federal Reserve, MPIW, and other mobile payment industry experts testified at House and Senate hearings in 2012. The House Financial Services Subcommittee on Consumer Credit examined the growing trend of mobile payments at a hearing held on March 22, 2012.[26] On March 29, 2012, the U.S. Senate Committee on Banking, Housing, and Urban Affairs held a hearing,

[25] Regulators included the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Consumer Financial Protection Bureau (CFPB), National Credit Union Association (NCUA), Federal Reserve Board (FRB), Conference of State Bank Supervisors (CSBS), Washington State Department of Financial Institutions, Massachusetts Division of Banking, Federal Trade Commission (FTC) and Federal Communications Commission (FCC).

[26] Panelists included Rich Oliver, formerly Executive Vice President and director of the Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, and representatives from PCI Data Security Standards Council, MasterCard, Smart Card Alliance and the Consumers Union. See http://www.c-span.org/Events/C-SPAN-Event/10737429273/.

"Developing the Framework for Safe and Efficient Mobile Payments,"[27] and held part two in July 2012.[28] Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System, testified on regulation of mobile payments before the Subcommittee on Financial Institutions and Consumer Credit, House Committee on Financial Services on June 29, 2012. She commented that current payments laws "may not be well-tailored to address the full range of mobile payment services in the marketplace."[29]

Summary

Each primary stakeholder in the mobile payments ecosystem has an innovative approach to how mobile payment capabilities can be rapidly and reliably developed and implemented. While their efforts have provided consumers with multiple options, they have complicated the development of interoperable standards for mobile payments and the widespread adoption of any one mobile payment solution. Given the fragmented and dynamic market, it is important for the FRB to regularly convene the mobile stakeholders and other parties, including regulators, to discuss the mobile ecosystem, especially as the newer solutions evolve.

III. Progress towards Achieving Benefits

At the end of 2010, the MPIW identified a number of clear benefits of a future U.S. mobile payments infrastructure that was built on an NFC contactless technology platform. This section evaluates progress towards achieving benefits such as improved security and fraud reduction, merchant cost efficiency, competitive technologies, value-added services, revenue and monetization opportunities, and data privacy, in light of environmental developments in the ecosystem.

Improved Security and Fraud Reduction

The planned migration from today's mag-stripe environment to more advanced technology introduces the potential for a more secure payments environment. In the first Mobile Payments Landscape paper, the MPIW acknowledged the potential for NFC/secure element technology, along with the intelligence and data storage capabilities of the contactless chip embedded in the mobile phone, to improve authentication

---

[27] See http://banking.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=eab14748-aea3-48f1-a4f8-88f49613f0e1

[28] Witnesses included professors and industry experts from the University of California, Berkeley, University of Indiana, and University of California, Berkeley School of Law.

[29] Witnesses included Sandra F. Braunstein, Director, Division of Consumer and Community Affairs, Board of Governors of the Federal Reserve System and Kenneth C. Montgomery, First Vice President and Chief Operating Officer, Federal Reserve Bank of Boston. See http://www.federalreserve.gov/newsevents/testimony/martin20120628a.htm.

and reduce the risk of fraudulent transactions.[30] However, it is too soon to attribute any actual fraud reduction or enhanced security to NFC chip technology or the applications and tools built into the mobile phone hardware in light of the slow growth of POS mobile payments. To further complicate the measurement of mobile-based fraud reduction, alternative mobile technology solutions which are simpler and less costly for merchants and FIs to deploy have emerged. Examples include QR codes and cloud-based solutions that can store and manage payment credentials remotely, possibly addressing some of the complexities associated with managing data in the secure element embedded in the mobile device.

The implementation of EMV chip technology in other countries has resulted in decreased card fraud and is predicted to reduce mobile payments fraud in the future. Most developed countries have already converted to EMV industry specifications, while the U.S. migration is in the early stages. EMV is important to the security of NFC card-based mobile payments because NFC uses the underlying EMV technology infrastructure, and relies on the same dynamic data authentication (DDA)[31] for mobile payment security. Despite the leadership role of the credit card networks in driving U.S. migration to EMV card payments, they do not agree on the cardholder verification method, generating a debate about the level of risk of chip-and-PIN vs. chip-and-signature.[32]

While consumer behavior surveys report that privacy and security are consumers' most important concerns, in actuality they use their mobile phones to interact quickly with websites, businesses, and other people, valuing their ability to access social media. Problems stem from consumer failure to adopt available safeguards such as PINs, passwords, device lock features or anti-virus software. They also continue to engage in risky behaviors such as opening spam emails and jail-breaking phones, behaviors that will require change if a wallet containing payment credentials is added to the mobile phone.

Mobile applications downloaded to the handset can expose payment platforms and networks to fraud and other security risks. The vulnerability posed by mobile applications is largely attributable to a lack of industry standards. This situation is somewhat mitigated by moderating oversight from Apple and

---

[30] Despite anecdotes claiming that NFC data can be intercepted as the device communicates with a terminal, momentarily exposing data in transmission or by other sophisticated hacking schemes, the only reported breaches have occurred in lab settings, with none reported in the real world.

[31] DDA uses an encryption key to generate unique, dynamic data values to authenticate the transaction when it is authorized by the card network. These values are only valid for one authentication. If a thief tries to re-use the payment account data, it will be out of sync with the number stored by the card issuer and rejected, making it harder to skim usable data and clone for counterfeiting

[32] MasterCard supports Chip and PIN as the most secure payment technique to provide the greatest protection against fraud liability to retailers and acquirers. Visa supports a range of cardholder verification methods (CVMs) with EMV chip, including signature, online PIN and no-signature for low-value, low-risk transactions. American Express also supports a range of CVMs with EMV contact chip, including signature, online pin and no-signature for low-value, low-risk transactions.

Google of their app stores. However, many smaller app stores operate independently in the mobile ecosystem, with little to no oversight. The major operating systems approach security very differently, with Android and its open platform characterized as the "Wild West" and Apple as the "Frontier Fort."

As mobile payment transaction volume increases, the mobile payments channel is expected to become a more attractive target for criminals. Security providers need to anticipate risks and incorporate automated mitigation tools where feasible, such as preloading mobile antivirus software on phones, and leveraging the ability of mobile phones to share real-time data (e.g., location and customer-entered authentication). The mobile device has a number of security attributes that have the potential to make the mobile channel more secure than the online channel against fraud and to repel fraud attacks.[33]

Many parties are involved in supporting the multi-faceted mobile payments ecosystem. All share in the responsibility for mitigating mobile payment security and fraud problems. The industry must collaborate to identify potential threats and vulnerabilities in the mobile payments ecosystem, to share applicable data, to assess the security gaps in the mobile process, and to assign responsibility for remedying these gaps. They must also develop interoperable standards, guidelines and rules for newer technologies. The MPIW is vested in recognizing and/or developing industry-wide solutions to the security challenges presented by mobile commerce and can leverage its expertise to: (1) identify evolving threats and vulnerabilities that exist for mobile; (2) address the need for stronger authentication; and (3) advance security awareness among consumers and industry stakeholders in the mobile payments ecosystem. Mobile has the potential to provide a safer payments option if leveraged appropriately.

Merchant Cost Efficiency

While merchants would like to use mobile payments as an opportunity to achieve efficiencies, impediments exist. For example, the traditional card model treats mobile contactless payments as card-not-present, but a shift to treating such transactions as card-present instead would reduce merchant costs. Applying mobile wallet fees is another example that may inhibit innovation and add incremental costs. A number of large and small merchants are still participating in NFC-wallet pilots, but without a strong

[33] These attributes include context, tactile interface, sensors, cloud and social media. Geo-location can be used to enhance authentication and detect fraudulent charges. Technology is emerging that will leverage the sensory features of swiping or sliding across mobile device screens or to authenticate signatures via their touch screens. The tactile interface also opens up the possibility of fingerprint verification for financial transactions or account logins. Other features include the camera functionality which can authenticate users through facial recognition. All of these attributes can be layered to enhance security and authentication. Camhi, Jonathan (2012, October 26). Why mobile will be more secure than online banking. *Bank Systems & Technology*. Retrieved from http://www.banktech.com/channels/why-mobile-will-be-more-secure-than-onli/240009653?pgno=1.

business model, and ability to reduce the cost of deployment, merchants continue to investigate lower-cost alternatives that are not card-based and not supported by NFC.

Migration to EMV is also impacting merchant cost efficiencies because it requires investments to upgrade terminals. Merchants must weigh the investments against the risk of liability responsibility for counterfeit fraud associated with mag-stripe data breaches and the benefit of reduced fraud. The MCX model could help to reduce merchant deployment costs by clearing and settling over a lower cost network such as ACH, rather than over the more expensive card networks.

Cloud-based payment services may offer merchants cost-effective and rapidly deployable capabilities. Often cloud-based technology leverages barcode technology and card tokenization to further reduce the likelihood and costs of dealing with fraud. Tokenization is a technology that enables the payment service provider to exchange a one-time payment token at the merchant's e-commerce or POS system to redeem for payment. On the other hand, barcode technology is a more feasible solution to other mobile payment technologies from a customer integration perspective. Several mature and start-up companies offer cloud-based payment solutions – which initially serviced small merchants, but are expanding to larger retailers. Some of these companies are incenting mobile payments with lower fees and loyalty programs.

As merchants develop their strategies for mobile payments, they must consider multiple options related to hardware, software, choice of technology platform, and how they implement external factors (e.g., EMV). Some industry stakeholders hope that the inclusion of NFC capability in POS terminals upgraded for EMV may encourage merchants to adopt mobile contactless payments at the POS. However, merchants still incur incremental costs to enable NFC and view implementation of EMV and use of NFC for mobile payments as two distinct investment decisions. For EMV, merchants want assurances that their investments are in sync with issuers and mobile operators.[34] For mobile payments, merchants must do a cost-benefit analysis on whether to buy an NFC-enabled terminal, whether to enable NFC functionality, and what payment brands to accept.

Competitive Technologies

The current mobile payments ecosystem depicts a fragmented market, rather than a cohesive interoperable mobile payments approach. The various emerging technologies have the potential to benefit the payments systems by improving overall efficiency and security in the long-term, and the end result will

[34] Randy Vanderhoof, interview with Payments Source, September 2012. The *EMV Migration Forum* was created in September 2012, under the leadership of Randy Vanderhoof, president of the SmartCard Alliance. The primary role of the Forum is to prepare merchants, acquirers, issuers and processors for the pending conversion to EMV smart card technology in the U.S.

likely include several competing models that could be categorized broadly as cloud-based or NFC-like. These systems will eventually co-exist and may be selected for payments based on their venue and risk profile. For example, QR codes may work well for micropayments in a closed-loop proprietary payment system. NFC solutions may be best applied in cases that require enhanced security features such as transit, where speed and convenience of processing a high volume of transactions is necessary.

Value-Added Services

Retail: The mobile payment and commerce landscape is opening doors for innovative value-added services that enhance mobile payments. Such services can be provided before and after the actual payment transaction. These services are instrumental to offering relevant and timely information to customers, increasing the likelihood of generating additional sales, strengthening brand loyalty, and offering additional points of interaction with the customer. Both NFC mobile and cloud-based digital wallets can allow for the generation of customized coupons, timely discounts, and loyalty and reward program tracking and redemption directly from the mobile device. Value-added services are becoming more important than the actual payment transaction for driving mobile payment adoption. For sustainability, the value proposition of mobile commerce will need to include concrete value-added services beyond payments.

The ability to collect and analyze information on consumer preferences and buying habits tied to mobile payment transactions may enable customized promotions and rewards, but may also present risk to the customer's transaction information if not managed properly. A driving force behind collection of the data is the desire for enhanced data monetization by the data owners (e.g., FI, card network, merchant, MNO, payment service provider), who want to leverage their data to increase profit and efficiency, improve customer experience, and build customer loyalty. Competition over data ownership and its subsequent use exists, and stakeholders will need to agree on how to protect, share and present the data, subject to customer preferences.

The concept of a mobile or digital wallet can create a convenient and efficient tool for the consumer in the long-term. Initially consumers may be frustrated by limited payment choices included in the wallet, and by providers flooding the market with wallet offerings to attempt to gain market share. Research by TSYS and Mercator Advisory Group shows that consumers wish to consolidate their store loyalty and rewards cards in the mobile phone, and want to pay for purchases with their preferred payment method in a mobile wallet.[35]

[35] TSYS and Mercator (2012). *2012 Consumer Debit Payment Choice Research Study*.

Transit: The benefits of mobile contactless payments for mass transit are starting to emerge. Some U.S. transit systems are exploring opportunities to leverage open-loop card networks for transit payments. Contactless chip payments, particularly in the mobile channel, provide a use case for interoperability, lower operating costs through reduced transit fare card issuance expense, and increased acceptance to address the myriad of different payment acceptance systems for transit authorities across the U.S. Today, most of the largest U.S. transit systems are already invested in smart card systems for more flexible and efficient revenue collections. A transition from proprietary transit-only systems to open-loop NFC contactless payments represents an opportunity for even greater efficiency, reduced operational costs, and enhanced consumer convenience. The 2012 Isis mobile wallet launch in Salt Lake City with the Utah Transit Authority is an example of one of the first commercially available mobile payment transit programs in the U.S. In October 2011, Google Wallet conducted a NFC mobile payments trial with the New Jersey Transit Authority for NFC.

Revenue and Monetization Opportunities

New nonbank players and the conjoining of industries unaccustomed to partnership are disrupting payment models, as mobile emerges as a new payment vehicle. The new models are evolving without one standard approach dominating the playing field, making it difficult to achieve revenue goals. Mobile advertising with customized, promotions-based consumer shopping behaviors represents a new source of revenue. The Google Wallet business model is built primarily on gathering of user data and subsequent advertising, in contrast to the Isis wallet model, which provides a neutral, fee-based platform on which bank issuers load their credit, debit, and prepaid cards. Three of the top U.S. mobile carriers (AT&T, Verizon and T-Mobile) invested in the Isis joint venture receive a share of revenue from card issuers for wallet payment transactions, together with rent paid by the issuers to add their customers' cards to the secure element. The revenue potential and cost implications associated with the rent model are unforeseen, particularly given that participation in the Isis wallet is currently limited to three financial institutions (Barclaycard, Capital One, and Chase).

New solutions will be developed in response to the need for business models that meet the expectations of all stakeholders in the ecosystem. The variety of payment solutions may advance new schemes for revenue and cost-sharing that benefit customers and merchants.

Data Privacy

The MPIW focused considerable attention on the need for data privacy in the mobile channel, recognizing that the success of the mobile payment ecosystem hinges on trust and transparency. Similar to other channels, mobile can expose payments data to new parties and create the opportunity for data to be compromised. While the rewards resulting from data monetization may benefit the consumer, misuse of

the data may create serious privacy considerations if the consumer's payment or personally identifiable information (PII) is used without the consumer's explicit consent (e.g., opt-in) and lead to potential harm and unintended consequences.

Privacy risks are heightened with data monetization in the mobile payments space. The use of location-based services (LBS) by merchants and payment service providers to drive active and passive mobile marketing efforts has also heightened the concerns around privacy. While it is expected that consumers must register and/or opt-in to the application to allow it to use their location information, they may unknowingly allow companies to compile detailed profiles of their lives. Some popular LBS-enabled tools lack clear and concise disclosures about personal information collection, how that data is used, and the process for consumer consent.

In response to concerns over privacy risks in the mobile commerce environment, the FTC issued its Final Privacy Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*,[36] in March 2012, and the Obama Administration released its Consumer Privacy Bill of Rights.[37] While these reports are guidelines, any well-publicized incidents of privacy intrusions could result in legislative or regulatory action.

IV. Update of Original Strategic Principles

The purpose of the initial paper was to inform the FRB and other interested parties of the MPIW's assessment of the foundational principles intended to guide the development of an integrated end-to-end mobile payments process that could promote successful adoption. At the time, MPIW members supported rapid achievement of these principles to advance the realization of the benefits of mobile payments. However, the last two years have witnessed considerable change in the market and the business models, while NFC mobile payments have not evolved as quickly as originally predicted. Cloud-based and other innovative technologies, coupled with new market entrants and creative partnerships, have changed the dynamics of the mobile payments ecosystem, calling for a re-evaluation and modification of the MPIW's original strategic principles.[38]

---

[36] Available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[37] In the report, the White House proposed legislation based on the privacy principles it contained and called on the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to convene stakeholders to develop enforceable codes of conduct implementing these principles for specific industries. The NTIA has since held a series of multi-stakeholder workshops to develop voluntary codes of conduct to protect users' privacy in specific business contexts.

[38] The following commentary presents policy propositions for the FRB's consideration and does not seek to influence competing technological or commercial models currently being developed in the industry.

Open Wallet concept has evolved to include both mobile and digital wallets

The successful model for an open mobile wallet has not changed; however the initial concept of a mobile wallet has expanded into a digital wallet. Two years ago, the MPIW's definition of a mobile wallet was focused on NFC contactless technology which would store payment credentials, coupons, rewards, and other value-added features in the secure element in the physical mobile phone. In contrast, a digital wallet leverages cloud computing (i.e. remote servers) and wireless networks to enable proximity and remote mobile purchases and bill payments, without requiring secure financial data to be embedded in the mobile device. In a digital wallet, a payment may also be transacted without the physical presence of the mobile device by using a mobile phone number and a PIN/password at the POS. Although the NFC/secure element solution remains a viable option, cloud-based mobile services also provide secure storage and access to payment credentials, without the limitations inherent in a hardware model. The open wallet will likely evolve to include some components of NFC with the secure element and cloud, depending on consumer chosen functionality in terms of the type of payment and payment-related apps pre-loaded onto the mobile device, or via download through various app stores.

A true digital wallet is expected to be open and ubiquitous, accepted at most merchant locations, and across a multiplicity of different payment terminals. It should allow complete access by all consumers for various services, including transit, vending and ATMs. None of the current mobile or digital wallets truly meet this open standard, based on the original vision. Rather, current business models offered by major stakeholders are largely based on card platforms, with loyalty features. As long as wallet participation is bilateral, requiring exclusivity agreements that motivate other businesses to work independently to develop their own versions of the wallet, progress towards a true open wallet will remain slow.

Convergence of multiple technology platforms for mobile payments

Although NFC contactless mobile payments remain a key component of this principle, NFC is no longer viewed by industry stakeholders as the exclusive technology that will drive mobile payment adoption. It may gain ground when NFC-enabled phones and merchant terminals become widely available, but the slow pace and cost of NFC implementation has led to the pursuit of alternative solutions and technologies among industry stakeholders.

Currently, support for and opposition to NFC varies widely across stakeholders in the mobile payments ecosystem. Some stakeholders are hedging their bets by finding opportunities to implement complementary and/or competing mobile payment schemes where the alternative mobile payment method may be more cost-effective and more suitable to a certain venue or service, until consumer demand for NFC reaches critical mass. Other stakeholders remain unconvinced about the viability of NFC as a business or technical platform for payments and are actively pursuing non-NFC solutions. Despite

reservations by some stakeholders and other market participants, NFC offers benefits that other mobile technologies may not. Unlike cloud and QR code technologies, NFC is standards-based for chips and the secure element. NFC is well-suited as a cash replacement for small dollar purchases. It can enhance opportunities for loyalty programs with two-way communication. Coupled with the secure element in the mobile device, NFC can process prepaid debit, electronic benefits and transfer (EBT), and transit payments, enhancing efforts for financial inclusion of the underbanked.

Establish a ubiquitous platform for existing and new clearing and settlement rails[39]

Existing clearing and settlement rails provide a sound foundation for mobile payments platforms and for mass adoption and consumer choice, without precluding the opportunity for new rails to emerge. Current mobile/digital wallet solutions are either leveraging existing rails or developing innovative ways to use them (e.g., ACH). One exception to the use of traditional payments rails is direct carrier billing (DCB), which charges mobile payments directly to the customer's wireless phone bill. This service is only being used for very small value digital content in the U.S.

Dynamic data authentication provides long-term integrity and security for transactions across all channels

Dynamic data authentication (DDA) provides a secure method for protecting user data such as cardholder and other sensitive data for card-based mobile contactless payment transactions. From a security perspective, EMV is important because it uses DDA to secure Chip and PIN payments and can further secure mobile contactless payments. NFC is an extension of EMV chip technology that adds a radio interface. POS terminals that are upgraded to comply with EMV specifications are capable of supporting the payment card brands contactless (NFC) payment applications and processing both contact (smartcard) transactions and contactless (mobile NFC) transactions, should merchants decide to enable that capability. At a minimum, U.S. merchants must upgrade their POS terminals to support EMV in order to avoid the liability shift for fraudulent card transactions.

Given the credit card networks' directive for EMV in the U.S., this principle has been updated to include migration to the EMV specifications and encouragement by the card networks of early adoption of this payment scheme to assist in strengthening the security of card and mobile payments, and to ensure stronger security of the payment system and enhanced protection of the payment transaction data.

[39] Existing rails include: credit, debit, ACH, prepaid and mobile carrier billing.

Develop and adopt a global interoperable platform in the U.S. for mobile payment standards and certification of payment methods, leveraging existing standards where possible

To accelerate the adoption of mobile payments in the U.S., mobile devices must work safely and securely, and be capable of performing payment functions consistently, regardless of the technology platform, application, wallet, or underlying payment method. Standards should be applied across mobile payment solutions through a platform that can ensure domestic and global interoperability of technology, process and security.

Certain components in the current mobile payments ecosystem are already standards-based. The most developed are global technical standards for NFC-based mobile payments and the associated secure element. Any mobile contactless payment form factor used via NFC at the POS should follow established contactless standards endorsed by the International Standards Organization (ISO) and NFC industry groups, such as Smart Card Alliance, NFC Forum, GSMA, and Mobey Forum.[40] In the U.S., mobile contactless payments employing computer chip security and NFC technology must be based on ISO standard 14443.[41] Minimum compliance requirements for adoption of NFC contactless payments should include dynamic data authentication, digital/mobile wallet contactless functionality, and inclusion of the secure element in the mobile device. Furthermore, the industry would benefit from further analysis of ISO 18092[42] as a potential extension of contactless payments to enable peer-to-peer communication in addition to card emulation achieved with ISO 14443.

NFC mobile payments must also be capable of supporting all payment methods and networks, comply with business rules and standards, and reside in a secure container in the mobile device to interface with mobile payment applications. Mobile stakeholders are working with solution providers to build NFC mobile payment platforms based on all three secure element options: SIM card, embedded NFC chip, and micro SD chip. While no one secure element option is dominant in the U.S. marketplace, the SIM card approach is more prominent in the global market.

---

[40] The NFC Forum develops NFC specifications for device architecture and protocols to ensure interoperability between conforming devices, while GlobalPlatform handles secure element specifications to support the development of internationally interoperable, multi-application NFC solutions. The GlobalPlatform scope includes setting specifications for securely loading confidential content (e.g. customer data) onto the card by external entities such as the Trusted Service Manager (TSM).

[41] ISO 14443 is an international standard that defines proximity cards used for identification, and the transmission protocols for communicating with it.

[42] ISO 18092 defines communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductive coupled devices operating at the center frequency of 13,56 MHz for interconnection of computer peripherals. It also defines both the Active and the Passive communication modes of NFCIP-1 to realize a communication network using NFC devices for networked products and also for consumer equipment.

For other components in the mobile payments ecosystem, standards do not exist. Mobile payments that leverage the cloud and QR codes do not have a standards framework. There are no defined end-to-end standards to support the efficient use and security of the mobile device, the actual mobile payment during the transaction process, and the provisioning of the mobile/digital wallet. Privacy and security standards related to downloadable mobile apps are needed. While control of the application marketplace by the operating system providers has been helpful, there is room for improvement in the development of consistent rules and security measures. With the exception of PCI, no consistent standards exist to guide the use of encryption and tokenization as tools to enhance mobile payment security.

Whether implementing NFC/hardware-based or cloud/software solutions, all U.S. mobile payments stakeholders support the principle of a safe and secure mobile payment transaction. While it may be premature to establish cohesive standards for mobile payments, it may be appropriate for a broad, organized effort in the U.S., led by the appropriate organizations and/or regulatory bodies, to engage mobile payment stakeholders in beginning to develop a high level set of principles and a common roadmap or taxonomy to sort out the different components for mobile payments. These principles should include an agreed upon set of interoperable standards that encompass mobile devices (smartphones), NFC chips, secure elements, cloud, QR codes and mobile applications. The standards (accredited or otherwise) must also support the provisioning and maintenance of credentialing, open interoperability, and related security and privacy concerns. The process should leverage the best of existing standards and rules, without diminishing future innovation for the benefit of consumers. The MPIW may be well-positioned to leverage collective industry expertise to identify the potential gaps in the current standards framework that could be addressed by best practices, guidelines and principles.

Neutral Trusted Service Managers (TSMs) should oversee the provision of shared security elements used in the mobile phone for an NFC solution

This principle was written to be deliberately broad, leaving the individual mobile payment providers to determine what TSM(s) to choose and how to utilize the TSMs to manage functions. For example, Google's TSM handles all the related services, while two TSMs (managed by the same company) support Isis, one for FIs and one for MNOs.

A TSM typically coordinates the technical and business relationships between multiple stakeholders, including MNOs and service providers such as banks, ticketing agencies and other public and private sector issuing authorities, to deliver and maintain end-user services on mobile devices. These functions include: providing end-to-end application security by authorizing access to the secure element as required by each of the stakeholders; and application lifecycle management, including over-the-air provisioning, personalization, activation, and deactivation of services and privileges.

Going forward, the MPIW may want to consider how interoperability, standards, and management of the digital wallet could be factored into the role of TSMs. The group should also discuss whether the time is right to broaden the TSM role for wallets in the U.S. to include other responsibilities such as customer service, certification of mobile payment applications and vendors, and how the TSM fits into the larger structure of the trusted intermediary.

Regulatory Clarity

Regulatory clarity continues to be a critical core principle. Some progress has been made towards industry understanding of the regulatory responsibilities and concerns related to mobile payments. The MPIW has primarily focused on enhancing communication between regulators and industry stakeholders and on monitoring current developments and education through conferences and other media. The MPIW and Federal Reserve will continue dialogue with regulators to clarify oversight responsibilities, help create regulatory guidelines for security and privacy, and develop business standards and best practices.

Understanding the Role of Nonbanks in the Mobile Payments Ecosystem

One of the unique qualities of the mobile payments ecosystem is the expanse and diversity of industry stakeholders. The mobile environment has created opportunities for many nonbanks to introduce innovation and creative partnerships to the evolution of the mobile payments ecosystem, contributing to the success of mobile payments adoption. Start-ups and mature nonbank businesses are developing apps and providing lower cost solutions (compared to traditional card rails) for making and accepting mobile payments, and for clearing and settling payments that leverage existing payment rails. Merchants and alternative service providers are also demonstrating increased interest and influence over the direction of the mobile payments ecosystem.

Participation by mobile app developers illustrates a potential risk/benefit paradigm that is introduced to the payments environment. Many mobile app developers are small and independent, and not as familiar with the regulations and risk management practices that characterize the financial services industry. Without some guidance and direction, mobile payment app developers could potentially create serious consumer payment vulnerabilities. Partnering with industry incumbents could help to educate them and mitigate risks.

While innovation is encouraged in the mobile payments marketplace, participation by new entrants, large and small, generates new risk to the ecosystem, along with new opportunities. It also raises questions about the need for third-party (nonbank) enhanced risk management considerations. Therefore, the need

to keep abreast of and understand nonbank activity in the payment space has been added to the MPIW strategic principles.

Summary of Principles

Overall, the original principles established by the MPIW hold true, albeit with some modifications, particularly the shift to an expanded mobile technology platform that includes both NFC and cloud-based mobile and digital wallets. Some change is not surprising with almost two years of experience testing different mobile models: the introduction of new participants, technologies, and services; learning what works and what does not; the influence of merchants on the cost structure of mobile payments; and all stakeholders gaining a better understanding of the consumer demands and security requirements. As the MPIW has grown in size and diversity of representation, it has broadened its perspective on the evolution of mobile payments in the United States.

This broader perspective lends itself to an expansion of the original strategic principles to emphasize two additional points: (1) understanding risks associated with nonbanks; and (2) recognizing that incorporating transparent value-added services –such as incentives and offers into mobile payment platforms –have the potential to motivate consumers to adopt mobile payments.

V. Long-term Vision

The MPIW's support for a secure and open mobile payments system remains unchanged. Despite the variety of technology platforms, the ultimate solution must be safe, open, interoperable, and available ubiquitously on any mobile device, with any bank or merchant, and ideally over any network. Security in mobile payments will continue to be top of mind for all stakeholders, particularly consumers and merchants, who must have confidence in the safety and reliability of the mobile payments system for it to succeed. Ongoing technology advancements and disruption will continue to alter the landscape; mobile and digital wallets will co-exist; technology platform and channel convergence will increase; and big data monetization will need to be included in the risk management process.

Ongoing Technology Advancements will Alter the Mobile Payments Landscape

The MPIW's ultimate long-term vision is for a safe, secure, and technically interoperable mobile ecosystem built on multiple technology platforms. However, in the absence of any limits or standards restricting entry, the mobile payments landscape will continue to introduce more alternative payment solutions in the near term.

Mobile and Digital Wallets will Co-Exist

Future wallet business models may leverage emerging standards such as the FIDO[43] Alliance that combine the strong device-level security (a characteristic of NFC) with cloud-based technologies, driving improved efficiencies and innovation for user experiences, while standardizing the back-end protocols for interoperability, ubiquity, and optimum security.

Increasing Channel Convergence using Existing Rails

The increasing ubiquity of mobile phone usage globally is driving commerce to the Internet and mobile channels. Subsequently, payment service providers are introducing solutions that leverage both channels, blurring the lines of demarcation among payment delivery methods.

Interestingly, there is little evidence of industry support for the creation of new clearing and settlement rails, suggesting that new payment systems will continue to build on existing infrastructure or create new models using components of the existing rails. It is very costly and complicated to build brand new payment rails and achieve scale, particularly in the United States where the existing payment rails are mature, trusted, secure and regulated.

Big Data Monetization with Risk Management Oversight

The MPIW initially predicted that customer data analytics and marketing efforts might need a combination of private and public oversight to avoid privacy violations. As a result, mobile industry participants will need to find ways to share customer information to establish sufficient audit trails to manage payments fraud. New mobile business models will need to strike a reasonable balance for information sharing between who needs to know and what information should be shared.

While alternative payment providers have demonstrated sufficient self-governance with respect to mobile marketing, future growth and competition in the mobile landscape may potentially compromise consumer privacy, creating opportunities for data mismanagement. This could be particularly true with nonbank technology start-ups that are unfamiliar with regulatory schemes and consumer protection laws associated with traditional financial services. Data owners may jeopardize consumer protections by leveraging data to maximize revenue. Increasing use of LBS to track consumers and offer real-time, customized promotions may also raise questions about access to customer data for marketing purposes. The CFPB will monitor consumer protections, including disclosures governing privacy. The FTC is also increasingly focused on developments in the mobile channel with respect to consumer protections and privacy, which may serve to strengthen industry self-governance.

---

[43] Fast Identity Online (FIDO) is an organization formed to enable interoperable strong authentication and authorization between mobile phones and cloud services. The FIDO Alliance was co-founded by Validity, PayPal, Infineon, Lenovo, and NokNok Labs and launched in February 2013.

VI. Conclusion

Much has happened in the two-plus years since the first MPIW report on the U.S. mobile payments landscape was published, and not entirely in the direction many industry stakeholders had anticipated. There have been some unexpected obstacles to mobile payment adoption, some surprises in the mix of players in the market, and some new solutions developed to compete with NFC. As a result, the U.S. mobile payments market and consumer adoption did not grow as quickly as expected. It is clear that mobile payments will continue to expand and become a permanent fixture in the payments system. However, without continued collaboration and movement toward open access, the likelihood of achieving mass adoption and the associated benefits to stakeholders, consumers, and the payment system is uncertain.

Next Steps for the MPIW

The MPIW will continue to convene and work collaboratively to inform the FRB, regulators, policymakers, and Congress on developments in the mobile payments industry and the adoption of open and interoperable mobile payment solutions, both for the retail POS as well as other venues. Much work remains to be done to achieve a viable mobile payment system, including development of a risk management program, implementation of necessary technology standards, identifying and closing regulatory gaps, strengthening stakeholder business cases, and achieving broad consumer adoption.

Gaining a better understanding of the risks and security requirements for mobile payments will be a top priority. This is a broad topic because of the many components and parties involved in provisioning and processing a mobile payment across different platforms. As such, the MPIW will first need to define the scope of the effort.

The MPIW will also provide input and recommendations for mobile and digital wallet standards and best practices in order to address compatibility, interoperability, privacy, and security (including accommodating multiple payment options and applications securely, accessing multiple payments networks).

Finally, the group will continue to educate members and engage outside groups in discussions on the long-term benefits of mobile payments in the retail space, and keep abreast of regulatory developments, particularly related to consumer protection and data privacy, and how the U.S. migration to EMV may impact the progress of mobile payments.

Appendix: MPIW Activity 2011-2012

January 2011	• Met to discuss current mobile activity and review draft of white paper
March 2011	• Published first white paper, *Mobile Payments in the United States: Mapping Out the Road Ahead*
July 2011	• Met to discuss mobile wallet, merchant business case, and security of NFC mobile payments • First meeting to feature inclusion of several merchants (previously represented by MAG) • Merchants expressed concerns related to business case for mobile payments, future role of NFC, processing costs, investment in terminal upgrades, and cost of PCI compliance • Attendees expressed need for broad education to allay consumer security and privacy concerns for mobile payments, and supported a roadmap that would allow for industry self-regulation
December 2011	• Met to discuss current trends related to mobile wallet initiatives (e.g., Google Wallet, Isis, Visa, PayPal), security requirements and end-to-end risk management, TSM roles and responsibilities, and interoperability and management of secure elements and multiple wallets • Prior to meeting, several MPIW members participated in series of calls to examine different NFC secure element approaches – embedded, SIM, microSD, and mobile payments in the cloud
April 2012	• Met with representatives from Federal and State banking agencies, FTC and FCC to discuss issues, concerns, and potential gaps in regulatory coverage of mobile payments in the United States
July 2012	• Published white paper, *The U.S. Regulatory Landscape for Mobile Payments*, summarizing the April 2012 meeting
September 2012	• Met with retailers and start-ups to understand their perspective on mobile payment opportunities and challenges
November 2012	Findings from security information presented at December 2011 meeting included in Federal Reserve Bank of Boston's white paper, *Mobile Phone Technology: Smarter than We Thought*.[44]
January 2013	• Met with mobile security experts to learn their perspectives on key mobile payment risks • Mobile payment security identified as an issue where collaboration is necessary • Formed security sub-group to analyze mobile payment vulnerabilities and authentication requirements
May 2013	• Published new white paper, *U.S. Mobile Payments Landscape – Two Years Later*

[44] http://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf, November 2012.

- Home
- About clearXchange
- Our Team
- Press
- Contact Us

Press

Journalists and analysts, please contact us directly at press@clearXchange.com.

Press Releases

3.17.15 U.S. Bank Becomes Member of clearXchange to Bring Customers Faster, More Secure Digital Payments

Minneapolis & San Francisco, March 17, 2015 – U.S. Bank, lead bank of U.S. Bancorp (NYSE: USB), has made an investment in and joined clearXchange, the largest bank-focused digital payments network in the United States. With the addition of U.S. Bank, the clearXchange network now includes 5 of the largest banks in the United States, along with multiple regional financial institutions, who together serve over 100 million online banking and 50 million mobile banking customers.

U.S. Bank, which has offered similar person-to-person payment services to customers for five years, will now be a member and co-owner of clearXchange. Through clearXchange, it will be even easier for U.S. Bank customers to send payments to anyone with a United States bank account from the security and convenience of their U.S. Bank online and mobile banking experience. The only information the sender needs is the receiver's mobile number or email address, eliminating the need to share sensitive account information.

"U.S. Bank is committed to bringing customers the most convenient and secure payment options available in the marketplace," said Gareth Gaston, executive vice president of omnichannel banking at U.S. Bank. "Digital person-to-person payments are far more convenient than writing a check or having enough cash on hand to pay the babysitter or split a rent payment. By joining with clearXchange, U.S. Bank customers have a better way to make those payments quickly, easily and safely. We also have the opportunity to explore other ways this payment exchange network could come to light through our unified, omnichannel approach to customer service."

"I'm very excited to welcome U.S. Bank to the clearXchange network," said Mike Kennedy, CEO of clearXchange. "This partnership will improve U.S. Bank's customer experience and further enhance the value of the clearXchange network to financial institutions and their customers."

U.S. Bank is the fifth owner of the network, joining current owners Bank of America, Capital One, JPMorgan Chase and Wells Fargo. Today, banks in the clearXchange network have access to the broadest group of digital bank customers in the United States, which enables seamless exchange of information and speeds up the person-to-person payment process. In addition, corporate and

EXHIBIT
K-14

government clients can benefit from the cost savings, security and speed of making disbursements over the clearXchange network.

Implementation of clearXchange services by U.S. Bank will take place in the future. Meanwhile, customers can continue to use the person-to-person payments U.S. Bank offers online and in mobile banking.

About clearXchange
Founded in 2011, clearXchange is a bank-focused payments company with customers including Bank of America (NYSE: BAC), Capital One (NYSE: COF), JPMorgan Chase (NYSE: JPM), U.S. Bank (NYSE: USB), Wells Fargo (NYSE: WFC) and multiple regional financial institutions. Membership is open to financial institutions of all sizes. clearXchange develops solutions for financial institutions to make digital payments easier and safer. With only the recipient's mobile number or email address, customers can send funds directly from their bank account to the recipient's bank account without requiring sensitive account information. Nationwide, clearXchange banks represent more than 100 million online banking consumers. The company is headquartered in San Francisco. For more information, visit https://www.clearXchange.com

About U.S. Bancorp
U.S. Bancorp (NYSE: USB), with $403 billion in assets as of December 31, 2014, is the parent company of U.S. Bank National Association, the fifth-largest commercial bank in the United States. The company operates 3,176 banking offices in 25 states and 5,022 ATMs and provides a comprehensive line of banking, brokerage, insurance, investment, mortgage, trust and payment services products to consumers, businesses and institutions. Visit U.S. Bancorp on the web at www.usbank.com.

Media Contacts:

U.S. Bank Corporate Communications
Teri Charest, 612-303-0732
teri.charest@usbank.com

or

clearXchange
Melissa Lowry, 415-813-4430
melissalowry@clearxchange.com

2.19.15 clearXchange Announced as Finalist for PYMNTS.com 2015 Innovator Awards

Prestigious Awards Presented in Live Ceremony at the Conclusion of the Innovation Project 2015

Boston, February 19, 2015 – PYMNTS.com, the premier source of news and commentary on innovation in payments and commerce is pleased to announce the finalists for the 2015 Innovator

Awards, including clearXchange, which is nominated in 3 categories: the NACHA Best Innovation ACH, Best Check Innovation, Best Invisible Innovation. clearXchange will join more than 80 finalists that will compete for Gold, Silver and Bronze Awards across 16 categories.

"We are proud to be a finalist for these awards in recognition of clearXchange's core role in the digital payment industry," said Mike Kennedy, CEO of clearXchange. "Today over 100 million online banking users are at a financial institution that is part of the clearXchange network. By using the clearXchange network, financial institutions can allow their customers to securely send and receive money using only an email address or mobile phone number."

The PYMNTS Innovator Awards are viewed as the most prestigious recognition in the payments industry and boast a submission, selection and voting process that is unmatched in intellectual rigor and competitive energy. A panel of judges made up of executives from across the payments spectrum viewed and deliberated on more than 600 submissions and narrowed them down to five finalists that will compete for 16 prestigious awards in categories like Most Innovative, Most Disruptive and Best New Technology.

The panel of judges included:

- Jan Estep, President and CEO, NACHA
- Matt Harris, Co-Founder and Managing General Partner, Bain Capital Ventures
- Matt Witheiler, General Partner, Flybridge Capital Partners
- Aaron Goldman, Principal, General Atlantic
- Hans Morris, Managing Partner, NYCA Partners; former President Visa
- Dan Rosen, Founder and Partner, Commerce Ventures
- Paul Purcell, Partner, Continental Advisors
- Karen Webster, CEO, PYMNTS.com

Voting is open now through February 25 on PYMNTS.com. Winners will be announced during a live ceremony at The Innovation Project 2015, powered by PYMNTS.com. The industry's foremost thought leadership event takes place March 18-19 on the campus of Harvard University and convenes the most thoughtful minds from established players, emerging disruptors, and entrepreneurial visionaries in the world of payments and commerce. This year's theme - Innovation At The Intersections – will explore the many forces outside of payments that are reinventing and reshaping how payments and commerce evolve.

To request an invitation, please click here.

About PYMNTS.com

PYMNTS.com is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of payments and commerce and make news. This powerful B2B platform is the #1 site for the payments and broader commerce ecosystem by traffic and the premier source of information about "what's next" in payments. C-suite and VP level executives turn to it daily for these insights, making the PYMNTS.com audience the most valuable in the industry. It provides an interactive platform for companies to demonstrate thought leadership, popularize products and, most importantly, capture the mindshare of global decision-makers. PYMNTS.com, where the best minds and best content meet on the web to learn "What's Next" in Payments and Commerce.

About the Innovation Project

Over two content-packed days this March 18 & 19, 2015, The Innovation Project 2015, powered by PYMNTS.com, will convene the most thoughtful minds from established players, emerging disruptors, and entrepreneurial visionaries in the world of payments and commerce on the campus of Harvard University. This year's theme - Innovation At The Intersections – will explore the many forces outside of payments that are reinventing and reshaping how payments and commerce evolve. Leading and participating in these discussions will be the most innovative, thoughtful and dynamic players from their sectors.

*Please note that The Innovation Project™ and PYMNTS.com℠ are not affiliated with Harvard University, nor is the Innovation Project™ 2015 a Harvard University program or activity.

Media Contacts:

Contact For PYMNTS.com
Brooke Hawkins, 617-374-4700
bhawkins@pymnts.com

2.19.15 clearXchange Announced as Finalist for PYMNTS.com 2015 Innovator Awards

Prestigious Awards Presented in Live Ceremony at the Conclusion of the Innovation Project 2015

Boston, February 19, 2015 – PYMNTS.com, the premier source of news and commentary on innovation in payments and commerce is pleased to announce the finalists for the 2015 Innovator Awards, including clearXchange, which is nominated in 3 categories: the NACHA Best Innovation ACH, Best Check Innovation, Best Invisible Innovation. clearXchange will join more than 80 finalists that will compete for Gold, Silver and Bronze Awards across 16 categories.

"Corporate and government institutions across the U.S. can now benefit from the savings, speed and security of making disbursements through the clearXchange network, directly into their customers' bank account," said Mike Kennedy, CEO of clearXchange. "We are honored to be a finalist for these prestigious awards in recognition of our first-of-a-kind electronic disbursement solution that promises to transform the $3 trillion business and government to consumer disbursement market."

The PYMNTS Innovator Awards are viewed as the most prestigious recognition in the payments industry and boast a submission, selection and voting process that is unmatched in intellectual rigor and competitive energy. A panel of judges made up of executives from across the payments spectrum viewed and deliberated on more than 600 submissions and narrowed them down to five finalists that will compete for 16 prestigious awards in categories like Most Innovative, Most Disruptive and Best New Technology.

The panel of judges included:

- Jan Estep, President and CEO, NACHA

- Matt Harris, Co-Founder and Managing General Partner, Bain Capital Ventures
- Matt Witheiler, General Partner, Flybridge Capital Partners
- Aaron Goldman, Principal, General Atlantic
- Hans Morris, Managing Partner, NYCA Partners; former President Visa
- Dan Rosen, Founder and Partner, Commerce Ventures
- Paul Purcell, Partner, Continental Advisors
- Karen Webster, CEO, PYMNTS.com

Voting is open now through February 25 on PYMNTS.com. Winners will be announced during a live ceremony at The Innovation Project 2015, powered by PYMNTS.com. . The industry's foremost thought leadership event takes place March 18-19 on the campus of Harvard University and convenes the most thoughtful minds from established players, emerging disruptors, and entrepreneurial visionaries in the world of payments and commerce. This year's theme - **Innovation At The Intersections** – will explore the many forces outside of payments that are reinventing and reshaping how payments and commerce evolve.

To request an invitation, please click here.

About PYMNTS.com

PYMNTS.com is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of payments and commerce and make news. This powerful B2B platform is the #1 site for the payments and broader commerce ecosystem by traffic and the premier source of information about "what's next" in payments. C-suite and VP level executives turn to it daily for these insights, making the PYMNTS.com audience the most valuable in the industry. It provides an interactive platform for companies to demonstrate thought leadership, popularize products and, most importantly, capture the mindshare of global decision-makers. PYMNTS.com, where the best minds and best content meet on the web to learn "What's Next" in Payments and Commerce.

About the Innovation Project

Over two content-packed days this March 18 & 19, 2015, The Innovation Project 2015, powered by PYMNTS.com, will convene the most thoughtful minds from established players, emerging disruptors, and entrepreneurial visionaries in the world of payments and commerce on the campus of Harvard University. This year's theme - Innovation At The Intersections – will explore the many forces outside of payments that are reinventing and reshaping how payments and commerce evolve. Leading and participating in these discussions will be the most innovative, thoughtful and dynamic players from their sectors.

*Please note that The Innovation Project™ and PYMNTS.com℠ are not affiliated with Harvard University, nor is the Innovation Project™ 2015 a Harvard University program or activity.

Media Contacts:

PYMNTS.com
Brooke Hawkins, 617-374-4700
bhawkins@pymnts.com

12.12.14 FirstBank Adds Person-to-Person Payment System to Its Powerful Mobile Banking App

Mobile payment system for Arizona FirstBank customers adds to robust mobile banking services

Phoenix, December 12, 2014 – FirstBank Holding Company, the highly successful bank with 15 branches in the Phoenix area, today announced a person-to-person (P2P) payments system as the newest tool in its robust mobile banking application. With this addition, FirstBank becomes the most recent bank to offer P2P payments through the clearXchange network, providing customers with an easy way to send and receive money via their mobile devices. FirstBank is the fourth member of the clearXchange network and will be going live today. It is the first regional bank in the nation to go live with the service.

clearXchange is the largest P2P payments network in the U.S. created by and for financial institutions, and the country's leading banks rely on clearXchange's financial technology to allow consumers and businesses to send and receive money using just an email or mobile number. More than 100 million people already have access to the clearXchange network directly through their current bank.

The addition of clearXchange allows FirstBank customers to send payments from their existing FirstBank account safely and conveniently using only the recipient's mobile number or e-mail address, and without providing sensitive account information. Customers of participating banks can easily transfer and receive money using their existing online or mobile banking service. Others whose bank is not yet part of the clearXchange network, only need to do a one-time registration at clearXchange.com to receive payments directly to their account at any U.S. bank.

"Joining the clearXchange network gives our customers a reliable, convenient and secure way to send and receive money," said Jim Reuter, executive vice president at FirstBank. "We're excited to continuously provide innovative services to our customers and enhance the flexibility of banking with FirstBank."

Mike Kennedy, CEO of clearXchange, adds, "With clearXchange, FirstBank provides customers with a seamless and secure person-to-person payments solution, making it easier to send money to family and friends. We are excited to add FirstBank's customers to our national network."

Since opening its first Arizona location in 2007, FirstBank has provided area residents and businesses with more than 2,025 loans worth more than $750 million. FirstBank is highly active with local communities where its employees live and work. The company donated more than $5 million to nonprofits in Arizona, California and Colorado last year and was the main sponsor of the inaugural Arizona Gives Day, a 24-hour online giving initiative aimed at increasing individual giving throughout the state, which raised more than $1 million for Arizona non-profits.

How clearXchange works

For banking customers, clearXchange enables P2P payments directly from a user's existing deposit account through their bank's online and mobile platforms. Customers do not need to open a new account or conduct financial transactions via a third-party service to transfer funds. Instead of difficult

to remember account numbers, customers use their email or mobile number. When receiving a payment, funds are directly deposited into the user's bank account. What's more, customers get all the services and protections that they get today from their banks.

For banks and credit unions, clearXchange is a compelling P2P network that easily integrates into online and mobile platforms. The financial institution continues to drive and maintain its own customer relationships and remains the center of their customers' financial lives. Enrolled customers conduct transactions on the bank's sites and receive support from their bank regardless of where a transaction is initiated.

For more information about the clearXchange network, go to https://www.clearxchange.com/.

About FirstBank

FirstBank operates more than 120 locations in Colorado, Arizona and California. FirstBank is the largest locally owned banking organization in Colorado, serving more than 650,000 customers. Since 2000, FirstBank has contributed more than $45 million and thousands of volunteer hours to charitable organizations.

FirstBank is unique in that a majority of its stock is owned by management and employees. For more information, go to www.efirstbank.com.

Media Contacts:

FirstBank
Brian Jensen, 303-235-1400
Brian.Jensen@efirstbank.com
or
Linhart Public Relations
Geoff Renstrom, 303-951-2564
grenstrom@linhartpr.com

9.30.14 BofA Merrill Introduces Digital Disbursements

New Offering Allows Companies to Make Payments to Their Customers Without Checks by Using Either a Mobile Phone Number or Email Address as the Identifier

New York, September 30, 2014 – Bank of America Merrill Lynch today announced the launch of Digital Disbursements, a new payment solution that enables companies to make payments to their customers digitally, eliminating the need to issue a check. The payments are directly routed to the bank account of the individual payee's choosing using either a mobile phone number or email address as the identifier. The solution leverages the technology behind person-to-person payments, a capability currently available to individual customers of Bank of America's consumer business.

"Digital Disbursements emerges from the rapidly evolving world of payments, in which both consumers and corporations are increasingly opting for faster, easier ways to send and receive money electronically," said Ather Williams III, head of Global Payments in Global Transaction Services (GTS). "Through this method, customers don't have to wait for the check to come in the mail and there is no need for companies to maintain sensitive personal bank account information." The types of business-to-consumer payments that could be supported by Digital Disbursements include rebates, refunds and claims payments.

Digital Disbursements was created to serve middle-market, large corporate and public sector clients. It uses the proven technology already in existence for person-to-person (P2P) payments, a capability currently offered by Bank of America's consumer business through the company's alliance with clearXchange. Individual consumers have adopted P2P payment practices in large numbers, and feedback from focus groups concluded that people are eager to receive payments from companies or government entities in the same way.

Corporate clients will receive the following benefits from Digital Disbursements:

- The ability to deliver funds to customers faster and with less complexity than a physical check.
- A reduction in end-to-end disbursement costs by as much as 75 percent when compared to a physical check. Merchants could potentially save more than US$1 billion annually by eliminating disbursement checks[1].
- Reduction in escheatment management, an administrative burden that is both costly and time consuming.
- Elimination of the need to obtain and store sensitive bank account information.

"Digital Disbursements is an example of true partnership and our commitment to collaborate across our businesses to deliver the best solutions for our clients based on their needs," said Bill Pappas, Global Wholesale Banking Technology and Operations CIO. "By leveraging proven technology, we were able to develop an innovative solution for our corporate clients which speeds the payment process from several days to only a few minutes."

"We are very proud to be one of the first banks to offer an alias-based business-to-consumer payments solution. Our corporate clients and their customers will benefit greatly from Digital Disbursements, which is an important step in the evolution of the payments industry in the United States," said Dub Newman, head of Global Transaction Services, North America.

Digital Disbursements solves challenges facing payers and payees, while aligning with evolving trends in technology usage. A recent study performed by the Federal Reserve found that 85 percent of consumers and 81 percent of businesses prefer not to provide bank account information to the payee when making a payment[2]. Separately, the trend towards mobile banking continues to rise, and it is anticipated that by 2018, 63 percent of the mobile consumer population in the United States will use mobile banking[3].

Digital Disbursements will be initially introduced to clients making payments in the United States. However, given the product's global application, and that clients and their customers want the same convenience wherever in the world they do business, the bank expects to extend Digital Disbursements to other regions in the future.

"clearXchange is pleased to support Digital Disbursements, an exciting new use of the clearXchange platform that will make payments easier, faster and more secure for both corporations and their customers," said Mike Kennedy, CEO of clearXchange. "Our partnership helps keep Bank of America Merrill Lynch at the forefront of innovation in the business-to-consumer payments market."

Bank of America Merrill Lynch offers a global suite of electronic and paper-based disbursement solutions to help companies optimize their working capital with greater precision and control. Solutions include: low-value payments (Automated Clearing House), wire transfers, cross-border payments and multicurrency payments, as well as card solutions and ePayables. Furthermore, the bank's expertise in foreign exchange means that companies can make international payments in over 140 currencies covering more than 200 countries and territories.

(1) Aite Group survey to 1,115 participants; Business-to-Consumer Disbursements: Time to Take Notice, June 5, 2012

(2) Federal Reserve System, Research on End-User Demand for Select Payment Attributes, 2014

(3) Javelin Strategy & Research, Mobile Payments to hit $20 Billion in 2012

Bank of America
Bank of America is one of the world's leading financial institutions, serving individual consumers, small businesses, middle-market businesses and large corporations with a full range of banking, investing, asset management and other financial and risk management products and services. The company provides unmatched convenience in the United States, serving approximately 49 million consumer and small business relationships with approximately 5,000 retail banking offices and approximately 16,000 ATMs and award-winning online banking with 30 million active users and more than 15 million mobile users. Bank of America is among the world's leading wealth management companies and is a global leader in corporate and investment banking and trading across a broad range of asset classes, serving corporations, governments, institutions and individuals around the world. Bank of America offers industry-leading support to approximately 3 million small business owners through a suite of innovative, easy-to-use online products and services. The company serves clients through operations in more than 40 countries. Bank of America Corporation stock (NYSE: BAC) is listed on the New York Stock Exchange.

Bank of America Merrill Lynch is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated, which is a registered broker-dealer and member of SIPC, and, in other jurisdictions, a locally registered entity. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA. Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured * May Lose Value * Are Not Bank Guaranteed.

Copyright 2014 Bank of America Corporation. All rights reserved. Bank of America, Merrill Lynch, Broadcort and their logos are trademarks of Bank of America Corporation and/or its affiliates.

Media Contact:

Louise Hennessy, Bank of America Merrill Lynch, 1.646.855.1403
louise.hennessy@bankofamerica.com

4.9.14 Payments with clearXchange disrupts banking

SAN FRANCISCO, CA, April 9, 2014 – Michael Kennedy, clearXchange CEO and co-founder, meets with CNBC to discuss his company's P2P network that allows customers to send person-to-person payments easily and securely with only an email address or phone number.

2.19.14 Capital One Joins clearXchange Network

Partnership expands payment options for customers

MCLEAN, VA, February 19, 2014 – Capital One Financial Corporation (NYSE: COF) and clearXchange today announced that Capital One, N. A. has joined the clearXchange network as an owner, becoming the fourth owner alongside Bank of America, JPMorgan Chase, and Wells Fargo and fifth bank customer of the clearXchange network. clearXchange is the first network in the U.S. created by and for financial institutions that lets customers send person-to-person payments easily and securely with only an email address or phone number. As a member of the network, Capital One will expand its capabilities to provide customers the ability to pay anyone with a U.S. bank account without requiring sensitive account information.

"Capital One is focused on bringing its customers innovative products and services that allow them to spend wisely and transact easily – when, where and how they want," said Jack Forestell, Executive Vice President of Digital at Capital One. "Partnering with clearXchange is another way we are bringing safe and secure payments through convenient, digital channels to our customers."

"We are excited to add Capital One to our network," said Mike Kennedy, CEO of clearXchange. "This partnership expands the value of the clearXchange network by enabling more customers to easily make secure payments to their friends and family, and it will drive additional innovation in person-to-person payments."

With the broadest network of digital bank customers in the US, clearXchange provides an innovative way for financial institutions to enable customers to move from cash and check to more user-friendly bank digital channels. clearXchange provides the flexibility and tools needed for banks to deliver a person-to-person payments solution to best meet their customers' unique needs.

About Capital One
Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N. A., had $204.5 billion in deposits and $297 billion in total assets as of December 31, 2013. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has more than 900 branch locations primarily in New York, New Jersey, Texas, Louisiana, Maryland, Virginia and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

About clearXchange
Founded in 2011, clearXchange is a bank-focused payments company with customers including Bank of America (NYSE: BAC), Capital One (NYSE: COF), FirstBank, JPMorgan Chase (NYSE: JPM), and Wells Fargo (NYSE: WFC), with membership open to banks and credit unions of all sizes. clearXchange develops solutions for financial institutions to make person-to-person payments easier and safer. With only the recipient's mobile number or email address, customers can send funds directly from their bank account to the recipient's bank account without requiring sensitive account information. Nationwide, clearXchange banks represent more than 50 percent of the consumer online banking market. The company is headquartered in San Francisco. For more information, visit https://www.clearXchange.com

---

10.10.13 FirstBank to Join the clearXchange Network

SAN FRANCISCO, CA and LAKEWOOD, CO, October 10, 2013 – clearXchange, the largest person-to-person (P2P) payments network in the U.S. created by and for financial institutions, and FirstBank, the second-largest bank by deposits in Colorado, announced today that FirstBank will join the clearXchange network.

With clearXchange, FirstBank customers will be able to send payments from their existing FirstBank account safely and conveniently using only the recipient's mobile number or e-mail address and without providing sensitive account information. With FirstBank, clearXchange continues its network expansion and drive to ubiquity, delivering value to customers of banks of any sizes. Nationwide, clearXchange banks represent more than 50 percent of the consumer online banking market.

"FirstBank is an innovative organization that shares clearXchange's vision for a seamless, reliable bank-focused payment network, open to everyone with a U.S. bank account," said Michael Kennedy, CEO of clearXchange. "We both recognize the power of banks and credit unions to collectively move from cash and checks to electronic payments – improving the customer experience and lowering costs."

FirstBank – with $12 billion in deposits and 115 locations in Colorado, Arizona and California – is the first non-founding member of the clearXchange network. clearXchange was launched in 2011 as a

bank-focused payments joint venture among Bank of America (NYSE: BAC), JPMorgan Chase (NYSE: JPM) and Wells Fargo (NYSE: WFC), with membership open to banks and credit unions of all sizes.

"Joining the clearXchange network allows FirstBank customers to send and receive money from the convenience and safety of our trusted FirstBank online and mobile channels," said Jim Reuter, president of FirstBank Support Services. "The reach of clearXchange made it the clear person-to-person network of choice to bring value to our customers," said Reuter.

How clearXchange works
For banking customers, clearXchange enables P2P payments directly from consumers' existing deposit accounts through their bank's convenient, secure online and mobile sites. There is no need to open a new account or conduct financial transactions away from their bank's trusted site. When getting paid, funds are directly deposited into the consumer's bank account. And customers get all the services and protections that they get today from their banks.

For banks and credit unions, clearXchange allows the bank to offer their customers a compelling P2P product within the bank's online and mobile session. The financial institution continues to drive and maintain its own customer experience and remain the center of their customers' financial lives. Enrolled customers conduct transactions on the bank's sites and receive support from their bank regardless of where a transaction is initiated.

About FirstBank
FirstBank operates more than 115 locations in Colorado, Arizona and California. FirstBank is the largest locally owned banking organization in Colorado, serving more than 600,000 customers. Since 2000, FirstBank has contributed more than $40 million and thousands of volunteer hours to charitable organizations. FirstBank is unique in that a majority of its stock is owned by management and employees. For more information, go to www.efirstbank.com.

About clearXchange
Founded in 2011, clearXchange is a joint venture among Bank of America (NYSE: BAC), JPMorgan Chase (NYSE: JPM), and Wells Fargo (NYSE: WFC). With the broadest network of digital bank customers in the U.S., clearXchange provides an innovative way for financial institutions to personalize payments and reach customers. It is the first network in the U.S. created by and for financial institutions that lets customers send person-to-person payments easily and securely. With only the recipient's mobile number or email address, customers can send funds directly from their bank account to the recipient's bank account without requiring sensitive account information. The safety and convenience of clearXchange allow customers to move from cash and check to more user-friendly bank digital channels. The company operates from offices in San Francisco and Charlotte, N.C. For more information, visit clearXchange.

9.10.13 clearXchange Names Michael Kennedy Chief Executive Officer

SAN FRANCISCO, September 10, 2013 – clearXchange, a joint venture among Bank of America (NYSE: BAC), Wells Fargo (NYSE: WFC) and JPMorgan Chase (NYSE: JPM), has named Michael Kennedy as the company's chief executive officer. Kennedy co-founded and served as chairman of clearXchange while working as executive vice president and head of Innovation and Payments

Strategy for Wells Fargo Bank. As CEO, Kennedy will devote 100 percent of his time to leading clearXchange. He will be based in San Francisco.

"The three founding banks have more than 50 percent of the nation's online banking market, which makes us the largest bank-focused person-to-person payment system," said Kennedy. "We are looking forward to serving even more customers by growing our end user base at the existing clearXchange banks, as well as adding new bank partners."

In a joint statement, the board said, "We knew it was critical to select a CEO who has a focus on the consumer, deep experience in emerging mobile and digital payments, and understands how banks operate. In Kennedy, we found that individual."

"clearXchange has tremendous upside for both consumers and the financial services industry," added Kennedy. "There are an estimated $900 billion in annual person-to-person payments in the U.S.[1], most of which are transacted in cash and checks. Helping to turn these person-to-person payments into digital transactions will enhance the experience for senders and receivers as well as take costs down for consumers and banks."

As executive vice president and head of Wells Fargo's Innovation and Payments Strategy, Kennedy drove mobile and emerging payments, strategy across all payment products, and technology research and development. Prior to this role, Kennedy led strategy and implementation for Wells Fargo's Wealth Management group, which he joined in 2004.

Before joining Wells Fargo, Kennedy worked at McKinsey & Company consulting to financial services institutions, was the head of Strategy and Business Development at Vail Associates, and was an associate at a venture capital firm.

Kennedy earned his Bachelor of Science with distinction and Masters of Science degrees in Industrial Engineering from Stanford University and his MBA with distinction from Harvard Business School.

About clearXchange
Founded in 2011, clearXchange is a joint venture among Bank of America (NYSE: BAC), Wells Fargo (NYSE: WFC) and JPMorgan Chase (NYSE: JPM). With the broadest network of digital bank customers in the US, clearXchange provides an innovative way for financial institutions to personalize payments and reach customers. It is the first network in the U.S. created by and for financial institutions that lets customers send person-to-person payments easily and securely. With only the recipient's mobile number or email address, customers can send funds directly from their bank account to the recipient's bank account without requiring sensitive account information. The safety and convenience of clearXchange allow customers to move from cash and check to more user-friendly bank digital channels. The company operates from offices in San Francisco and Charlotte, N.C. For more information, visit https://clearXchange.com.

[1]From the August 2012 Aite report "Sizing Online and Mobile Banking P2P payments in the United States."

5.25.11 Bank of America, Chase, Wells Fargo form new venture to help consumers make person-to-person payments electronically

CHARLOTTE, NEW YORK and SAN FRANCISCO, May 25, 2011 – Bank of America, JPMorgan Chase and Wells Fargo today announced that they have formed a new venture to enable their customers to move money more conveniently and safely using a mobile number or email address. clearXchange is the first bank-owned solution of its kind and the service is available to its partners today.

Customers of the three banks will be able to move funds directly from their existing checking accounts using an email address or mobile number – instead of providing checking account and routing numbers. The clearXchange service will roll out nationally and there are plans over time to expand it to include other financial institutions and endpoints to create a money movement capability across the industry.

"This is an innovative game-changer in electronic payments," said Mike Kennedy, EVP and Head of Payments Strategy at Wells Fargo. "We want our customers to be able to easily send money to anyone without having to establish a new account outside their primary bank. All our customers need to know is the email address or mobile number of a friend or family member and we will take care of the rest utilizing clearXchange."

The three banks will own and run clearXchange, with Bank of America's John Feldman serving as General Manager. Financial terms were not disclosed.

"Our goal is to provide convenient and safe financial services options for our customers," said David Owen, eCommerce, Claims and Fraud Executive at Bank of America. "By creating a utility like clearXchange, we are able to meet the needs of our customers and differentiate our capabilities from other offerings in the marketplace."

"clearXchange will allow us to make our popular person to person payments service even better," said Jack Stephenson, Director of Mobile, eCommerce and Payments at JPMorgan Chase. "Chase customers will be able to send and receive money even more quickly and easily – with full confidence their funds are in a bank account without worrying about cash, checks or higher-cost services."

clearXchange is headquartered in Charlotte, North Carolina.

Media Contacts:

Tara Burke, Bank of America, (203) 292-6590
tara.a.burke@bankofamerica.com

Christine Holevas, Chase, (312) 732-6206
christine.holevas@chase.com

Gabe Boehmer, Wells Fargo, (503) 886-4186
gabriel.h.boehmer@wellsfargo.com

What the Industry Is Saying

clearXchange will shake up the P-to-P market. ... This is a big-play.

5.25.12 | American Banker | BTN

Making an electronic payment might never have been easier than this: Wells Fargo has introduced clearXchange, a person-to-person payments platform that doesn't require the sender to know its recipient's bank account number.

5.24.12 | ZDNet

Wells Fargo is the first bank to roll out nationally the clearXchange service for person-to-person-payments.

5.24.12 | Wells Fargo Press Release

P2P is a great place for banks to take a stand, they have a competitive advantage, they have consumers already enrolled... so if that's where your money already is, you can move it from one bank to another.

8.1.11 | Bank Technology News

It's nice to see banks using the power of their collaborative action to demonstrate that innovation can come from the bank side of the payments world as well.

5.31.11 | Glenbrook Partners

Payment strategies like the one announced by the big three banks, clearXchange, are not just important product developments, they are essential to keeping the financial institution industry in the game…the collaboration of Bank of America, Wells Fargo, and JPMorgan Chase in the new P2P network clearXchange makes for a giant leap in ubiquity.

5.26.11 | Mercator

Any capability that is more broadly introduced to the market just makes it better for all of us.

5.25.11 | American Banker

ClearXchange would seem to keep banks relevant at a time when many bankers worry that tech newcomers and established alternative-payments providers such as PayPal Inc. are encroaching on their turf.

5.25.11 | Digital Transactions

Find out how it works and how your financial institution can benefit from clearXchange.

Receive a Payment Notification?

Log in or create a clearXchange profile to get your payment.
Login | Start Now

Privacy
|
Sitemap

©2015 clearXchange Intellectual Property. All rights reserved.

ABOUT SSL CERTIFICATES

FDIC Consumer News

Spring 2014

Person-to-Person (P2P) Payments Online: What to Know Before You Click and Send That Money

When it comes time to pay the babysitter or reimburse a friend for lunch, most people use cash or write checks. But an increasing number of others instead turn to their computer or smartphone to make a person-to-person or "P2P" payment.

P2P payments can be convenient, but there are potential costs and risks, in areas such as the privacy of your personal information. ***FDIC Consumer News*** first introduced readers to P2P payments in 2011, and now we are offering our latest suggestions.

How a P2P service works: Banks and other companies offer different P2P payment services. Most share certain features: You establish an online account and designate one or more payment sources (such as your checking account, credit card or prepaid card) that you'll use to pay people. To send money to someone, you'll provide the recipient's information — in many cases, his or her e-mail address. To get money from someone, you may need to provide your bank account information or other details to the sender's P2P service provider.

"P2P payments may be convenient — for both the sender and the recipient — but if you or your recipient will have to jump through a lot of hoops to use it, that promise of convenience can suddenly fade," said Elizabeth Khalil, a Senior Policy Analyst at the FDIC.

Fees: There are numerous possibilities. Is there a fee to sign up? A fee to send money? A fee to receive money? Is there a single, fixed transaction fee for a service or is it calculated as a percentage of the transaction amount?

"Shop around to find a service with costs that seem reasonable," Khalil recommended. "And if you are the recipient and the fee to receive money seems high, don't be shy about telling the sender you would prefer to be paid another way."

Privacy: Be aware of the service's privacy practices and how your information — and that of your recipients — will be used. If you decide to use the service, set all available privacy settings to your preferences. Some services may, for example, share certain aspects of your transaction activity with other users, such as your social media "friends." If you don't want that to happen, evaluate whether the service's privacy settings allow you to turn off that feature. Because a P2P service provider's privacy practices can change, periodically check its policies and your privacy settings to ensure they still are set in the way you want.

Funds availability: Know when the money you send will be charged to your credit card or deducted from your account. Also be clear on when that money will be available to the recipient. "It may be quick to make a P2P payment, but that doesn't mean the recipient can access the funds right away," said Khalil. "When money is available can vary depending on which P2P service you're using."

EXHIBIT
K-15

Your rights and dispute resolution: Know what the service's user agreement says about resolving errors and disputes. For example, what will happen if the service pays the wrong person or the wrong amount? And, what if you caused the error by mistyping the recipient's e-mail address or the amount you wanted to send? That can easily happen, especially when you're typing on a small mobile phone.

"If the payment is drawn from your checking or savings account, or a credit card, you will have rights under federal law to have the error resolved," said Richard Schwartz, Counsel in the FDIC's Legal Division. "But if the payment comes from somewhere else, like funds you have on hold in an account with the payment service provider, you might not have the same legal protections. Instead, you might have to rely on the service's own policies or perhaps state laws applicable to money transfers. In any case, find out what the service provider's user agreement says will happen if something goes wrong."

Bank or nonbank: "If you're interested in using P2P payments, ask your bank whether it offers the service. And if your bank doesn't, try other banks," Khalil said. "While a number of non-bank companies also offer P2P payments, there can be benefits to working with a bank, such as the opportunity to maintain a financial relationship and obtain other products and services at reasonable rates." another potential benefit is that funds held in your bank account are FDIC-insured, which may not be the case with a nonbank P2P account.

Previous Story Table of Contents Next Story

Solutions

Customer & Channel Management

Account Aggregation Services

Bank Platforms

Biller Solutions

Branch Solutions

Credit Union Platforms

Electronic Billing & Payment Solutions

Lending Solutions

Loyalty & Reward Solutions

Mobile Solutions

Mobiliti

Mobiliti Enterprise

Mobiliti Advantage

Mobiliti Business

Mobiliti Edge

Mobiliti Reach

SpotPay

Mobile Source Capture

Mobile Access for Nautilus

Mobile Access for Director

Certainty and Confidence in Your Mobile Channel

Complete Mobile Payments

The Highest Mobile Adoption and Usage

Online Banking Solutions

Output Solutions

Personal Payments Services

Walk-In Solutions

Wealth Management Solutions

Insights & Optimization

Payments

Processing Services

Meet the growing demands of your customers' mobile banking needs and rapidly achieve a compelling return on investment with Mobile Solutions from Fiserv.

Consumers demand access to mobile banking, such as mobile person-to-person (p2p) payments. Offering your customers mobile banking solutions is a necessity in order to stay competitive in the financial services industry. It is important for businesses to adopt enterprise-wide mobile financial services strategies that will enhance your customers' banking experiences and at the same time give you significant returns on your investment. More financial institutions globally and in the U.S. trust mobile solutions from Fiserv than from any other vendor.

Our Solution

We offer the industry's leading mobile banking, alerting, database access, workflow, and payments solutions, perfect for banks and credit unions of all sizes. Our solutions offer a wealth of features that lower the total cost of ownership and help you to reach more consumers, including:

- The broadest range of mobile transactions, from simple banking inquiries to a complete set of mobile alerting and payment models, satisfying the needs of every customer segment
- Simultaneous support of all three mobile access modes – SMS, mobile browser and downloadable application – through a single integrated platform
- The most comprehensive enrollment and customer care tools and reporting across both the online and mobile channels
- Enterprise-grade channel management capabilities, including service analytics, security management, diagnostic resources and tools that facilitate full integration into the financial institution's core infrastructure assets
- Scalability to capitalize on new mobile channels, evolving technology and diverse customer segments
- A broad range of integration and pre-integration options to reduce the implementation workload on your organization
- Fully integrated mobile deposit
- Mobile access to your enterprise content management to electronically review and approve documents

Our mobile solutions are recognized as the best go-to-market solutions for financial institutions that are looking to satisfy today's needs for mobile banking while supporting the evolution of their mobile channel. We have the most sustainable, market-proven solutions available as evidenced by:

- Mobiliti™ from Fiserv Recognized as the Market Leader in the 2014 Ovum Global Mobile Banking Vendor Evaluation
- Fiserv has the fastest selling mobile solutions in the market with over 2,000 financial institutions having selected our mobile solutions

The Rise of the Mobivore: Serving the Mobile-Only Consumer

Many digital businesses are successfully serving these mobile-only users – or "mobivores" – but are financial institutions providing a compelling user experience for consumers who only want to interact and transact through their smartphones?

Read the blog

Mobile Banking for Business Gains Momentum

While many businesses are using or planning to adopt digital banking services, capitalizing on this opportunity isn't as simple as offering businesses the same digital services as retail accountholders.

Read the article

Mobiliti from Fiserv Recognized as the Market Leader in Ovum Global Mobile Banking Vendor Evaluation

Mobiliti™ mobile banking solution was named the market leader in "Ovum Decision Matrix: Selecting the Next Generation Mobile Banking Solution."

Read the press release

Recommended Resources

The Rise of the Mobivore: Serving the Mobile-Only User

Mobile-only users – or "mobivores" – are a fast growing segment in the mobile banking population. Serving the small but growing number of mobivores will require financial

EXHIBIT
K-16

Risk & Compliance

- Fiserv offers a full professional support staff to provide guidance and/or implementation expertise
- Fiserv provides best practices that are the result of ongoing investments in user experience research and testing, technology innovation, business intelligence and operational quality

Benefits

With Mobile Solutions, you'll be able to reach all your customers wherever they are. The benefits include:

- Achieving universal reach and driving the highest levels of mobile banking, alerting and payment adoption and usage, leading to the highest strategic yield
- Delivering the most complete mobile payments offering to your customers, including p2p payments, bill payments and payments at the point-of-sale
- Opening up new market segments, including satisfying the needs of technologically savvy consumers
- Saving money by serving consumers through the mobile channel, which costs less than traditional channels such as the branch and contact center
- Reducing your complexity by pre-integrating our product into existing industry products and services
- Providing the lowest possible implementation and operational risks through rigorous governance, security management and compliance measures

What We Offer

Mobiliti
Mobiliti™ from Fiserv is a hosted solution that gives community banks and credit unions the tools and expertise to deliver powerful, world-class mobile banking and payment services - with minimum impact on budgets, human resources and implementation timeframes.

Mobiliti Enterprise
Mobiliti Enterprise™ from Fiserv is an extensible, highly configurable, mobile financial services solution for mobile banking, alerts and payments. This mobile enterprise solution gives your financial institution complete control over what is offered as well as how those services are provided to your customers.

Mobiliti Advantage
Mobiliti Advantage™ from Fiserv is an out-of-the-box mobile banking solution for the U.S. market that can be deployed quickly, ensuring not only a quick jumpstart to your mobile strategy, but also support of seamless enhancements as this channel – and its users' needs – evolve over time

Mobiliti Business
Mobiliti Business™ from Fiserv is a hosted offering that enables you to deploy a scalable solution integrated with Business Online™. A turnkey product with flexible branding options, Mobiliti Business gets you up and running in the shortest amount of time possible.

Mobiliti Edge
With a focus on international markets, Mobiliti Edge™ from Fiserv delivers a comprehensive mobile financial services platform, which includes out-of-box mobile payments and enterprise alert capabilities.

institutions to think differently about the mobile channel.

Download the white paper

Sold! Cross-Selling in the Mobile Channel

Financial institutions have an opportunity to generate added value from the mobile channel through cross-selling products. With the right tools and technologies, selling of these products via the mobile channel will grow wallet and market share.

Download the white paper

Mobiliti Reach

Mobiliti Reach™ from Fiserv enables banks in emerging economies to deliver a complete and carrier-independent mobile banking and payments solution. Aimed for major banks in rapidly evolving economies, Mobiliti Reach will enable your organization to lead the way in reaching existing banked customers, and new unbanked and underbanked consumer segments.

SpotPay

SpotPay™ from Fiserv enables small businesses to accept credit and debit mobile payments anywhere, anytime, using a secure card reader attached to iOS or Android™ mobile devices, while financial institutions enjoy a new recurring income stream.

Mobile Source Capture

Given the popularity of smartphones, mobile deposits have emerged as an essential product for financial institutions to offer. Mobile Source Capture™ from Fiserv provides your customers and members the ultimate convenience in making a remote deposit.

Mobile Access for Nautilus

Financial institutions can't afford to limp along with operational inefficiencies. With Nautilus® from Fiserv, you can create, organize and control access for all types of content across your business from a single interface.

Mobile Access for Director

Director® from Fiserv manages virtually any document, including reports, check images, statements, notices, scanned documents and emails, helping your bank build an easily accessible information repository. This comprehensive solution contains dozens of integrated modules and works with our Premier®, Precision® and Cleartouch® account processing platforms.

Certainty and Confidence in Your Mobile Channel

Managing risks and maintaining customer confidence are vital to your financial institution. Fiserv delivers the organizational, product and operational confidence allowing financial institutions to get ahead of the curve while managing the risks associated with running the mobile channel.

Complete Mobile Payments

With our industry-leading solutions in payments, Fiserv empowers financial institutions to successfully deliver on all aspects of the emerging mobile ecosystem, including person-to-person payments, bill payment and payments at the point-of-sale.

The Highest Mobile Adoption and Usage

From our mobile adoption services to delivering a compelling user experience, Fiserv enables you to achieve the highest levels of mobile adoption and usage.

Contact Us About Mobile Solutions

© 2015 Fiserv, Inc., or its affiliates.

The New York Times

Bucks
Making the Most of Your Money

Person-to-Person Payments Get Easier at Big Banks

By **Tara Siegel Bernard**

May 25, 2011 5:58 pm

Three of the nation's biggest banks introduced a service that will enable their customers to move money from their checking accounts using only an e-mail address or a mobile phone number.

Bank of America, JPMorgan Chase and Wells Fargo already introduced the transfer service, called clearXchange, in Arizona, and it will roll out in more markets in coming months. It will be available nationwide within a year.

The new service will improve upon banks' existing person-to-person payment services, and it will compete directly with PayPal, which has shuttled money between consumers for years.

But the banks claim that their new service will be more convenient because it cuts out the middle man: PayPal isn't a bank, so you need to fund your account with money from a checking or other account. With the banks' service, the money will be ferried directly from your checking account to the person you want to pay. And it doesn't require you to dig around for a routing or other account number, as some services require.

"The key thing here is that you don't have to set up any additional accounts," said Mike Kennedy, head of payments strategy at Wells Fargo and chairman of clearXchange. "People have a primary savings and checking account with their institution and that is what they want to transact out of."

The new service should save consumers time — though paper checks and cash still work just fine. But it's unclear how much, if anything, it will cost. Pricing is up to

EXHIBIT
K-17

each participating bank. If banks do charge for the service, you'll have to figure out if the convenience factor makes it worthwhile.

So how will it work? Let's say you want to pay your friend back for dinner. If you both bank at any of the institutions in the network, you can reimburse your friend in a couple of ways. You can do it on the spot with your cellphone by accessing your bank's mobile application or mobile banking site. Or, you can do it from your bank's Web site on your computer.

Either way, you would then enter their name, mobile phone number or e-mail address, and the amount you want to transfer. There's also an optional "memo" field to note what the payment is for.

After you hit send, the recipient will then get an e-mail or text message that alerts them of your payment with instructions on how to make sure it lands in the correct account. The first time they use the service, they will need to register their e-mail or phone number so it's associated with their account.

That raised several concerns in my mind: What happens if you mistype your buddy's e-mail address or mobile phone number and the wrong person gets the message – will they be able to retrieve your money instead? Or what if someone hacks into your e-mail account and finds the note that someone wants to send you $200?

In all of those scenarios, bank executives said the potential thief would need to have your online banking user name and password. If someone did manage to break into your online banking account, they could conceivably send your money to their own account. That's not a new threat though. If a fraud were to occur, the banks said they would refund the person sending the money as soon as possible.

Many banks already offer person-to-person payment services. At ING Direct, for instance, you can send money from your phone or your computer using the person's name, e-mail address and the last four digits of their bank account number; you can save their information on a drop down menu for future payments. (ING customers with iPhones can also transfer money to one another by entering the amount in the bank's mobile app and "bumping" their phones).

But the banks that are part of the new exchange argue that their service makes the process even easier, for both senders and recipients. For instance, recipients in many existing services would need to enter their routing number on the bank site of the person sending them money. In the clearXchange system, they can retrieve their money using their own bank.

The exchange hopes to lure more institutions to its service – it's already discussing those possibilities with other big banks – which would increase the population of people who can transfer money this way. And eventually, the banks said they plan to offer the same service to customers who want to send money outside of the network.

Would you use the new service? And would you pay for it?

© 2015 The New York Times Company

Digitally Driven Neo-Consumer Gives Rise to Innovation in Banking

*by **Rod Hsu** on Jun 13, 2014 | **Technology**, **Research***

22 Tweet 4 Like 6 Share

It's no secret that for every day that passes, consumers are becoming increasingly connected to technology. With every new device, better network connection and fresh app, dependence on technology intensifies, ingraining itself further into our daily lives.

While digital usage is rapidly advancing across most segments of the population, one digitally savvy cohort in particular is leading the surge and consequently responsible for the proliferation of disruption across a host of industries.

Call them millennials, the social media generation, or neo-consumers – regardless of the classification the common thread found throughout this digitally driven generation is an obsession with personalization and instantaneity in all aspects of their lives. Yet, until recently, this cohort has been relatively unaddressed as a generation by financial institutions.

Conventional banks, unable to meet evolving customer needs through traditional service offerings, are beginning to adopt new technologies to digitize transactions. For example, the **Royal Bank of Canada** recently launched its RBC wallet to streamline contactless POS payments and add versatility to the user experience.

Yet, despite adoption of new digital products by these leading financial institutions, **a new study** reveals young Canadians are open to foregoing traditional brick-and-mortar banks in favor of online-only options. The study, released by Accenture, reports 40% of young respondents are looking to use an online-only bank.

This growing acceptance has already started to give rise to a new class of **online options**. While mobile and web components are a crucial part of the equation, the groundswell of popularity will result from their customer-centric user experience – a significant point of differentiation when compared to existing alternatives.

Specifically, to appeal to the neo-consumer segment, these online and mobile alternatives must include the following attributes:

- Zero fees: Free transactions (deposits, withdrawals, and money transfers between members)

Rod Hsu

Rod Hsu is President at nTrust, an online and mobile peer-to-peer money transfer platform that allows members to store, use and move money locally and around the globe as fast and seamlessly as sending a text. *» more*

Techvibes
Like
13,970 people like Techvibes.
Facebook social plugin

Who's Hiring

Hootsuite Media, Inc. 152 jobs
Vancouver, Canada

BrainStation 81 jobs
Toronto, Canada

43 jobs

EXHIBIT
K-18

- Simple, instant web and mobile interface: allows users real-time access to funds
- Increased user experience: integration with cutting-edge platforms like beacon technology
- Physical product: Pre-paid cards allow users to take funds offline
- Borderless: ability to easily transfer money internationally and access account while abroad
- Convenience: Ability to pay for goods or services – especially micro type purchases under $10 – via mobile devices further eliminates the need to carry cash

Additionally, as the future consumer becomes increasingly socially minded, this group will continue to opt for companies that enable social change. As we've seen with product-based companies like **TOMS** and **Warby Parker**, the service-based businesses that will succeed in the future will create opportunities for users to easily yet meaningfully **give back to communities**.

With a greater focus on convenience and access to finances, especially amongst **younger generations**, and ever-increasing digital demand, not only can we expect a surge in neo-banks, but the eventual decline of cash.

accenture

Company:
Accenture
Location:
Philadelphia, Pennsylvania, United States

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills, and technologies... ***» more***

Shopify
Ottawa, Canada

Cymax Stores Inc. 41 jobs
Burnaby, Canada

Mogo Finance Technology Inc. 29 jobs
Vancouver, Canada

ClearlyContacts.ca 29 jobs
Vancouver, Canada

Autodata Solutions 24 jobs
London, Canada

BCLC 22 jobs
Vancouver, Canada

Mobify 21 jobs
Vancouver, Canada

Intelex Technologies 14 jobs
Toronto, Canada

Recent Comments

- **Ski Baron**
  What a terrible article, can't believe you get paid to write this stuff unless it is Apple or Google paying you. You didn't mention anything about the new BB10 OS and basically just talk about...

  Falling Out of Love with BlackBerry · 16 minutes ago

- **charlie2010**
  re: " and found that its much-hyped keyboard swipe feature was more complicated than innovative. Gee, I guess the Red Dot design awards and high consumers ratings all got it wrong, guess they...

  Falling Out of Love with BlackBerry · 1 hour ago

- **AppleBerrySandwich**
  Curve is a piece of junk. I fell out of love with my Curve not long after I got it. Silly article.

  Falling Out of Love with BlackBerry · 3 hours ago

- **John Jones**
  Nothing different with other companies touchscreen phones either. I'd say Blackberry is the only one that is innovative . Qnx powered true multi tasking no app freezing no ancient home buttons....

0 Comments Techvibes - Technology News Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

AROUND THE WEB WHAT'S THIS?

Eater for Plated
Millennials Are Ditching Delivery for This Dinner Hack

Yahoo! Finance | Motif Investing
Will This Startup Kill The ETF Revolution?

Prophet
The Latest Thinking on Customer Experience: Download eBook

CreditCards.org
3 Credit Cards With Outrageous Cash Back Rewards

ALSO ON TECHVIBES - TECHNOLOGY NEWS

MakerBloks, GradeSlam and OfficeVibe Shine at TechCrunch Pitch … 3 comments

Apple Watch, Now Available to Preorder, is Extremely Expensive in … 3 comments

Privacy Commissioner Says Bell's Customer Surveillance … 3 comments

Falling Out of Love with BlackBerry 13 comments

Falling Out of Love with BlackBerry · 3 hours ago

Powered by Disqus

Subscribe Add Disqus to your site Privacy

Where Mobile Payments are Headed in 2015

*by **Rod Hsu** on Jan 6, 2015 | **Technology***

With the announcement of Apple Pay and Abiliba's global expansion, digital wallets and mobile payments became mainstream for consumers and small businesses in 2014, with 32% of consumers using alternative forms of payments this year.

As the affordability of mobile devices integrates them further into our daily lives, there's no doubt 2015 will be the year we see mainstream adoption from both consumers and businesses.

Looking ahead, there will be a few influential key points that will shape the mobile payment space in 2015.

Big Brand Adoption

Since Apple Pay put the spotlight on mobile payments, the perceptions of both consumers and businesses are shifting and becoming more open to alternative methods of payment. W

ith prominent **brands** debuting their mobile alternatives users are becoming increasingly comfortable with the idea of using the cloud to move their money, as a result we will see a big increase in user adoption in 2015.

Abandoning of Archaic Technology

As the United States gradually **moves away** from outdated swipe-and-sign payment systems, the need for innovative POS technology will emerge as a result of consumer demand and we will see North America's payment space drastically change. Businesses are becoming more open to accepting various forms of mobile payments, which will result in them adapting to a variety of technologies.

With more fraud accountability, businesses will be forced to adjust to the changing market to keep up with user demand and new legislation.

Big Data Continues to Reign

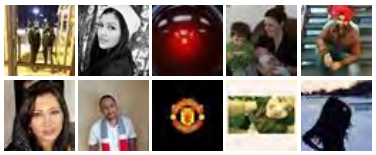
One of the biggest benefits to cashless transactions is big data. Harnessing the data gathered from online and mobile transactions will allow for targeted loyalty and a better understanding of customer information and trends.

Alternative payments will shape the future of retail and how merchants and businesses connect and communicate with their customers.

74 Tweet 16 Like

Rod Hsu

Rod Hsu is President at nTrust, an online and mobile peer-to-peer money transfer platform that allows members to store, use and move money locally and around the globe as fast and seamlessly as sending a text. *» more*

Techvibes
Like
13,970 people like Techvibes.

Facebook social plugin

Who's Hiring

Hootsuite	**Hootsuite Media, Inc.** Vancouver, Canada	152 jobs
	BrainStation Toronto, Canada	81 jobs
		43 jobs

EXHIBIT
K-19

Security is Vital

With a predicted increase in mobile activity, security will be tested and will need to adapt to the growing demand. The recent security breaches, such as that of **Target** or **Home Depot**, will leave doubt with consumers of whether or not mobile payments are trustworthy.

However, when choosing alternative forms of payments always look for security certification. Some alternative financial institutions offer equal security to that of traditional banks. For example, **nTrust** provides users the highest technical security standard in North America and is licensed, registered and regulated by FINTRAC.

Sophisticated Wearables

Wearables are just debuting to consumers but payment and financial institutions are only just starting to explore the integration within the payment space. With the high adoption of mobile banking and one-touch payment options, users are ready for contactless payments.

Wearables will continue to break into the market in 2015 and consumers are welcoming integrated payment options.

Out with the Old Bank

Traditional banking will need to modernize and find ways to cooperate and leverage services and offerings to compete with companies moving into the alternative payment space. Conventional banks have already started to co-brand with tech companies to provide alternative services to their customers.

2015 will be the year where we will see if traditional banks are able to seamlessly transition into the mobile payment space and offer their customers the latest cutting edge technology. They will need to keep working smarter to establish synergies in these market segments or they run the risk of being left behind.

Everything will be connected as mobile payments become mainstream; users are demanding a seamless user experience as well as additional features on top of payments and money transfers. To elevate their mobile payment platforms companies will be looking to merge the user experience of payment, loyalty cards and incentives; this is where the synergy in traction will come from in this space.

nTrust

Company:
nTrust
Location:
Vancouver, British Columbia, Canada

nTrust is the leader in convenient money transfer solutions that allow people to seamlessly transfer money anywhere in the world, helping our members enrich their lives, the lives of their friends and family, and their communities. nTrust was founded on the vision of creating a better way to send money whenever and wherever people need it most. In 2010, a trip overseas inspired the team to... *» more*

Shopify
Ottawa, Canada

Cymax Stores Inc. 41 jobs
Burnaby, Canada

Mogo Finance Technology Inc. 29 jobs
Vancouver, Canada

ClearlyContacts.ca 29 jobs
Vancouver, Canada

Autodata Solutions 24 jobs
London, Canada

BCLC 22 jobs
Vancouver, Canada

Mobify 21 jobs
Vancouver, Canada

Intelex Technologies 14 jobs
Toronto, Canada

Recent Comments

- **Ski Baron**
  What a terrible article, can't believe you get paid to write this stuff unless it is Apple or Google paying you. You didn't mention anything about the new BB10 OS and basically just talk about...

  Falling Out of Love with BlackBerry · 16 minutes ago

- **charlie2010**
  re: " and found that its much-hyped keyboard swipe feature was more complicated than innovative. Gee, I guess the Red Dot design awards and high consumers ratings all got it wrong, guess they...

  Falling Out of Love with BlackBerry · 1 hour ago

- **AppleBerrySandwich**
  Curve is a piece of junk. I fell out of love with my Curve not long after I got it. Silly article.

  Falling Out of Love with BlackBerry · 3 hours ago

- **John Jones**
  Nothing different with other companies touchscreen phones either. I'd say Blackberry is the only one that is innovative . Qnx powered true multi tasking no app freezing no ancient home buttons....

0 Comments Techvibes - Technology News Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

AROUND THE WEB WHAT'S THIS?

Hewlett-Packard
What If Your Internet Was 50 Times Faster? It's Coming

Instant Checkmate
Americans can't believe this new controversial website is legal!

CMSWire
Microsoft Makes Office 365 Cheap Enough That You Can Ignore Google

Brilliant Earth
6 Engagement Rings with Amazing Little Details

ALSO ON TECHVIBES - TECHNOLOGY NEWS

Canadian Crowdfunding Campaigns You May Want to Fund This Week 1 comment

Falling Out of Love with BlackBerry 13 comments

Free Tickets Now Available for Tech Fest Waterloo 1 comment

Augmented Reality, Meta Glasses Score Spotlight at We Are … 4 comments

Subscribe Add Disqus to your site Privacy

blog comments powered by Disqus

Falling Out of Love with BlackBerry · 3 hours ago

Powered by Disqus

Results **1** - **10** of about **57** for **conditional approval 304**. Search took **0.03** seconds.

Next >

Sort by date posted / Sort by relevance

[PDF] Conditional Approval #304 April 1999

... Comptroller of the Currency Administrator of National Banks Washington, DC
20219 **Conditional Approval #304** March 5, 1999 April 1999 **...**
www.occ.gov/static/interpretations-and-precedents/apr99/ca304.pdf - 66k - 1999-06-30

[PDF] Conditional Approval #304 April 1999

... Comptroller of the Currency Administrator of National Banks Washington, DC
20219 **Conditional Approval #304** March 5, 1999 April 1999 **...**
www.occ.gov/static/bit/ca304.pdf - 66k - 2009-12-07

[PDF] Conditional Approval #389 June 2000

... 12 See, OCC **Conditional Approval #304** (March 5, 1999) (**Approval** for Citibank NA to own indirectly a membership interest in three limited liability **...**
www.occ.gov/static/interpretations-and-precedents/jun00/ca389.pdf - 50k - 2013-01-02

[PDF] Conditional Approval #317 August 1999

... Del. Code. Ann. tit. 6, § 17 (1999). 13 **Conditional Approval** No. **304** (Mar. 5, 1999) (approving the use of both the cost and **...**
www.occ.gov/static/interpretations-and-precedents/aug99/ca317.pdf - 47k - 1999-09-09

[PDF] Conditional Approval #361 March 2000

... 332 (October 18, 1999) and **Conditional Approval** No. **304** (March 5, 1999) (national banks may provide electronic bill presentment and payment **...**
www.occ.gov/static/bit/ca361.pdf - 94k - 2009-12-07

[PDF] Conditional Approval #332 November 1999

... 304 (March 5, 1999) (national banks may invest in an LLC that will offer 9 electronic bill presentment and payment services); **Conditional Approval ...**
www.occ.gov/static/interpretations-and-precedents/nov99/ca332.pdf - 56k - 1999-12-06

OCC: OCC Opinions and Letters on Permissible Electronic **...**

... Conditional Approval No. 332. Transpoint, **Conditional Approval** No. **304** (March 5, 1999). **... Conditional Approval** No. **304**. 2. Stored Value. **...**
www.occ.gov/topics/bank-operations/bit/opinions-and-letters.html - 115k

Related Searches

conditional approval
occ conditional approval
1999 conditional approval
304 march 5 1999 electronic
304 march 5 1999 national
18 1999 conditional approval
approval 304 march 5 1999
conditional approval 304 march 5
see eg occ conditional approval

EXHIBIT K-20

[PDF] **Conditional Approval** 882

... Conditional Approval #882 November 2008 **...** Middletown, New York ("the Bank") to establish a branch at 715 Route **304**, Bardonia, Rockland County **...**
www.occ.gov/static/interpretations-and-precedents/nov08/ca882.pdf - 11k - 2008-11-18

[PDF] **Conditional Approval** #332 November 1999

... 304 (March 5, 1999) (national banks may invest in an LLC that will offer 9 electronic bill presentment and payment services); **Conditional Approval ...**
www.occ.gov/static/bit/ca332.pdf - 56k - 2009-12-07

[PDF] **Conditional Approval** #361 March 2000

... 332 (October 18, 1999) and **Conditional Approval** No. **304** (March 5, 1999) (national banks may provide electronic bill presentment and payment **...**
www.occ.gov/static/interpretations-and-precedents/mar00/ca361.pdf - 94k - 2000-03-27

1 2 3 4 5 6 **Next**

conditional approval 304 **Search**

Search Within Results
Advanced Search
Search Tips

Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

Conditional Approval #304
April 1999

March 5, 1999

Mr. John S. Rudman
Vice President
Citibank, N.A.
425 Park Avenue
New York, New York 10043

Re Application by Citibank, N.A. to invest in three Limited Liability Companies through an existing operating subsidiary
Application Control No. 1998-WO-08-0028

Dear Mr. Rudman:

This is in response to the operating subsidiary application ("Application") submitted by Citibank, N.A., New York, New York ("Citibank" or "Bank"). Pursuant to Section 5.34(e)(1) of the regulations of the Comptroller of the Currency ("OCC"), 12 C.F. R. § 5.34(e)(1), Citibank proposes to indirectly own a membership interest in three limited liability companies, TransPoint, L.L.C. ("TransPoint"), TransPoint Technology & Services, L.L.C. ("Technology"), and TransPoint Accounting, L.L.C. ("Jointco") (collectively, the "LLCs") and thereby engage in electronic bill payment and presentment services over the Internet. Citibank will hold its interest in the LLCs through an existing, wholly owned operating subsidiary, Citicorp Electronic Commerce Inc. ("CECI"). For the reasons discussed below, the application is approved, subject to the conditions set forth herein.

A. Background

By agreements dated August 31, 1998, CECI and MSFDC (a joint venture between Microsoft Corporation ("Microsoft") and First Data Corporation ("First Data") (collectively, "Owner Companies") agreed to form a joint venture that will offer electronic bill payment and presentment services over the Internet. The agreements contemplate the creation of two new limited liability companies: (1) TransPoint; and (2) Technology (whose members will be CECI and MSFDC).[1]

[1] The agreements also contemplate the formation of Jointco as a subsidiary of Technology and TransPoint, to be owned equally by both. Therefore, Jointco will be indirectly owned by Citibank, through CECI, by TransPoint and Technology.

EXHIBIT
K-21

Through TransPoint and Technology, Citibank and MSFDC will offer electronic bill payment and presentment services over the Internet.

TransPoint is expected to have title to consumer contracts, trademarks and certain other intangible assets. Technology will act as a subcontractor to TransPoint and will perform payment and information processing services on behalf of TransPoint. Jointco, which exists for tax and accounting convenience, will not perform any services other than accounting services. In addition, the LLCs will rely upon the services of the Owner Companies and third party vendors. Pursuant to the LLC Agreements, TransPoint, Technology, and Jointco will perform adequate due diligence of all vendors with which each such company will do business to ascertain any such vendor's compliance with FFIEC guidance with respect to Year 2000 related issues.[2]

CECI will have a 5 percent membership interest in TransPoint and a 25 percent membership interest in Technology. CECI will obtain its interest in TransPoint in exchange for a capital contribution. MSFDC will be a 95 percent member of TransPoint, contributing goodwill and biller contracts. Both members of Technology will make an initial capital contribution to Technology composed of cash, intellectual property or other specified property. Upon making such capital contributions, CECI will have an initial membership interest of 25 percent of Technology and MSFDC will have a 75 percent membership interest. Profits and losses for each LLC will be shared in proportion to the members' proportional interests in the particular LLC. Both TransPoint and Technology will be individually managed by a Board of Directors. In the case of TransPoint, each Owner Company will be entitled to designate one director. In the case of Technology, each Owner Company will name two directors to its Board.

TransPoint initially will engage in one activity that provides a service to consumers, enabling them to electronically pay bills that TransPoint presents electronically. This activity has two components. The first component, bill presentment, allows sellers and service providers, such as utilities, to effect Internet presentment of bills directly to a customer's desktop computer. The second component, bill payment services, involves a return payment on presented bills which can also be electronically made and includes both remittance and posting to bank accounts. More specifically, the service operates in the following manner. Bills that would have been rendered in print form are produced in an electronic form and sent to the TransPoint Service Center. The Service Center consolidates bills from a number of billers so that consumers may view all their bills in one Web site. Consumers may

---

[2] Citibank represents that the LLCs internal data processing systems will be year 2000 ready within the time frames specified in OCC Advisory Letter 97-6 and other subsequent OCC issuances. The LLCs are performing due diligence to ensure that any and all third-party data processing service providers or purchased applications or systems it uses, including those provided by the Owner Companies, will be year 2000 compliant in accordance with OCC issuances. Further, the LLCs are conducting and will continue to conduct extensive testing on all external parties that interface with the LLCs, notably financial institutions and billers, to ensure they are year 2000 compliant. Moreover, pursuant to condition number four of this letter, the LLCs are subject to OCC supervision, examination, and regulation, including with respect to year 2000 readiness.

access their bills by visiting a single Web site which seamlessly lets them view bills produced from the Service Center. Consumers then review bills and schedule payments. Electronic remittance information is returned to the biller and payments are routed either directly to the biller or the biller's lockbox provider.

Citibank expects the LLCs to make their services available through a variety of channels including financial institutions' or other financial service providers' on-line banking programs and Internet gateways or portals such as the Microsoft Network (MSN) and Microsoft.com. The LLCs will also make their services available to consumers directly through their own Web site.[3]

Generally, for the bill presentment component, TransPoint will contract directly with billers. However, in some cases, TransPoint will enter into contracts with entities called biller service providers. These biller service providers will then act as subcontractors to TransPoint in the electronic bill presentment service. In both cases, the arrangement will take the form of a service agreement, which will contain contractual protections for TransPoint such as limits on liability and waivers of certain types of damages and warranties.

Although specific operational roles are not settled for the bill payment component, TransPoint will serve as an intermediary, subcontracting to third party vendors as necessary.[4] If TransPoint receives funds in its own name, these funds will be held in a trust account pending payments settlement. TransPoint, however, expects that it will have no risk exposure in the clearing and settlement process for bill payment. TransPoint will use the ACH, or other such batch settlement to effect clearing and settlement, making payment to billers only after it has received final payment for funds from a consumer, or a consumer's financial services provider. Furthermore, TransPoint will have no contractual obligation to make any payment until it has received any required funds. Moreover, in the event any payment to a biller (whether accomplished via the ACH or other batch settlement) is

---

[3] Under the Electronic Fund Transfer Act ("EFTA"), 15 U.S.C. § 1693, and Federal Reserve Board's implementing regulation, Regulation E (12 C.F.R. Part 205), TransPoint is required when dealing directly with consumers to provide a number of disclosures to consumers in writing, including error resolution procedures, fees and charges, change in terms notices, liabilities for unauthorized use, and service provider's liability. Citibank has represented that TransPoint will charge no fees to consumers for its services. In addition, Citibank has represented that TransPoint will provide any and all disclosures consistent with Regulation E to its direct consumers. Financial intermediaries will be responsible for providing such disclosure to those consumers who receive services indirectly from TransPoint. The Federal Reserve Board is in the process of amending Regulation E and issued an interim rule effective March 25, 1998, which authorizes electronic disclosure with consumer consent. The OCC expects that TransPoint will comply with the interim and final rules, including with respect to its plans to send EFTA disclosures to its direct consumers via electronic means.

[4] The OCC expects that TransPoint will develop and implement a risk management plan that identifies all specific material risks and identifies mechanisms that it will use to manage and control those risks. The OCC will evaluate the adequacy of this risk management plan as part of its on-going supervision of the LLCs.

reversed for any reason, TransPoint's contract with the biller will permit TransPoint to initiate a debit entry to the biller's account.[5]

B. Analysis

A national bank may engage in activities that are part of or incidental to the business of banking by means of an operating subsidiary. 12 C.F.R. § 5.34. In a variety of circumstances, the OCC has permitted national banks to own, either directly, or indirectly through an operating subsidiary, a minority interest in an enterprise.[6] The OCC has concluded that national banks are legally permitted to make a minority investment in a company provided four criteria or standards are met.[7] These standards, which have been distilled from our previous decisions in the area of permissible minority investments for national banks and their subsidiaries, are:

> (1) *The activities of the enterprise in which the investment is made must be limited to activities that are part of or incidental to the business of banking.*
>
> (2) *The bank must be able to prevent the enterprise from engaging in activities that do not meet the foregoing standard, or be able to withdraw its investment.*
>
> (3) *The bank's loss exposure must be limited, as a legal and accounting matter, and the bank must not have open-ended liability for the obligations of the enterprise.*

---

[5] In connection with the services that it provides directly to customers or indirectly through financial intermediaries such as banks, TransPoint may have access to personal and private customer information, including financial and account information. In this regard, TransPoint has adopted a statement of Information Privacy Principles that governs the daily operations of the Internet bill presentment and payment service and the collection, retention, and use of personal and private customer information. Under the statement, TransPoint represents that it does not share such customer information with any third parties for any reason whatsoever, except to comply with appropriate legal and regulatory processes. Personal and private customer information will be maintained subject to established security, confidentiality, and accuracy standards intended to preclude unauthorized access or disclosure of customer information. TransPoint will require through contract that all business partners, including financial intermediaries that indirectly offer TransPoint's services to their customers, uphold the same standards for the protection and processing of personal and private customer information. Citibank represents that TransPoint will monitor compliance with the requirements in this statement through its internal audit program, will provide appropriate employee training and communication, and will take appropriate disciplinary measures to enforce the privacy commitments contained in the statement.

[6] *See, e.g.*, OCC Conditional Approval Letter No. 219 (July, 15, 1996).

[7] *See* Interpretive Letter No. 692, *reprinted in* [1995-1996 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81,007 (November 1, 1995), and OCC Interpretive Letter No. 694, *reprinted in* [1995-1996 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81,009 (December 13, 1995).

(4) *The investment must be convenient or useful to the bank in carrying out its business and not a mere passive investment unrelated to that bank's banking business.*

We conclude, as discussed below, that Bank's proposed acquisition of membership interests in LLCs satisfies these four criteria.

1. The activities of the enterprise in which the investment is made must be limited to activities that are part of or incidental to the business of banking

OCC precedents on non-controlling ownership have recognized that the enterprise in which a national bank takes an equity interest must confine its activities to those that are part of, or incidental to, the business of banking. As described in greater detail above, Citibank represents that the LLCs will engage in electronic bill payment and presentment services over the Internet. These activities are part of the business of banking and permissible for national banks under 12 U.S.C. § 24 (Seventh).

Bill presentment involves the aggregation, storage, and transmission of billing information from businesses to their customers. It can be done in several ways.[8] However, in this case, the LLCs will operate as an Internet-based consolidator of biller information so that customers of participating billers can obtain billing information from all their participating billing firms by accessing a single Web site. The LLCs will obtain charges and related information from billers and then provide an electronic system by which customers of billers can retrieve that information. The amount of information provided to customers of billers by the LLCs will vary and be determined largely by each participating biller. Some billers will elect to provide only summary information and payment execution, others may also provide bill details and other related information directly through the LLC and indirectly through hyperlinks from LLCs' Web site to the biller's Web site.

The OCC has found that electronic bill presentment is part of the business of banking.[9] This conclusion is well supported by judicial and agency precedent. The Supreme Court has found that 12 U.S.C. §24(Seventh) permits a national bank to "do those acts and occupy those relations which are usual or necessary in making collections of commercial paper and other evidences of debt" for its customers.[10] Similarly, the courts have recognized that "a traditional banking function [is]

---

[8] *See, e.g.,* Furst, Lang and Nolle "Technological Innovations in Banking and Payments," *OCC Quarterly Journal*, Vol. 17, No. 3 (Sept. 1998) at 27-28 and "Online bill presentment set to explode," *Online Banking Newsletter*, Vol. 2, Issue 32 (August 11, 1997).

[9] *See* Conditional Approval No. 221 (Dec. 4, 1996) (national banks may establish and electronic gateway to support, among other things, electronic bill presentment).

[10] *Miller v. King*, 223 U.S. 505, 510 (1912).

collecting and remitting funds for other parties."[11] Thus, OCC has long held that billing and collecting services are permissible for national banks, whether done conventionally[12] or electronically.[13] The OCC has also recognized that as part of an electronic collection or payments process, national banks may store and transmit information related to the underlying transactions such as electronic data interchange.[14]

The proposed bill payment function in this case involves not only the transmission of the payment order or electronic funds transfer from the customer to the appropriate party (e.g., the biller's bank) but also of the remittance information from the customer to the biller. Again there a number of different ways that this can be arranged.[15] Clearly, the electronic transmission of payments orders with related information is part of the business of banking.[16]

Accordingly, the activities in which the LLCs will engage are part of the business of banking.[17] Thus, the first standard is satisfied.

2. The bank must be able to prevent the enterprise from engaging in activities that do not meet the foregoing standard, or be able to withdraw their investment

---

[11] *Corbett v. Devon*, 12 Ill. App.3d 559, 299 N.E.2d 521, 529 (App. Ct. 1st Cir. 1973).

[12] OCC Interpretive Letter No. 712, *reprinted in* [1995-1996 Transfer Binder] Fed. Banking Law. Rep. (CCH) ¶ 81-027 (February 29, 1996) (billing and collection services for medical service providers); Unpublished Letter from Peter Liebesman, Assistant Director, Legal Advisory Services Division (August 27, 1985) (billing services).

[13] OCC Interpretive Letter No. 836, *reprinted in* [1996-1997 Transfer Binder] Fed. Banking Law. Rep. (CCH) ¶ 81-290 (March 12, 1996) (data processing and electronic data interchange system to assist in the billing and collection for medical services); OCC Interpretive Letter No. 731, *reprinted in* [1995-1996 Transfer Binder] Fed. Banking Law. Rep. (CCH) ¶ 81-048 (July 1, 1996)(operation of electronic toll collection system).

[14] OCC Interpretive Letter No. 836, *supra*; OCC Interpretive Letter No. 732, *reprinted in* [1995-1996 Transfer Binder] Fed. Banking Law. Rep. (CCH) ¶ 81-049 (May 10, 1996); OCC Interpretive Letter No. 653, reprinted in [1994-1995 Transfer Binder] Fed. Banking Law. Rep. (CCH) ¶ 83,601 (Dec. 22, 1994); OCC Interpretive Letter No. 419, *reprinted in* [1988-1989 Transfer Binder] Fed. Banking Law. Rep. (CCH) ¶ 85,643 (Feb. 16, 1988).

[15] *See*, *e.g.*, *Electronic Bill Payment/Presentment Business Practices: Draft for Public Comment*, Bill Payment Council, November 12, 1998 (http:\\www.nacha.org\billpay).

[16] *See*, *e.g.*, OCC Interpretive Letter No. 653, supra.

[17] Citibank represents and undertakes that the activities of the operating subsidiary will be conducted in accordance with OCC policies. In addition, each of the Agreements specifies that TransPoint, Technology, and Jointco will be subject to the examination, supervision, and regulation of the OCC.

This is an obvious corollary to the first standard. It is not sufficient that the entity's activities are permissible at the time a bank initially acquires its interest; they must also remain permissible for as long as the bank retains an ownership interest.

The limited liability company agreements ("Agreements") under which LLCs are to be formed contain provisions to ensure that LLCs will engage only in activities that are permitted for national banks and their subsidiaries. In particular, the Agreements provide that their respective LLC will not engage in an activity which is impermissible for a national bank or an operating subsidiary thereof. Moreover, in the event the OCC determines that an activity is impermissible, each LLC will have 30 days to cease engaging in the activity, modify the activity to comply with the OCC's determination, or determine to continue to engage in the activity. In the event the last option is selected, CECI has represented that it will withdraw from each LLC.

Accordingly, the second standard is satisfied.

3. The bank's loss exposure must be limited, as a legal and accounting matter, and the bank must not have open-ended liability for the obligations of the enterprise

a. Loss exposure from a legal standpoint

A primary concern of the OCC is that national banks should not be subjected to undue risk. Where an investing bank will not control the operations of the entity in which the bank holds an interest, it is important that a bank's investment not expose it to unlimited liability.

With respect to the third standard, Citibank's loss exposure is limited, and CECI does not have open-ended liability for the obligations of the LLCs. Bank's risk of loss will be limited by both the corporate veil of the operating subsidiary and by Delaware law. As a legal matter, investors in a Delaware limited liability company do not incur liability with respect to the liabilities or obligations of the limited liability company solely by reason of being a member or manager of the limited liability company. Del. Code Ann. Tit. 6, § 18-303 (Michie Cum. Supp. 1996).[18] In addition, the Agreements provide that: (i) no member of LLCs shall have the authority to bind an LLC of which it is a member; and (ii) the members of LLCs are not liable for the debts, obligations or liabilities of an LLC of which it is a member. Thus, the Bank's loss exposure for the liabilities of the LLCs will be limited by statute and by the Agreements establishing LLCs.

b. Loss exposure from an accounting standpoint

---

[18] In addition, the Agreements establishing LLCs specifically provide that none of the members shall be personally liable for any debts, obligations or liabilities of LLCs.

In assessing a bank's loss exposure as an accounting matter, the OCC has previously noted that the appropriate accounting treatment for a bank's less than 20 percent ownership share or investment in a corporate entity is to report it as an unconsolidated entity under the equity or cost method of accounting. The Bank has advised the OCC that the accounting treatment for its 5 percent investment in TransPoint (through CECI) is under the cost method of accounting. Under the cost method of accounting, losses recognized by the investor will not exceed the amount of the investment (including extensions of credit or guarantees, if any) shown on the investor's books.

Additionally, the OCC has previously noted that the appropriate accounting treatment for a bank's 20 to 50 percent investment in a company is to report it as an unconsolidated entity under the equity method of accounting. Bank will account for its 25 percent investment in Technology (through CECI) under the equity method of accounting. Under the equity method of accounting, unless the bank has guaranteed any of the liabilities of the entity or has other financial obligations to the entity, losses are generally limited to the amount of the investment, including loans and other advances shown on the investor's books. Thus, Bank's loss, through CECI, from an accounting perspective would be limited to the amount invested in Technology and Bank will not have any open-ended liability for the obligations of Technology.

Accordingly, for legal and accounting purposes, the Bank's potential loss exposure, through CECI, should be limited to the amount of CECI's investment in the LLCs. Since that exposure will be quantifiable and controllable, the third standard is satisfied.

4. The investment must be convenient or useful to the bank in carrying out its business and not a mere passive investment unrelated to that bank's banking business.

A national bank's investment in an enterprise or entity must also satisfy the requirement that the investment have a beneficial connection to the bank's business, *i.e.*, be convenient or useful to the investing bank's business activities, and not constitute a mere passive investment unrelated to that bank's banking business. Twelve U.S.C. § 24(Seventh) gives national banks incidental powers that are "necessary" to carry on the business of banking. "Necessary" has been judicially construed to mean "convenient or useful."[19] Our precedents on bank non-controlling investments have indicated that the investment must be convenient or useful to the bank in conducting *that bank's* business. The investment must benefit or facilitate that business and cannot be a mere passive or speculative investment.[20]

---

[19] *See Arnold Tours, Inc. v. Camp*, 472 F.2d 427, 432 (1st Cir. 1972).

[20] *See, e.g.*, Interpretive Letter No. 543, *reprinted in* [1990-1991 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 83,255 (February 13, 1991); Interpretive Letter No. 427, *reprinted in* [1988-1989 Transfer Binder] Fed. Banking L.

In this instance, the proposed share ownership by Citibank is not merely evidence of a passive relationship, but is rather the result of the strategic business relationship created between Citibank and Owner Companies as evidenced by the organization of the LLCs. Citibank and Owner Companies plan to develop a fully-integrated electronic bill payment and presentment system to be offered to businesses, banks, and other customers. The ownership interests to be held by Citibank in the LLCs provide the method of involving Citibank in the provision of the bill payment and related services contemplated by this application, and of compensating Citibank for what it brings to the LLCs. In addition, the Bank's investment in the LLCs will be convenient and useful to Citibank in allowing it to provide additional services to its customers, as well as to gain additional expertise in the provision of banking services over the Internet, in general, and electronic bill payment and presentment, in particular. Thus, the investment is not a mere passive investment unrelated to Bank's banking business.

Accordingly, the fourth standard is satisfied.

C. Conclusion

Based upon the information and representations you have provided, and for the reasons discussed above, we conclude that the Bank may invest in the LLCs,[21] and that the application are approved subject to the conditions:

1. The LLCs may engage only in activities that are part of, or incidental to, the business of banking;

2. The Bank, through CECI, will have veto power over any activities of the LLCs that are inconsistent with Condition 1, or will withdraw from the LLCs in the event they engage in an activity inconsistent with Condition 1.

Rep. (CCH) ¶ 85,651 (May 9, 1988); Interpretive Letter No. 421, *reprinted in* [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,645 (March 14, 1988).

[21] While not currently incorporated in the service, the joint venture plans to add two additional activities. One activity would allow businesses to present bills to other businesses. A second activity would allow consumers to use the service to pay any bill, even bills not initially presented through the service. Citibank seeks authority to retain its investment in the venture upon its commencement of these activities. However, the OCC currently does not have sufficient information on these activities to determine whether to approve such activities. Accordingly, this letter considers only the pending application by Citibank to make minority investments in LLCs as they are currently structured. The OCC will consider any additional activities pursuant to 12 C.F. R. § 5.34 when all of the facts and circumstances surrounding them are provided by Citibank.

3. The Bank will account for their investment in the LLCs under the equity or cost method of accounting; and

4. The LLCs will be subject to OCC supervision, regulation, and examination.[22]

The conditions of this approval are "condition[s] imposed in writing by the agency in connection with the granting of any application or other request" within the meaning of 12 U.S.C. § 1818. As such, the conditions are enforceable under 12 U.S.C. § 1818.

If you have any questions regarding this decision, please contact John W. Graetz, Licensing Expert (Financial Analyst), in Bank Organization and Structure at (202) 874-5060, or John Soboeiro, Senior Attorney, Bank Activities and Structure at (202) 874-5300.

Sincerely,

/s/

Julie L. Williams
Chief Counsel

---

[22] Elements of the services to be provided by the LLCs will be performed by the Owner Companies. These services will constitute activities pursuant to the Bank Service Company Act. (12 U.S.C. § 1861 *et seq.* ("BSCA")). To the extent that Owner Companies perform these services for banks through the LLCs, Owner Companies would be subject to federal banking regulation and examination to the same extent as if such services were being performed by banks themselves. *See* BSCA § 1867(c).

Results **1** - **10** of about **43** for **conditional approval 389**. Search took **0.03** seconds.

Next >

Sort by date posted / Sort by relevance

[PDF] Conditional Approval #389 June 2000

Page 1. O Comptroller of the Currency Administrator of National Banks Washington, DC 20219 **Conditional Approval #389** May 19, 2000 June 2000 **...**
www.occ.gov/static/interpretations-and-precedents/jun00/ca389.pdf - 50k - 2013-01-02

Related Searches

conditional approval
ii supra 389 legal basis
occ conditional approval
supra 389 legal basis investment
389 legal basis investment banking
conditional approval letter
decision occ conditional approval

[PDF] Conditional Approval #220 December 1996

... See, eg, OCC **Conditional Approval** Letter No. **...** of all financial transactions." R. Miller and D. VanHoose, Modern Money and Banking **389**-91 (3d ed **...**
www.occ.gov/static/interpretations-and-precedents/dec/conda220.pdf - 81k - 1999-05-08

[PDF] Conditional Approval #297 January 1999

... Conditional Approval #297 **...** performed by a qualified credit analyst and the **approval** of the **...** II, supra at **389** ("The legal basis for investment banking **...**
www.occ.gov/static/interpretations-and-precedents/jan99/ca297.pdf - 145k - 1999-05-08

[PDF] Conditional Approval #220 December 1996

... See, eg, OCC **Conditional Approval** Letter No. **...** of all financial transactions." R. Miller and D. VanHoose, Modern Money and Banking **389**-91 (3d ed **...**
www.occ.gov/static/bit/ca220.pdf - 81k - 2009-12-07

[PDF] Conditional Approval #331 November 1999

... 1999 ("First Tennessee Decision"), OCC **Conditional Approval** No. **...** terms and conditions of this **approval** to be **...** II, supra at **389** ("The legal basis for **...**
www.occ.gov/static/interpretations-and-precedents/nov99/ca331.pdf - 169k - 1999-12-06

[PDF] Conditional Approval #262 December 1997

... Conditional Approval #262 **...** National Bank in Connection with Application for **Approval** (August 13 **...** II, supra at **389** ("The legal basis for investment **...**
www.occ.gov/static/interpretations-and-precedents/dec97/ca262.pdf - 237k - 1999-05-08

[PDF] Conditional Approval #241 May 1997

... Conditional Approval #241 **...** The **approval** of the majority-in-interest of the partners will be required **...** **389**, reprinted in[1988-1989 Transfer Binder] Fed **...**
www.occ.gov/static/interpretations-and-precedents/may97/ca241.pdf - 46k - 1999-05-08

EXHIBIT K-22

[PDF] **Conditional Approval** #309 May 1999

... See 12 CFR §5.34(e)(2)(ii)(J). See also **Conditional Approval** Letter No **...** II, supra at **389** ("The legal basis for investment banking activities of national **...**
www.occ.gov/static/interpretations-and-precedents/may99/ca309.pdf - 162k - 1999-05-28

[PDF] **Conditional Approval** #351 February 2000

... 1999) ("Commerce II Decision"), OCC **Conditional Approval** No. **...** conjunction with an application **approval**, and any **...** II, supra at **389** ("The legal basis **...**
www.occ.gov/static/interpretations-and-precedents/feb00/ca351.pdf - 144k - 2000-03-08

[PDF] Investment in Subsidiaries and Equities

... 12 See, for example, **Conditional Approval** No. 322 (July 30, 1999); **Conditional Approval** No. **...** **389**, supra; Interpretive Letter No. 244 (Jan. **...**
www.occ.gov/publications/publications-by-type/licensing-manuals/opsubs.pdf - 614k - 2014-12-17

1 2 3 4 5 **Next**

conditional approval 389 **Search**

Search Within Results
Advanced Search
Search Tips

Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

Conditional Approval #389
June 2000

May 19, 2000

Mr. Joseph R. Bielawa
Vice President and Assistant General Counsel
Chase Manhattan Bank USA, N.A.
Legal Department
270 Park Avenue, 39th Floor
New York, NY 10017

Robert L. Andersen
Senior Vice President & Assistant General Counsel
First Union Corporation
One First Union Center (0630)
Charlotte, North Carolina 28288

Robert G. White
Vice President & Senior Counsel
Wells Fargo Law Department
633 Folsom Street, 7th Floor
San Francisco, California 94107

Re Application by Chase Manhattan Bank USA, N.A., Wilmington, Delaware, First Union National Bank, Charlotte, North Carolina, and Wells Fargo Bank, N.A., San Francisco, California to continue to invest in a limited liability company.
Application Control No. 2000-WO-08-0004

Dear Messrs. Bielawa, Andersen, and White:

This is in response to your application of February 29, 2000, and supplemented by letter of April 19, 2000, pursuant to section 5.34(e)(1) of the regulations of the Office of the Comptroller of the Currency (AOCC≅), 12 C.F.R. э 5.34(e)(1), proposing that several national banks (ABanks≅)[1] be

[1] The national banks joining in this request are: Chase Manhattan Bank USA, N.A., Wilmington, Delaware; First Union National Bank, Charlotte, North Carolina; and Wells Fargo Bank, N.A., San Francisco, California.

EXHIBIT
K-23

approved to hold noncontrolling interests in a limited liability company (collectively, "Applications"). Currently, the Banks' operating subsidiaries own membership interests in a limited liability company, Spectrum EBP, LLC ("LLC"), which engages in electronic bill presentment services over the Internet.[2] The Banks wish to continue, through their operating subsidiaries, as noncontrolling investors in the LLC after the LLC expands its activities to include the electronic payment of bills, transfer of money, and related data processing for these services. For the reasons discussed below, the Applications are approved, subject to the conditions set forth herein.

A. Background

The LLC currently provides a Aswitch@ through which bank customers and others are able to receive bills electronically from a variety of sources. The LLC has developed standards for the electronic presentation of billing information, creating a biller file and biller directory, and entering into relationships and arrangements with a variety of entities in order to receive bills from billers and route bills to a large number of customers. In addition to acting as a switch, the LLC translates the billing information into electronic format.[3]

The LLC proposes to provide electronic payment services to complement its electronic bill presentment services. Specifically, the LLC intends to develop a complete payment system that will permit the payment of electronically presented bills and provide data processing related to those payments for the LLC participants who operate bill presentment Internet sites. The LLC also proposes to provide a payment service that would allow the customers of a participating customer service provider ("CSP") to make electronic payments that would not be linked to a presented bill. This service would allow customers of a participating customer service provider to pay another person without the presentation of a bill through the LLC and under circumstances where a debtor/creditor relationship does not exist.[4]

The proposed service would operate in the following manner. A customer provides payee information from her personal computer to her bank's computer banking site. The customer's CSP receives a payment request and payee information and forwards them to the LLC. The CSP receives the payment instruction and deducts the amount from the customer's transaction account. The LLC receives payee information and posts it to the payee directory. The LLC debits the payment amount to CSP through the LLC settlement system and forwards payment

---

[2] The OCC approved the subsidiaries' investment in the LLC's current activities in Conditional Approval No. 332 (October 18, 1999) ("Spectrum Letter").

[3] For more detailed information concerning the current operations of the LLC, see the Spectrum Letter.

[4] The OCC expects that the LLC will modify and implement any existing risk management plan to identify the specific material risks associated with the added service; including monitoring the transaction flow for patterns of transactions that might indicate unauthorized use of CSP customer funds. The OCC will evaluate the adequacy of any risk management plan as part of its on-going supervision of the LLC.

instruction to the check printing facility to issue a check.[5] A check drawn on the LLC's account is then cut and mailed to the appropriate payee. In addition, the LLC's payment system will process and settle payment transactions.

Although the LLC will establish relationships with a number of CSPs, each CSP will have access only to that information related to its own customers. In connection with these services, the LLC may have access to personal customer information, including financial and account information. It is understood that the LLC will not share such customer information with any third parties except where the information is needed in order for the LLC to complete a transaction.[6]

B. Analysis

A national bank may engage in activities that are part of or incidental to the business of banking by means of an operating subsidiary.[7] In a variety of circumstances, the OCC has permitted national banks to own, either directly, or indirectly through an operating subsidiary, a noncontrolling interest in an enterprise.[8] The OCC has concluded that national banks are legally permitted to make a noncontrolling investment in a company provided four criteria or standards are met.[9] These standards, which have been distilled from our previous decisions in the area of permissible noncontrolling investments for national banks and their subsidiaries, are:

> (1) The activities of the enterprise in which the investment is made must be limited to activities that are part of, or incidental to, the business of banking (or otherwise authorized for a national bank).
>
> (2) The bank must be able to prevent the enterprise from engaging in activities that do not meet the foregoing standard, or be able to withdraw its investment.

---

[5] Alternatively, the LLC may outsource its payment system, directory maintenance and check printing.

[6] The LLC may share customer information in response to a subpoena where required by a law or order of a court or arbitrator, or in connection with a lawful investigation or examination; and with the LLC's subcontractors, processors, auditors or other third parties that assist the LLC in fulfilling its contractual obligations to a CSP. In sharing with third parties, the LLC requires such third parties to abide by the confidentiality principles adopted by the LLC. The LLC will monitor compliance with the requirements in this statement through its internal audit program, will limit its employees' and others' access to information, will maintain and require subcontractors and others to maintain security standards and procedures intended to preclude unauthorized access to or disclosure of information.

[7] 12 C.F.R. § 5.34.

[8] *See, e.g.*, Conditional Approval Letter No. 219 (July, 15, 1996).

[9] *See* Interpretive Letter No. 692 (November 1, 1995); Interpretive Letter No. 694 (December 13, 1995).

(3) The bank's loss exposure must be limited, as a legal and accounting matter, and the bank must not have open-ended liability for the obligations of the enterprise.

(4) The investment must be convenient or useful to the bank in carrying out its business and not a mere passive investment unrelated to that bank's banking business.

We conclude, as discussed below, that the Banks' investment in the LLC will continue to satisfy these four criteria upon the LLC's expansion of activities.

1. The activities of the enterprise in which the investment is made must be limited to activities that are part of, or incidental to, the business of banking (or otherwise authorized for a national bank).

The National Bank Act, in relevant part, provides that national banks shall have the power:

> [t]o exercise . . . all such incidental powers as shall be necessary to carry on the business of banking; by discounting and negotiating promissory notes, drafts, bills of exchange, and other evidences of debt; by receiving deposits; by buying and selling exchange, coin, and bullion; by loaning money on personal security; and by obtaining, issuing, and circulating notes . . . .

The Supreme Court has held that this powers clause of 12 U.S.C. ∋ 24(Seventh) is a broad grant of power to engage in the business of banking, which is not limited to the five enumerated powers. Further, national banks are authorized to engage in an activity if it is incidental to the performance of the enumerated powers in section 24(Seventh) *or* if it is incidental to the performance of an activity that is part of the business of banking.[10] Since national banks must be able to make use of modern technology in performing their business, the OCC=s Interpretive Ruling 7.1019 permits national banks to Aperform, provide, or deliver through electronic means and facilities any activity, function, product, or service that [they are] otherwise authorized to perform, provide, or deliver."[11]

The expansion of the LLC's activities to include electronic bill payment services is legally permissible. The OCC previously has concluded that such services are part of the business of banking.[12] This conclusion is supported by judicial and agency precedent. The Supreme Court has found that 12 U.S.C. § 24(Seventh) permits a national bank to "do those acts and occupy those relations which are usual or necessary in making collections of commercial paper and

---

[10] *NationsBank of North Carolina, N.A. v. Variable Annuity Life Ins. Co.,* 513 U.S. 215 (1995).

[11] 12 C.F.R. § 7.1019.

[12] *See*, OCC Conditional Approval #304 (March 5, 1999) (Approval for Citibank N.A. to own indirectly a membership interest in three limited liability companies and thereby engage in electronic bill payment and presentment services over the Internet.)

other evidences of debt" for its customers.[13] Similarly, the courts have recognized that a "traditional banking function [is] collecting and remitting funds for other parties."[14] The OCC has also held that billing and collecting services are permissible for national banks, whether done conventionally or electronically.[15] In addition, the OCC has also determined that as part of an electronic collection or payment process, national banks may store and transmit information related to the underlying transactions such as electronic data interchange.[16] Finally, the transmission of the payment order or electronic funds transfer from the customer to the appropriate party (e.g., the biller's bank) and of remittance information from the customer to the biller is also legally permissible.[17]

Accordingly, the additional activities in which the LLC will engage are permissible for national banks. Thus, the first standard is satisfied.

> *2. The banks must be able to prevent the enterprise from engaging in activities that do not meet the foregoing standard, or be able to withdraw their investment*

This is an obvious corollary to the first standard. It is not sufficient that the entity's activities are permissible at the time a bank initially acquires its interest; they must also remain permissible for as long as the bank retains an ownership interest.

As previously determined by the OCC in the Spectrum Letter, the limited liability company agreement ("Agreement")[18] under which the LLC was formed contains provisions to ensure that the LLC would engage only in activities that are permitted for national banks and their subsidiaries. In particular, the Agreement provides that the LLC will not engage in an activity which is impermissible for a national bank or an operating subsidiary thereof, that any member may withdraw if the member reasonably determines that the LLC is engaged or proposes to engage in activities that are not legally permissible for a national bank or a subsidiary thereof, and that, in the event the OCC determines that an activity is impermissible, the LLC will cease

---

[13] *Miller v. King*, 223 U.S. 505, 510 (1912).

[14] *Corbett v. Devon*, 12 Ill. App.3d 559, 299 N.E.2d 521, 529 (App. Ct. 1st Cir. 1973).

[15] OCC interpretive Letter No. 712 (March 12, 1996) (permissibility of bank performing billing and collection services for medical service providers); Unpublished Letter from Peter Liebesman, Assistant Director, Legal Advisory Services Division (August 27, 1985) (permissibility of bank providing billing services); OCC Interpretive Letter No. 836 (March 12, 1996) (permissibility of bank's data processing and electronic data interchange system to assist in the billing and collection for medical services).

[16] OCC Interpretive Letter No. 836, *supra*; OCC interpretive Letter No. 732 (May 10, 1996); OCC Interpretive Letter No. 653 (December 22, 1995); OCC Interpretive Letter No. 419 (February, 16, 1988).

[17] *See*, OCC Conditional Approval No. 304, *supra*; OCC Interpretive Letter No. 653, *supra*.

[18] *See* Spectrum Letter.

to engage in that activity. The proposed expansion of activities by the LLC will not alter the terms of the Agreement.

Accordingly, the second standard is satisfied.

3. The banks' loss exposure must be limited, as a legal and accounting matter, and the bank must not have open-ended liability for the obligations of the enterprise

a. Loss exposure from a legal standpoint

A primary concern of the OCC is that national banks should not be subjected to undue risk. Where an investing bank will not control the operations of the entity in which the bank holds an interest, it is important that a bank's investment not expose it to unlimited liability.

With respect to the third standard, Banks' loss exposure will continue to be limited, and Banks do not, and will not, have open-ended liability for the obligations of the LLC. Banks' risk of loss will be limited by both the corporate veil of the operating subsidiary and by Delaware law. As a legal matter, investors in a Delaware limited liability company do not incur liability with respect to the liabilities or obligations of the limited liability company solely by reason of being a member or manager of the limited liability company. Del. Code Ann. Tit. 6, § 18-303 (Michie Cum. Supp. 1996). In addition, the Agreement provides that: (i) no member of the LLC shall have the authority to bind the LLC; and (ii) the members of the LLC are not liable for the debts, obligations or liabilities of the LLC. Thus, the Banks' loss exposure for the liabilities of the LLC will continue to be limited by statute and by the Agreement establishing the LLC.

b. Loss exposure from an accounting standpoint

In assessing a bank's loss exposure as an accounting matter, the OCC has previously noted that the appropriate accounting treatment for a bank's 20 to 50 percent ownership share or investment in a corporate entity is to report it as an unconsolidated entity under the equity method of accounting. Banks each will continue to account for their investment in the LLC under the equity method of accounting. Under the equity method of accounting, unless the investor has extended a loan to the entity, guaranteed any of its liabilities, or has other financial obligations, the investor's losses are generally limited to the amount of the investment shown on the investor's books.[19] Thus, Banks' losses from an accounting perspective would continue to be limited to the amount invested in the LLC and Banks will not have any open-ended liability for the obligations of the LLC.

Therefore, for both legal and accounting purposes, the Banks' potential loss exposure arising from their respective investments in the LLC should continue to be limited to the amount of

[19] *See generally,* Accounting Principles Board, Op. 18 ¶ 19 (1971).

those investments. Since that exposure will continue to be quantifiable and controllable, the third standard is satisfied.

> *4. The investment must be convenient or useful to the bank in carrying out its business and not a mere passive investment unrelated to that bank's banking business.*

A national bank's investment in an enterprise or entity must also satisfy the requirement that the investment have a beneficial connection to the bank's business, *i.e.*, be convenient or useful to the investing bank's business activities, and not constitute a mere passive investment unrelated to that bank's banking business. Twelve U.S.C. § 24(Seventh) gives national banks incidental powers that are "necessary" to carry on the business of banking. "Necessary" has been judicially construed to mean "convenient or useful."[20] Our precedents on bank non-controlling investments have indicated that the investment must be convenient or useful to the bank in conducting *that bank's* business. The investment must benefit or facilitate that business and cannot be a mere passive or speculative investment.[21]

In this instance, the proposed expansion of activities by the LLC is designed to complement the LLC's current bill presentment business by adding bill payment and other related services. Thus, the proposed expansion of the LLC's services, which will be available to the Banks' customers, further demonstrates that Banks' investment in the LLC is not a mere passive investment unrelated to Banks' banking business.

Accordingly, the fourth standard is satisfied.

C. Conclusion

Based upon a thorough review of the information you provided, including the representations and commitments made both in your letters and in the Board filing incorporated therein by reference, and for the reasons discussed above, we conclude that the Banks may continue to hold their noncontrolling equity investments in the LLC upon the LLC's expansion of its current activities, subject to the following conditions:

> (1) The LLC will engage only in activities that are permissible for a national bank;
>
> (2) In the event that the LLC engages in an activity that is inconsistent with condition number one, Banks will withdraw from the LLC;
>
> (3) the Banks account for their respective investments in the LLC under the equity method of accounting; and

---

[20] *See Arnold Tours, Inc. v. Camp*, 472 F.2d 427, 432 (1st Cir. 1972).

[21] *See, e.g.*, Interpretive Letter No. 543 (February 13, 1991); Interpretive Letter No. 427 (May 9, 1988); Interpretive Letter No. 421 (March 14, 1988).

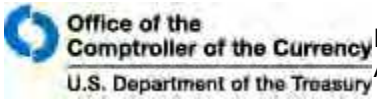
(4) The LLC will be subject to OCC supervision and examination, subject to the limitations and requirements of 12 U.S.C. § 1831v.

The conditions of this approval are Aconditions imposed in writing by the agency in connection with the granting of any application or other request≅ within the meaning of 12 U.S.C. ∋ 1818. As such, the conditions are enforceable under 12 U.S.C. ∋ 1818. If you have any questions, please contact Beverly Evans, Senior Licensing Analyst, Bank Organization and Structure, at 202-874-5060, or John Soboeiro, Senior Attorney, in the Bank Activities and Structure Division, at 202-874-5300.

Sincerely,

-signed-

Julie L. Williams
First Senior Deputy Comptroller and Chief Counsel



Ensuring a Safe and Sound Federal Banking System for All Americans

EXHIBIT
K-24

Public Service Announcements

Events

Media Press Room

Search News and Issuances Archive

-
- Publications

Alphabetical Listing

Publications by Topic

Bank Management

Bank Operations

Capital Markets

Capital Policy

Community Affairs

Compliance/BSA

Consumer Protection

Credit

Dispute Resolution

Economics

Examinations

International Banking

Laws and Regulations

Publications by Type

Annual Reports

Comptroller's Handbook

Licensing Manual

Economics Working Papers

Other Publications/Reports

Survey of Credit Underwriting Practices Report

-
- Tools and Forms
-
- Topics

Bank Management

Bank Operations

Capital Markets

- 2007
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- 1999
- 1998
- 1997
- 1996
- 1995

- ▶Bulletins
  - 2015
  - 2014
  - 2013
  - 2012
  - 2011
  - 2010
  - 2009
  - 2008
  - 2007
  - 2006
  - 2005
  - 2004
  - 2003
  - 2002
  - 2001
  - 2000
  - 1999
  - 1998
  - 1997
  - 1996
  - 1995
  - 1994
  - Pre-1994
  - Rescinded
- ▶Alerts
  - 2015
  - 2014
  - 2013
  - 2012
  - 2011
  - 2010
  - 2009
  - 2008
  - 2007
  - 2006
  - 2005
  - 2004
  - 2003

- 2002
- 2001
- 2000
- 1999
- 1998
- 1997
- 1996
- 1995

- ►Consumer Advisories
  - 2011
  - 2010
  - 2009
  - 2008
  - 2007
  - 2006
  - 2005
- ►Congressional Testimony
  - 2015
  - 2014
  - 2013
  - 2012
  - 2011
  - 2010
  - 2009
  - 2008
  - 2007
  - 2006
  - 2005
  - 2004
  - 2003
  - 2002
  - 2001
  - 2000
  - 1999
  - 1998
  - 1997
  - 1996
  - 1995
- ►Speeches
  - 2015
  - 2014
  - 2013
  - 2012
  - 2011
  - 2010
  - 2009
  - 2008
  - 2007
  - 2006
  - 2005
  - 2004

- 2003
- 2002
- 2001
- 2000
- 1999

- ►Advisory Letters
  - 2004
  - 2003
  - 2002
  - 2001
  - 2000
  - 1999
  - 1998
  - 1997
  - 1996
  - 1995
  - Pre-1995
  - Rescinded
- Public Service Announcements
- Events
- Media Press Room
- Search News and Issuances Archive

- ►Publications
  - Alphabetical Listing
  - ►Publications by Topic
    - Bank Management
    - Bank Operations
    - Capital Markets
    - Capital Policy
    - Community Affairs
    - Compliance/BSA
    - Consumer Protection
    - Credit
    - Dispute Resolution
    - Economics
    - Examinations
    - International Banking
    - Laws and Regulations
  - ►Publications by Type
    - Annual Reports
    - Comptroller's Handbook
    - Licensing Manual
    - Economics Working Papers
    - Other Publications/Reports
    - Survey of Credit Underwriting Practices Report
- Tools and Forms
- ►Topics
  - ►Bank Management
    - Community Banks

- Minority Depository Institutions
- Mutual Savings Associations

- ►Bank Operations
  - Accounting
  - Bank Information Technology (BIT)
  - Financial Crime
- ►Capital Markets
  - Asset Management
  - Balance Sheet Management
  - Financial Markets
- Capital Policy
- ►Community Affairs
  - Community Outreach
  - Publications
  - Resource Directories
- ►Compliance/BSA
  - Bank Secrecy Act
  - Community Reinvestment Act (CRA)
  - Consumer Compliance
- ►Consumer Protection
  - Credit Cards, Debit Cards, And Gift Cards
  - Credit Reporting
  - Depository Services
  - Fair Lending
  - Flood Disaster Protection
  - Foreclosure Prevention
  - Fraud Resources
  - Mortgages
  - Payday Lending
  - Privacy
  - Servicemembers' Civil Relief Act
  - Truth In Lending
- ►Credit
  - Commercial Credit
  - Retail Credit
- ►Dispute Resolution
  - Consumer Complaints
  - Bank Appeals
- ►Economics
  - Economics Staff
  - Economics Working Papers
- ►Examinations
  - Assessments & Fees
  - Examinations Overview
- ►International Banking
  - Outreach
  - International Banking Supervision

- International Groups
- ►Laws & Regulations
  - OCC Regulations
  - Enforcement Actions
  - Interpretations and Precedents
  - Legislation of Interest
  - Litigation
- ►Licensing
  - Corporate Activities
  - Interpretations & Actions
  - National Banks & Federal Savings Associations Lists

OCC BULLETIN 2002-23

Subject: Electronic Banking
Date: May 28, 2002

To: Chief Executive Officers of All National Banks, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Description: Final Rule

The OCC has issued a final rule governing national banks' ability to conduct business using electronic technologies. The regulation was published in the *Federal Register* on May 17 and, except for one provision, is effective on June 17. The exception is a provision containing certain disclosure requirements for national banks that have co- branded Web sites or other shared electronic space. That provision takes effect on July 1.

Among the most significant changes, the final rule:

- Codifies recent OCC interpretive letters approving the use of finder authority by national banks to engage in activities made possible by technological developments.
- Sets forth the factors the OCC considers in determining whether an electronic activity is part of, or incidental to, the business of banking.
- Clarifies that state law is not applicable to a national bank's conduct of an authorized activity through electronic means or facilities if the state law, as applied to the activity, would be preempted pursuant to traditional principles of federal preemption, and describes the preemption standards established by Supreme Court precedents.
- Codifies the excess capacity doctrine, clarifying that a national bank may market and sell electronic capacities "legitimately acquired or developed by the bank for its banking business," as well as the "by- product doctrine," a well-established doctrine closely related to excess capacity that applies to production, such as software.
- Codifies OCC interpretations that permit national banks, as part of a digital signature transaction, to act as a certification authority that issues certificates verifying the identity of the certificate holder and any other attribute for which verification is part of, or incidental to, the business of banking, e.g., financial capacity.
- Codifies OCC interpretations that permit a national bank to collect, process, transcribe, analyze, and store banking, financial, and economic data for itself and its customers as part of the business of banking. The final rule also permits a national bank to process additional types of data to the extent convenient or useful to provide or market the financial data processing services.
- Clarifies that a national bank will not be considered "located" in a state simply because it maintains technology, such as a server or an automated loan center, in that state or because customers in that state electronically access a bank's products and services.
- Requires that a national bank that shares electronic space (such as Web pages or Web sites) with another business take reasonable steps to clearly, conspicuously, and understandably distinguish between products and services offered by the bank and those offered by the other business.

The rule creates a new subpart E to part 7 of the OCC's regulations to house these and other OCC provisions related to the conduct of national bank activities through electronic means.

This rule is the result of a review by the OCC of its regulations with the goal of revising them in ways that would facilitate bank use of technology, consistent with safety and soundness. This review began with the publishing of an advance notice of proposed rulemaking (ANPR) in the *Federal Register* on February 2, 2000 (65 Fed. Reg. 4895). The proposed rule, which reflected the comments we received on this ANPR, was published in the *Federal Register* on July 2, 2001 (66 Fed. Reg. 34855).

For further information, contact Bank Information Technology Division at (202) 649-6340.

Julie L. Williams
First Senior Deputy Comptroller and Chief Counsel

Related Links

- 67 FR 34992

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 7

[Docket No. 02–07]

RIN 1557–AB76

Electronic Activities

AGENCY: Office of the Comptroller of the Currency, Treasury.

ACTION: Final rule.

SUMMARY: The Office of the Comptroller of the Currency (OCC) is amending its regulations in order to facilitate national banks' ability to conduct business using electronic technologies, consistent with safety and soundness. This final rule groups together new and revised regulations addressing: national banks' exercise of their Federally authorized powers through electronic means; the location, for purposes of the Federal banking laws, of a national bank that engages in activities through electronic means; and the disclosures required when a national bank provides its customers with access to other service providers through hyperlinks in the bank's website or other shared electronic ''space.''

EFFECTIVE DATE: Section 7.5010 shall take effect on July 1, 2002. All other sections of this final rule shall take effect on June 17, 2002.

FOR FURTHER INFORMATION CONTACT: Heidi M. Thomas, Special Counsel, Legislative and Regulatory Activities, (202) 874–5090; James Gillespie, Assistant Chief Counsel, (202) 874–5200; or Clifford Wilke, Director, Bank Technology, (202) 874–5920.

SUPPLEMENTARY INFORMATION: On July 2, 2001, the OCC published a notice of proposed rulemaking (NPRM) in the **Federal Register** requesting comments on a proposal to update our regulations to reflect national banks' use of new technologies and to provide simpler, clearer guidance to national banks engaging in electronic activities.[1] The proposal codified several positions that the OCC has taken previously in published interpretive letters to national banks. The proposal also created a new subpart E to part 7 of the OCC's regulations to house these and other OCC provisions related to the conduct of national bank activities through electronic means.[2]

Our proposal was the result of a focused review of our regulations with the goal of revising them in ways that would facilitate national banks' use of technology, consistent with safety and soundness. We initiated this review by publishing an advance notice of proposed rulemaking (ANPR).[3] We developed the proposed rule, in large part, on the comments received on this ANPR.

Description of Proposal, Comments Received, and Final Rule

The OCC received 22 comment letters on the proposal.[4] These comments include 10 from national banks, bank subsidiaries, and bank holding companies; 5 from financial services trade associations; 4 from credit card banks or lenders; 1 from a State regulatory group; and 2 from other interested parties. The majority of commenters supported adoption of an electronic banking regulation in the form we proposed.

Some commenters, however, suggested modifications or articulated concerns with certain aspects of this proposal. In light of these comments, we have modified certain provisions of the proposed rule. The most significant comments, and our responses, are discussed in the following section-by-section analysis. As in the preamble to the proposal, this section-by-section description is divided into three categories: national bank powers; ''location'' with respect to the conduct of electronic activities; and, safety and soundness requirements for shared electronic ''space.''

A. National Bank Powers

1. National Bank Finder Authority (Revised § 7.1002)

As we described in the proposal, the OCC has long permitted a national bank to act as a finder to bring together buyers and sellers of financial and non-financial products and services. Under our current rules, a national bank acting as a finder may identify potential parties, make inquiries as to interest, introduce or arrange meetings of interested parties, and otherwise bring parties together for a transaction that the parties themselves negotiate and consummate.[5] Recently, national banks have used the finder authority to engage in new activities made possible by technological developments, especially the Internet.[6]

[1] 66 FR 34855 (July 2, 2001).

[2] The OCC notes that it has established a website that contains information relating to electronic banking activities. *See http://www.occ.treas.gov/netbank/netbank.htm*. This site includes a listing of opinions, approval letters, supervisory guidance, and other issuances on this subject and provides links to many of the documents listed in this preamble.

[3] 65 FR 4895 (Feb. 2, 2000).

[4] The OCC received four other letters commenting on a study of banking regulations regarding the online delivery of financial services conducted by the Federal banking agencies pursuant to section 729 of the Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338, 1476 (Nov. 12, 1999) (''GLBA''), *codified at* 12 U.S.C. 4801.

[5] *See* 12 CFR 7.1002.

[6] *See* OCC Conditional Approval No. 369 (Feb. 25, 2000) (national bank may host a virtual mall consisting of a web page with links to third-party merchants arranged according to product or service offered; OCC Interpretive Letter No. 875, *reprinted in* [Current Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81–369 (Oct. 31, 1999) (the components of Internet services package that involve hosting of commercial web sites, registering merchants with search engines and obtaining URLs, and electronic storage and retrieval of the data set for a merchant's on-line catalog are permissible finders activities authorized for national banks pursuant to 12 U.S.C. 24(Seventh)); OCC Conditional Approval No. 221 (Dec. 4, 1996) (national banks, in the exercise of their finder authority, may establish hyperlinks between their home pages and the Internet pages of third-party providers so that bank customers will be able to access those non-bank web sites from the bank site); Letter from Julie L. Williams, Chief Counsel (Oct. 2, 1996) (unpublished) (national bank as finder may use electronic means to facilitate contacts between third-party providers and potential buyers); OCC Interpretive Letter No. 611, *reprinted* in [1992–1993 Transfer Binder] Fed.

EXHIBIT
K-25

Section 7.1002 of the OCC's rules addresses national banks' finder authority. The proposal sought comment on several changes to that provision. First, the proposal stated that it is part of the business of banking for a national bank to engage in finder activities, codifying the position the OCC has taken in various interpretive letters.[7]

Second, the proposal added a number of specific examples illustrating the range of finder activities the OCC has authorized to date. The preamble to the proposal made clear that this list was illustrative and not exclusive, and that the OCC may find new activities to be authorized under the finder authority that are not specifically enumerated in the regulation.

Finally, the proposed rule modified the statement in the current rule that the authority to act as a finder does not enable a national bank to engage in activities that would characterize the bank as a broker under Federal law that are not otherwise permissible for national banks.[8] We proposed this modification because the concept of what constitutes acting as a broker is changing in response to technology and is expanding for purposes of some regulatory requirements that are unrelated to the authority of national banks to conduct the activity.[9] As we said in the proposal, however, this modification does not affect whether activities regulated as brokerage under State law are permissible for a national bank.

We received a number of comments on proposed § 7.1002. Some of these comments urged the OCC to include additional activities in the illustrative list of those permissible for a national bank acting as finder. For example, one commenter requested that the OCC authorize national banks, acting as finders, to participate in negotiations, negotiate on behalf of parties to a transaction, and bind parties to a transaction so long as the bank itself is not a party and obligated as a principal. Another commenter requested that the OCC endorse a broad role of banks as electronic agents.

After carefully reviewing these comments, we have declined to make changes to the extent suggested.[10] Rather, we will consider these, and similar expanded types of finder activities, on a case-by-case basis for the time being.

We have, however, modified the proposal to clarify certain other aspects of the finder authority that do not cause a national bank to be a participant in the transaction. Thus, the final rule provides that a national bank may act as an intermediary between interested parties and establish rules of general applicability governing the use and operation of the finder service.

In response to a commenter's suggestion, we have also changed the reference ''buyers and sellers'' in § 7.1002 to ''interested parties to a transaction'' so that the rule recognizes that national banks can bring together different types of parties to a transaction in addition to buyers and sellers. This commenter noted in particular that in the Internet environment, there may be many parties to a transaction beyond the buyer and seller, such as service providers, consultants, software developers, and regulatory authorities. We agree with this observation. We also note that the definition of buyers and sellers includes analogous parties, such as lessors and lessees. In addition, as the scope of permissible finder activities is not dependent on the nature of goods or services sold, national banks can act as finder with respect to non-financial products and services.[11] We also have removed the word ''service'' in § 7.1002 to clarify that national banks acting as a finder may make communications concerning a third party's provision of both products and services.

The preamble to the proposed rule stated that the examples of permissible national bank finder activities were illustrative and not exclusive, and that the OCC may find new activities to be authorized under the finder authority that are not included in the examples. A number of commenters requested that we amend the regulatory text itself to state that these examples are not exhaustive. We agree that making this statement in the text of the regulation itself will remove any ambiguity on this point. Therefore, the final rule includes language indicating that permissible finder activities are not limited to those listed as examples in the regulation.

2. Electronic Banking B—Scope (new Subpart E and § 7.5000)

The proposal created a new Subpart E of part 7, so that regulations pertaining to electronic activities would appear in one place. Proposed § 7.5000 described the purpose of Subpart E, which addresses national banks' use of electronic technology to deliver products and services, consistent with safety and soundness. To more accurately reflect the content of this section, we have changed the title of § 7.5000 in the final rule from ''Scope'' to ''Purpose of subpart E.''

The majority of commenters supported the creation of a new, separate subpart for electronic banking-related provisions. Although one commenter suggested a regrouping of the provisions in new subpart E, we believe that the organization of the subpart as proposed presents the subject

Banking L. Rep. (CCH) ¶ 83,449 (Nov. 23, 1992) (national bank linking non-bank service providers to its communications platform of smart phone banking services is within its authority as a finder ''in bringing together a buyer and seller;'' national banks may act as finders by providing to their customers links to non-banking, third-party vendors' Internet web sites); OCC Interpretive Letter No. 516, *reprinted* in [1990–1991 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 83,220 (July 12, 1990) (national banks as finder may provide electronic communications channels for persons participating in securities transactions).

[7] *See, e.g.*, OCC Interpretive Letter No. 824, *reprinted in* [1997–1998 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81,273 (Feb. 27, 1998) (determining, in the context of insurance activities, that the ''finder function is an activity authorized for national banks under 12 U.S.C. 24(Seventh) as part of the business of banking.''). The OCC makes this determination pursuant to its authority under section 24(Seventh) to authorize activities as part of the business of banking. *NationsBank of North Carolina* v. *Variable Annuity Life Insurance Co.*, 513 U.S. 251, 258 n.2 (1995) (VALIC) (''We expressly hold that the ''business of banking'' is not limited to the enumerated powers in [section] 24 Seventh and that the Comptroller therefore has discretion to authorize activities beyond those specifically enumerated.''). In VALIC, the Court noted that the Comptroller's exercise of discretion is subject to a reasonableness standard. *Id.* It is clear that our determination that finder activities are part of the business of banking satisfies this standard. *See Norwest Bank Minnesota, N.A.* v. *Sween Corp.*, 118 F.3d 1255, 1260 (8th Cir. 1997) (determining that finder activities were authorized for a national bank because ''allowing banks to use their expertise as an intermediary effectuating transactions between parties facilitates the flow of money and credit through the economy.''). The *Sween* court did not distinguish between activities that are ''part of'' the business of banking and those that are ''incidental to'' that business, relying, instead, on the pre-VALIC formulation of the analysis as whether an activity is ''closely related to an express power and is useful in carrying out the business of banking.'' *Id.* at 1260 (quoting *First Nat. Bank of Eastern Arkansas* v. *Taylor*, 907 F.2d 775, 778 (8th Cir. 1990)). The court's conclusions are nonetheless clear that finder activities are authorized pursuant to 12 U.S.C. 24(Seventh) and that the Comptroller's determination to that effect, embodied in the OCC's regulations, was a reasonable construction of the statute.

[8] The prior rule contained the express statement that acting as a finder does not include activities that would characterize the bank as a broker under applicable Federal law.

[9] *See, e.g.*, ''SEC Redefines What Triggers B/D Registration,'' VII *Compliance Rep.* 1 (Apr. 10, 2000); and ''On-line Brokerage: Keeping Apace of Cyberspace,'' Report of Laura S. Unger, Commissioner, U.S. Securities and Exchange Commission 98–106 (Nov. 1999).

[10] We note, however, a bank may accept an offer without first communicating the offer to the actual party to the transaction if that party has given direction to the bank to accept offers that meet pre-determined criteria. In that case, the bank is communicating offers and acceptances because it has been directed to make an acceptance by its client.

[11] *See* OCC Corporate Decision No. 97–60 (July 1, 1997).

matter clearly and concisely. Therefore, we have not altered the arrangement of new Subpart E in the final rule.

3. Electronic Banking Activities That Are Part of, or Incidental to, the Business of Banking (§ 7.5001)

In response to new technologies and evolving financial markets, national banks are continually developing new electronically-based activities and products. Proposed § 7.5001 was designed to assist banks that are contemplating these new electronic activities and products by identifying the factors the OCC uses to determine whether such an activity or product is part of, or incidental to, the business of banking, pursuant to 12 U.S.C. 24(Seventh).

In general, commenters supported the approach taken by this section. However, a few commenters noted specific issues with the section as drafted. These issues are discussed below.

Purpose. Proposed § 7.5001(a) provided the purpose of the new section and described the general parameters of national banks' ability to engage in electronic activities.[12] It expressly set out the OCC's authority to impose conditions on the exercise of newly authorized activities if necessary to ensure that the activities are conducted safely and soundly and in accordance with applicable law and supervisory policies. We received no comments on this portion of proposed § 7.5001(a), and therefore have adopted it, with changes to improve clarity.

Proposed § 7.5001(a) also stated that State law applies to a national bank's conduct of electronic activities to the extent such law would apply if the activity were conducted by the bank through traditional means. A few commenters suggested modifications to this statement. However, because § 7.5002 of the proposed rule contains the same applicability of State law provision, we have deleted this provision in § 7.5001 as redundant and unnecessary. These comments, therefore, are described in the discussion of § 7.5002, below.

Activities that are part of the business of banking. Proposed § 7.5001(b) provided that an electronic activity is authorized for national banks as part of the business of banking if the activity is permitted under 12 U.S.C. 24(Seventh) or other statutory authority applicable to national banks, or otherwise constitutes part of the business of banking. The proposal set forth four factors the OCC considers in determining whether an electronic activity is part of the business of banking.[13]

The first factor is whether the electronic activity is functionally equivalent to, or a logical outgrowth of, a recognized banking activity. As indicated in the preamble to the proposed rule, this factor is based on judicial precedents approving activities that traditionally have been performed by banks, that are functionally similar to recognized banking activities, or that represent advances in recognized banking practices.[14] We received no comments objecting to, or requesting modifications of, this factor. Therefore, we are adopting this factor as proposed.

The second factor in proposed § 7.5001(b) is whether the proposed activity strengthens the bank by benefiting its customers or its business. Courts have long recognized that national banks' ability to serve the needs of their customers by offering appropriate products and services is crucial to their capability to compete successfully. Courts have also approved many activities on the basis that they benefit a bank's customers or the bank's business itself.[15] Examples of the types of activities the OCC would look to include those where the activity increases service, convenience, or options for bank customers or lowers the cost to banks of providing a product or service. We also received no comments objecting to, or requesting modifications of, this factor. The final rule therefore adopts this factor as proposed.

The third factor in proposed § 7.5001(b) is whether the activity presents the types of risk that banks are experienced in managing. One commenter requested that the OCC change this factor instead to whether the activity ''involves risk that can be sufficiently assessed and managed by the bank.'' This suggested modification appears substantially identical to the proposal in practical effect. Since we have utilized the proposed factor—whether the activity presents the types of risks that banks are experienced in managing—in interpretive letters issued prior to this proposal,[16] we have decided to adopt the third factor as proposed.

Finally, the fourth proposed factor recognized the relevance of State law in the analysis the OCC conducts when it receives requests regarding the permissibility of new electronic activities for national banks. Since the statutory reference to the ''business of banking'' does not imply that there are two distinct businesses of banking—one for Federally-chartered and another for State-chartered banks—activities that are recognized as permissible for State banks are at least a relevant factor in determining whether an electronic activity is part of the business of banking.[17] We received no comments or requests for modification on this factor. The final rule clarifies that the activities encompassed by this factor include activities authorized for a State-chartered bank expressly by State law or otherwise.

The preamble to the proposed rule stated that a proposed activity does not necessarily have to satisfy all of these four factors in order to be permissible. One or more of these factors may be sufficient, depending on the specific facts and circumstances presented. One commenter requested that, in addition to the preamble, the regulatory text include the statement that an activity does not need to meet all of the listed factors to be permissible. In response,

[12] Paragraph (a) of § 7.5001 of the proposed rule has been recodified as paragraphs (a) and (b) of § 7.5001 in the final rule.

[13] The final rule recodifies these factors as § 7.5001(c)(1).

[14] *See, e.g., M & M Leasing Corp.* v. *Seattle First Nat'l Bank*, 563 F.2d 1377 (9th Cir. 1977), *cert. denied*, 436 U.S. 956 (1978) (national bank leasing of personal property permissible because it was functionally interchangeable with loaning money on personal security and therefore incidental to the express power of loaning money on personal security); and *VALIC*, 513 U.S. at 259–60 (national bank annuity sales are permissible because they are functionally similar to other financial investment products banks have long been authorized to sell).

[15] *See Merchants' Bank* v. *State Bank*, 77 U.S. (10 Wall.) 604, 648 (1870) (''The practice of certifying checks has grown out of the business needs of the country.''). *See also Clement National Bank* v. *Vermont*, 231 U.S. 120, 140 (1913) (''the bank should be free to make * * * reasonable [depositors'] agreements, and thus promote the convenience of its business. * * *'').

[16] *See Merchants' Bank*, 77 U.S. at 648 (''A bank incurs no greater risk in certifying a check than in giving a certificate of deposit.''); *M & M Leasing*, 563 F.2d at 1383 (leasing personal property functionally equivalent to secured lending because the risks to the bank of such leasing were essentially the same as if the bank had made secured loans to buyers of the same property). *See also* Decision of the Comptroller of the Currency on the Operating Subsidiary Application by Zions First National Bank, Salt Lake City, Utah, OCC Conditional Approval No. 267, *reprinted in* [1997–1998 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81,256 (Jan. 12, 1998) at 13 (acting as a certification authority involves core competencies of national banks and thus entails risks similar to those that banks are already expert in handling).

[17] The U.S. Supreme Court has relied upon the permissibility of an activity for State banks as a factor in the analysis of permissible national bank powers. *See Colorado Nat'l Bank* v. *Bedford*, 310 U.S. 41 (1940), in which the Court, concluding that national banks had the authority to conduct a safe-deposit business, stated that ''State banks, quite usually, are given the power to conduct a safe-deposit business. We agree with the appellant bank that such a generally adopted method of safeguarding valuables must be considered a banking function authorized by Congress.'' *Id.* at 49–50.

we have added a statement explaining that the weight given a particular factor depends on the facts and circumstances.

Finally, we have modified the first sentence of proposed § 7.5001(b) by deleting the phrase ''or is otherwise part of the business of banking.'' That phrase is unnecessary in light of the statement elsewhere in this subsection that an activity is authorized for national banks as part of the business of banking if the activity is described in section 24 (Seventh).

Electronic activities that are incidental to the business of banking. Consistent with judicial precedent,[18] proposed § 7.5001(c) provided that an activity is incidental to the business of banking if it is convenient or useful to an activity that is specifically authorized for national banks or to an activity that is otherwise part of the business of banking. Relying on these same precedents, proposed § 7.5001(c) distilled and set forth in two factors the elements the OCC considers in determining whether an activity is convenient or useful to the business of banking.[19]

The first factor is whether the activity facilitates the production or delivery of a bank's products or services, enhances the bank's ability to sell or market its products or services, or improves the effectiveness or efficiency of the bank's operations in light of risks presented, innovations, strategies, techniques, and new technologies for producing financial products and services. In applying this factor, the OCC has determined that the provision of certain electronic products and services is permissible, as incidental to the business of banking, when needed to package successfully or promote other banking services.[20] We also have recognized a category of incidental activities based on the operation of the bank itself as a business concern. Banking activities that fall in this category may include hiring employees, issuing stock to raise capital, owning or renting equipment, borrowing money for operations, purchasing the assets and assuming the liabilities of other financial institutions, and operating through optimal corporate structures, such as subsidiary corporations or joint ventures. Various Federal statutes have implicitly recognized national banks' authority to perform the activities necessary to conduct their business.[21] In each case, the statutes presume the existence of corporate power to conduct the bank's business under 12 U.S.C. 24(Seventh).

We noted in the preamble to the proposed rule that the authority of banks to deliver and sell products and services or improve the effectiveness of their operations must be viewed in light of innovations, strategies, techniques and new technologies for marketing financial products and services. These grants of power must be given a broad and flexible interpretation to allow national banks to utilize modern methods and meet modern needs.[22] The proposal noted that market and technological changes that will affect the banking industry will shape the OCC's future determinations of whether an activity is incidental to the business of banking.

The second factor listed in proposed § 7.5001(c) is whether the activity enables the bank to profitably use capacity acquired for its banking operations or otherwise avoid economic waste or loss. For example, it is well settled that a nonbanking activity can be incidental when it enables a bank to realize gain or avoid loss from activities that are part of, or necessary to, its banking business. Federal statutes and case law also recognize national banks' need to optimize the value of bank property by authorizing banks to sell excess space or capacity in that property.[23] Section 7.5004, which pertains to excess capacity, is a specific application of this general principle in the electronic context.

We received no specific comments on these factors and have therefore retained them both in the final rule. We have, however, modified the second factor by removing the word ''profitably'' to conform this factor to the excess capacity doctrine set forth in § 7.5004.

As with determinations regarding whether an activity is part of the business of banking, specific facts may implicate one or both of these factors, and the activity need not satisfy each factor to be permissible as incidental to that business. At the request of a commenter, the OCC has added a clarification of this point, in § 7.5001(d)(2) of the final rule.

Two commenters discussed the effect of this new § 7.5001 on the application process the OCC uses to determine whether national banks and their operating subsidiaries may engage in new activities, set forth in 12 CFR part 5. One commenter requested more specificity on the use of the factors relevant to determining whether an activity is incidental to banking and asked that the OCC clarify whether it expects banks to include these factors in applications to offer new electronic services. This commenter also asked whether the OCC intends to alter or streamline this application process in light of the factors listed in § 7.5001.

We do not believe that substantive changes to the application process in part 5 are necessary at this time based on this codification of the factors the OCC examines when determining whether an activity is authorized pursuant to 12 U.S.C. 24(Seventh). These factors are derived from OCC opinion letters, which explain them in sufficient detail that additional guidance is not needed in the rule. A bank that wishes us to consider whether a proposed activity is permissible pursuant to 12 U.S.C. 24(Seventh) should describe in its filing how its proposed activity meets one or more of these factors. If it subsequently appears that technical changes to the application

[18] *See Arnold Tours, Inc.* v. *Camp*, 472 F.2d 427, 432 (1st Cir. 1972), which held that a national bank's activity is authorized as an incidental power if ''it is convenient or useful in connection with the performance of one of the bank's established activities pursuant to [the five] express powers'' enumerated in 12 U.S.C. 24(Seventh); *Franklin Nat. Bank* v. *New York*, 347 U.S. 373 (1954); *Wyman* v. *Wallace*, 201 U.S. 230 (1906); and *First Nat'l Bank of Charlotte* v. *National Exch. Bank of Baltimore*, 92 U.S. 122 (1875).

[19] The final rule recodifies these factors as § 7.5001(d)(1).

[20] *See* OCC Interpretive Letter No. 754, *reprinted in* [1996–97 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81–118 (Nov. 6, 1996) (national bank operating subsidiary may sell general purpose computer hardware to other financial institutions as part of larger product or service when necessary, convenient, or useful to bank permissible activities).

[21] For example, Federal laws refer to limits on persons who can serve as bank employees, to the permissible disposition of bank stock, and to the existence of bank subsidiaries. *See, e.g.*, 12 U.S.C. 78 (defining persons ineligible to be bank employees); 12 U.S.C. 83 (limiting national bank's purchase of its own stock); 12 U.S.C. 24(Seventh) (limiting presupposed authority of national bank to own a subsidiary engaged in the safe deposit business; 12 U.S.C. 371d (1994) (defining ''affiliates'' to include subsidiaries owned by national banks); GLBA section 121 (defining ''financial subsidiary'' as a subsidiary ''other than'' a subsidiary that conducts bank-permissible activities under the same terms and conditions that apply to the parent bank or a subsidiary expressly authorized by Federal statute).

[22] In *VALIC*, the Supreme Court recognized that the concepts of the ''business of banking'' and of activities ''incidental'' to that business must be sufficiently flexible to accommodate the constant evolution of banking services. *See VALIC*, 513 U.S. at 259–260. *See also M & M Leasing*, 563 F.2d at 1382 (noting that ''commentators uniformly have recognized that the National Bank Act did not freeze the practices of national banks in their nineteenth century forms. * * * [W]e believe the powers of national banks must be construed so as to permit the use of new ways of conducting the very old business of banking.'').

[23] *See* 12 U.S.C. 24 (Seventh) and 29; *Perth Amboy National Bank* v. *Brodsky*, 207 F. Supp. 785, 788 (S.D.N.Y. 1962) (''It is clear beyond cavil that the statute [12 U.S.C. 29] permits a national bank to lease or construct a building, in good faith, for banking purposes, even though it intends to occupy only a part thereof and to rent out a large part of the building to others.'').

or notice process are desirable, we will initiate a separate rulemaking proposing those changes.

Another commenter suggested that the OCC establish an ''optional, expedited notice procedure for new activities as a way of enabling banks to bring products to market quickly within the umbrella of OCC deference.'' We believe, however, that the OCC's current processes are sufficiently flexible to allow national banks to offer new electronic products and services expeditiously, consistent with safety and soundness considerations. In general, national banks are not required to notify or obtain OCC approval to engage in permissible activities within the bank. In addition, national banks may already offer many permissible electronic products or services through an operating or financial subsidiary without filing a notice or application with the OCC. (For new activities to be performed in an operating or financial subsidiary, the after-the-fact notice or application provisions of 12 CFR part 5 apply.) As indicated in the discussion above, the factors set forth in § 7.5001 will assist banks in their determination as to whether a new activity is permissible. A bank that is uncertain about the permissibility of a new activity may request an interpretive opinion from the OCC.

4. Furnishing of Products or Services by Electronic Means and Facilities (§ 7.5002)

The OCC's rules currently provide that a national bank may perform, provide, or deliver through electronic means and facilities any function, product, or service that it is otherwise authorized to perform, provide or deliver.[24] This so-called ''transparency doctrine'' is a key provision for national banks engaging in electronic activities because it calls for the OCC to look through the means by which the product is delivered and focus instead on the authority of the national bank to offer the underlying product or service.

We have relied on this transparency doctrine to approve a number of technology-based activities, such as web site hosting and the operation of a ''virtual mall,'' that are otherwise permissible under a national bank's finder authority. Similarly, we have approved electronic bill presentment activities because billing and collecting services are permissible for national banks.[25]

The proposal moved the transparency rule to § 7.5002 of new subpart E and expanded it to include examples of activities the OCC has found to be permissible. These changes were proposed in order to provide clearer guidance to national banks that wish to engage in new electronic activities.

One commenter requested that we clarify that these examples in § 7.5001 are not exclusive, and that we would consider the authorization of new activities under the transparency doctrine that may not be illustrated through the examples provided. The commenter's suggestion is consistent with the purpose of the provision, and the final rule clarifies that these examples are illustrative, not exclusive.

Other commenters requested that we expand the list of examples in the text of § 7.5002 to include other specific activities. One suggested that this list include the provision of communications services relating to all aspects of transactions between buyers and sellers. This facilitation of communication between interested parties is an inherent part of a bank's finder activities, and therefore may be conducted electronically.[26] We have therefore amended the regulatory text to include this activity in the list of examples of permissible electronic activities based on the transparency doctrine.

Other commenters suggested adding a number of specific activities that the OCC has not yet approved as permissible for national banks. We have not adopted these suggestions. Our experience is that decisions about the permissibility of new electronic activities are best made in the context of specific tests and circumstances that enable us to consider the practical and supervisory effects of, as well as the legal basis for, the determination. We will accordingly continue our practice of case-by-case review, followed by codification of key precedents, as appropriate, from time to time. As noted previously, this codification does not serve to limit the activities that may be found to be permissible, and we will continue to review new activities on a case-by-case basis.

Consistent with the principle that it is the substance of an activity—and not its electronic form—that is key to the determination of whether it is permissible, the final rule provides that when a national bank engages in an electronic activity based on the transparency doctrine, the electronic activity will not be exempt from the regulatory requirements and supervisory guidance, including those prescribed by OCC regulations or contained in other OCC issuances, that would apply if the activity were conducted by non-electronic means or facilities. This new provision clarifies that national bank activities will continue to be governed by OCC regulatory requirements and supervisory guidance regardless of whether that activity is conducted electronically or by traditional means.

A few commenters suggested modifications in the provision addressing the applicability of State law that appeared at proposed § 7.5002(b), as well as at proposed § 7.5001(a), both provisions being very similar in substance and in wording. One commenter asked that the OCC expressly preempt State laws that purport to regulate activities conducted by electronic means. Another stated that the OCC should require a national bank to comply only with the laws of the jurisdiction from which its electronic products or services are offered. A third commenter asked that we specifically clarify that other preemption rules in Federal law also apply to the electronic banking activities of national banks, such as the preemption rules set forth in the Electronic Signatures in Global and National Commerce Act (E-Sign). [27]

The final rule contains only one provision on the applicability of State law, now located at § 7.5002(c). This provision has been modified to address certain of the concerns the commenters have raised by clarifying the scope of preemption described in the rule, and to reflect developments in the law pertaining to electronic commerce.

In general, the application of State law to activities conducted by national banks through electronic means presents issues of preemption that are determined under traditional principles of Federal preemption derived from the Supremacy Clause of the United States Constitution [28] and applicable judicial precedent. The OCC's rules—currently and as amended by this final rule—

[24] *See* 12 CFR 7.1019.

[25] *See* OCC Conditional Approval No. 369 (Feb. 25, 2000) (national bank may host a virtual mall consisting of a web page with links to third-party merchants arranged according to product or service offered); OCC Conditional Approval No. 304 (Mar. 5, 1999) (electronic bill presentment is part of the business of banking). *See also* OCC Conditional Approval No. 220 (Dec. 2, 1996) (the creation, sale, and redemption of electronic stored value in exchange for dollars is part of the business of banking because it is the electronic equivalent of issuing circulating notes or other paper-based payment devices like travelers checks); OCC Conditional Approval No. 267, *supra* note 16 (a national bank may store electronic encryption keys as an expression of the established safekeeping function of banks).

[26] *See* Letter from Elizabeth H. Corey, Attorney (May 18, 1989) (unpublished); Letter from John M. Miller, Acting Deputy Chief Counsel (July 26, 1977) (unpublished).

[27] Pub. L. 106–229, 114 Stat. 464 (June 30, 2000).

[28] U.S. Const. art. VI, cl. 2.

provide that a national bank may conduct by electronic means any function or activity that it is otherwise authorized to conduct. The resolution of any issue about the applicability of State law to an activity that a national bank conducts electronically is, accordingly, governed by the preemption principles that would apply to activities conducted by traditional means.

However, when the activity is being conducted by electronic means, and thus is potentially geographically boundless, a consideration unique to the purpose and characteristics of the national bank charter becomes an element of this preemption analysis. Through the national bank charter, Congress established a banking system intended to be nationwide in scope, and authorized the creation of national banks, whose powers were intended to be uniform, as established by Federal law, regardless of where in the nation they conducted their business. As the Supreme Court has said:

> National banks are instrumentalities of the federal government, created for a public purpose, and as such necessarily subject to the paramount authority of the United States. It follows that an attempt by a state to define their duties, or control the conduct of their affairs is absolutely void, wherever such attempted exercise of authority expressly conflicts with the laws of the United States, and either frustrates the purpose of the national legislation, or impairs the efficiency of these agencies of the federal government to discharge the duties for the performance of which they were created.[29]

This freedom from State control over a national bank's powers protects national banks from conflicting local laws unrelated to the purpose of providing the uniform, nationwide banking system that Congress intended. And, as the Supreme Court also recognized, Congress was concerned not just with the application of certain States' laws to individual national banks, but also with the application of *multiple* States' standards which would undermine the uniform, national character of the powers of national banks throughout the system. This point was made clearly by the Supreme Court in *Easton* v. *Iowa,* 188 U.S. 220 (1903):

> That legislation [*i.e.,* legislation creating and regulating national banks] has in view the erection of a system extending throughout the country, and independent, so far as the powers conferred are concerned, of state legislation which, if permitted to be applicable, might impose limitations and restrictions as various and as numerous as the states. * * * [W]e are unable to perceive that Congress intended to leave the field open for the states to attempt to promote the welfare and stability of national banks by direct legislation. If they had such power it would have to be exercised and limited by their own discretion, *and confusion would necessarily result from control possessed and exercised by two independent authorities.*[30]

Thus, in analyzing the potential for State laws to be applicable to activities conducted by national banks via electronic means, it is also necessary to recognize in the preemption analysis that application of a multiplicity of State requirements in itself is an important factor in the analysis. Particularly where an activity is conducted via electronic means and is potentially accessible to a customer without any necessary connection to where the customer is physically located, application of multiple State law standards to that particular activity conflicts with the uniformity of standards under which national banks were designed to operate. The final rule's provision on the applicability of State law accordingly provides that the applicability of State law to a national bank's conduct of its authorized activities through electronic means and facilities is governed by traditional principles of Federal preemption derived from the Supremacy Clause, and that, therefore, a State law would not be applicable to such activities if the State law stands as an obstacle to the achievement of a Federal objective, namely, the ability of national banks to exercise uniformly their Federally authorized powers—in this case, through electronic means or facilities.[31]

The phrase ''stands as an obstacle'' was used by the Supreme Court in *Barnett Bank of Marion County* v. *Nelson*[32] as one of several formulations reflecting the standard for determining whether a State law is preempted, and we intend the use of this phrase to reflect the full dimensions of the Court's reasoning in that case. Notably, in *Barnett,* the Supreme Court cited *National Bank* v. *Commonwealth,*[33] a case decided very shortly after the establishment of the national banking system. In that decision, the Court held that the State law in question was not preempted because it did *not* ''interfere with, or impair [national banks'] efficiency in performing the functions for which they are designed * * *.''[34] This language was echoed 26 years later in the Court's decision in *Davis* v. *Elmira Savings Bank,* where the Court expressly recognized that State law may not ''frustrate the purpose'' of the ''national legislation'' creating the national banking system or ''impair the efficiency'' with which national banks function as the components of a uniform, nationwide banking system.[35] Clearly, the application of a multiplicity of State-based standards, each potentially altering—in different ways—the extent and manner in which a national bank may exercise any particular Federally authorized power through electronic means, would stand as an obstacle to achievement of the Federal objective, namely, a uniform, nationwide banking system,[36] and ''interfere with'' and ''impair'' the efficiency with which national banks are able to perform activities authorized under Federal law[37] through electronic means and facilities. The final rule contains revisions to appropriately reflect these considerations in determining the applicability of State law.

5. Composite Authority to Engage in Electronic Banking Activities (§ 7.5003)

We noted in the preamble to proposed § 7.5003 that some electronic banking activities that appear novel may actually be merely a collection of interrelated activities, each of which is permissible under well-settled authority. Thus, to clarify national banks' authority to conduct this type of composite activity, we proposed to adopt a new § 7.5003, which provides that an electronic

[29] *Davis* v. *Elmira Savings Bank,* 161 U.S. 275, 283 (1896). *See also Marquette Nat. Bank of Minneapolis* v. *First of Omaha Serv. Corp.,* 439 U.S. 299, 314–315 (1978); *First Nat. Bank of San Jose* v. *California,* 262 U.S. 366, 369 (1923) (''[A]ny attempt by a state to define [national banks'] duties or control the conduct of their affairs is void, whenever it conflicts with the laws of the United States or frustrates the purposes of the national legislation, or impairs the efficiency of the bank to discharge the duties for which it was created.'').

[30] *Easton,* 188 U.S. at 229, 231–232 (emphasis added).

[31] Of course, in some instances, Federal law will specify that national banks are to look to State law standards to determine the extent of their power to conduct certain activities (*e.g.,* establishment of intrastate branches, scope of fiduciary powers) or the manner in which a particular power may be exercised (*e.g.,* insurance).

[32] 517 U.S. 25 (1996).

[33] 76 U.S. (9 Wall.) 353 (1870).

[34] *Id.* at 362.

[35] *Davis,* 161 U.S. at 283, 284. In *Davis,* the Court held that a New York law purporting to require the receiver of an insolvent national bank to make preferential payment of receivership assets to ''any savings bank'' that had funds on deposit at the failed bank was preempted by the Federal statute requiring pro rata payment of such assets to any creditors who could prove their claims. The Court reasoned that one of the purposes of the ''national legislation'' creating the national banking system was ''to secure . . . a just and equal distribution of the assets of national banks among all unsecured creditors, and to prevent such banks from creating preferences in contemplation of insolvency. This public aim in favor of all the citizens of every state of the Union is manifested by the entire context of the national bank act.'' *Id.* at 284.

[36] Easton, 188 U.S. at 229, 231–32; *Davis,* 161 U.S. at 283–85.

[37] *National Bank,* 76 U.S. (9 Wall.) at 362; *Davis,* 161 U.S. at 283.

product or service comprised of several elements or activities is authorized if each of the constituent elements or activities is authorized.

Commenters supported this proposal because it addresses the reality that electronic products and services rarely fit into one specific category of authority. Thus, we are adopting this rule as proposed.

6. Excess Electronic Capacity (§ 7.5004)

The proposed rule in § 7.5004 recognized that the OCC has long applied the ''excess capacity'' doctrine to the technology resources of national banks to enable them to avoid waste and deploy those resources efficiently. [38] While the doctrine originated to allow banks to use excess real property efficiently, it has taken on particular significance as banks conduct more business through developing technologies such as Internet access, software production and distribution, long line telecommunications and data processing equipment, electronic security systems, and call centers.[39] Accordingly, we proposed to relocate the excess electronic capacity rule from current § 7.1019 to new subpart E and to add specific examples. The final rule adopts this approach, but amends the proposal in response to comments received.

The proposed rule stated that a national bank may acquire or develop excess capacity ''in good faith for banking purposes.'' In applying this test, the OCC and the courts consistently have reviewed a bank's objective business reasons for obtaining the excess capacity. To clarify the appropriate focus of the excess capacity test, and to avoid creating any misperception that the focus is on the subjective intent or mental state of bank management, the final rule states that a national bank may market and sell electronic capacities ''legitimately acquired or developed by the bank for its banking business.'' The ''legitimate'' standard incorporates the requirement that the excess capacity must be acquired in ''good faith'' for banking purposes.[40] This test recognizes the broad policy of optimization of resources and avoidance of loss or waste. To further clarify how the excess capacity doctrine is to be applied, we have provided specific and non-exclusive examples in the regulation to illustrate when legitimate excess electronic capacity may be acquired.

The final rule also adopts the proposed examples of excess capacity in equipment or facilities of national banks that have been found to have been acquired legitimately for banking purposes. The examples in the final rule are not exclusive, but merely illustrate uses of excess electronic capacity that we have approved. As our approvals to date demonstrate, the determination that a particular acquisition of excess electronic capacity is permissible is fact-specific. Accordingly, we encourage banks with questions regarding appropriate uses of excess electronic capacity to consult with the OCC.

In the preamble to the proposed rule, the OCC asked whether the final rule should codify a doctrine closely related to excess capacity: the so-called ''by-product doctrine.'' Under this authority, a national bank may sell by-products, such as software, legitimately developed by the bank for or during the performance of its permissible data processing functions. A number of commenters urged the OCC to explicitly codify the by-product doctrine. They noted that as part of their electronic banking products or internal operations, national banks often internally design and create software or other products that may have broader application. The by-product doctrine enables national banks to sell such products into the general market and, thus, gain revenue to offset internal development costs.

We have determined that it would be helpful to recodify the by-product doctrine in the final rule. Until 1984, the OCC's data processing rule specifically recognized the by-product doctrine.[41] Although this language was deleted from the rule in 1984,[42] it was not done with the intention to change the OCC's position regarding this theory. The 1984 revision was merely a non-substantive format change in the rule done largely to avoid potential confusion. The OCC believes that it has now developed a considerable body of precedent on the by-product doctrine that will help provide adequate guidance on these issues and reduce the risk of confusion.[43]

7. National Bank Acting as a Digital Certification Authority (§ 7.5005)

The OCC has permitted a national bank to act as a certification authority [44] that issues certificates verifying the *identity* of the certificate holder to support digital signatures.[45] Proposed § 7.5005 would codify this position. Comments supported this proposal and it is adopted without significant change in paragraph (a) of § 7.5005.

The preamble to the proposed rule requested comments on whether the final rule should also authorize national banks to issue digital certificates that verify attributes beyond mere identity, *i.e.,* the authority or financial capacity of the certificate holder. We invited comment on the extent to which national banks propose to engage in these activities, how they will be structured, and whether permitting national banks to issue certificates to verify additional attributes beyond identity presents unique risks.

Generally, commenters strongly supported extending the certification authority to attributes beyond identity. Commenters said that verification of certificate holder transaction authority and financial capacities are necessary for banks to be able to effectively market electronic banking services. These commenters noted that national banks have long had experience in certifying the financial capacity of their

[38] The excess capacity doctrine holds that a bank properly acquiring an asset to conduct its banking business is permitted, under its incidental powers, to make full economic use of the property if using the property solely for banking purposes would leave the property underutilized. *See* OCC Conditional Approval No. 361 (Mar. 3, 2000).

[39] *See* OCC Interpretive Letter No. 742, *reprinted in* [1996–1997 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81–106 (Aug. 19, 1996); OCC Interpretive Letter No. 677, *reprinted in* [1994–1995 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 83,625 (June 28, 1985); Letter from William Glidden (June 6, 1986) (unpublished); Letter from Stephen Brown (Dec. 20, 1989) (unpublished); and OCC Conditional Approval No. 361 (Mar. 3, 2000).

[40] *See* OCC Interpretive Letter No. 888, *reprinted in* [2000–2001 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81,407 (Mar. 14, 2000). *See also Brown* v. *Schleier*, 118 F. 981 (8th Cir. 1902), *aff'd.* 194 U.S. 18 (1904).

[41] *See* 12 CFR 7.3500 (1983).

[42] *See* 49 FR 11157 (Mar. 26, 1984).

[43] *See, e.g.*, OCC Interpretive Letter No. 284, *reprinted in* [1983–1984 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,448 (Mar. 26, 1984); OCC Interpretive Letter No. 449, *reprinted in* [1988–1989 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,673 (Aug. 23, 1988); and OCC Interpretive Letter No. 677, *supra* note 53.

[44] *See* OCC Conditional Approval No. 267, *supra* note 16.

[45] Digital signatures are a form of electronic authentication that permit the recipient of an electronic message to verify the sender's identity. In order for a digital signature system to operate successfully, the message recipient must have assurance that the public key used to decode a message is uniquely associated with the sender. One method of providing that assurance is for a trusted third-party (called a ''certification authority'') to issue a digital certificate attesting to this association. The certification authority generates and signs digital certificates to verify the identity of the person transmitting a message electronically. The mathematical function the sender uses to encode a message is called the sender's private key. The related function that the recipient of the message uses to decode the message is called the sender's public key. In public key infrastructure (''PKI'') systems based on asymmetric encryption, each private key is uniquely associated with a particular counterparty public key. Thus, if one has assurance that a specific private key is associated with a person and under his or her sole control, any message that can be decoded using that person's public key may be assumed to have been sent by that person.

customers. For example, banks issue letters of credit or loan approval letters to give comfort to third parties that the bank customer has the financial capacity to consummate contemplated transactions. Banks also manage and verify account numbers, account balances, and transactions charged to those account numbers. Some commenters requested that the final rule not be limited to a particular list of functions. They noted that the methods and usefulness of certification authority services will continue to evolve. Thus, they urged that the final rule should enhance flexibility so that a certificate can be issued for any purpose where the underlying verification is part of the business of banking. They requested that the final rule list particular attributes, such as financial capacity, as examples of this extended certification authority activity.

However, other commenters urged the OCC to consider the risks that may arise when the new certification activities either are combined with or approximate in function the existing authority for independent undertakings. [46] The commenters were particularly concerned that any new authority to issue extended certificates relating to financial capacity might raise risks similar to those assumed by banks issuing letters of credit and other independent undertakings.

The final rule provides that national banks may issue digital certificates to verify any attribute for which verification is part of or incidental to the business of banking and lists several types of financial capacity as examples of such attributes. This list is intended to be non-exclusive. We will consider what other attributes might be verified in an electronic certificate on a case-by-case basis so that the potential risks can be better assessed.

We recognize that the extended authority to issue non-identity digital certificates presents supervisory issues. We have existing guidance on digital certificates (OCC Bulletin 99–20), and intend to update that guidance to address issues arising under the extended authority codified in § 7.5005(b). These issues arise in part because the party issuing the certificate is verifying an attribute—such as financial capacity—that can and does change over time.

If a bank were to verify that funds will be available on a certain date in its certificates, the bank would, in effect, be engaging in an electronic independent undertaking. However, the extended certificate authority codified in § 7.5005(b) is distinct from independent undertakings, both analytically and operationally. To facilitate this distinction, the final rule clarifies by examples the types of financial verifications that the OCC intends to authorize in extended certifications. Specifically, the final rule lists examples of permissible financial certifications that involve verification of the following existing facts: (1) Account balance as of a particular date; (2) lines of credit as of a particular date; (3) past performance of customer (like a credit report); and (4) verification of customer relationship as of a particular date. Each of these verifications represents a statement of fact as of a particular current or previous date with respect to the certificate subscriber. Thus, financial certificates do not represent a promise by the certificate authority bank to the relying party that particular funds will be available or advanced for a particular transaction. For this reason, a financial certification is distinguished from an independent undertaking, which is a promise by a bank to make available funds for a particular transaction upon presentation of specified documents. An independent undertaking exposes the issuing bank to credit risk; a properly formulated and limited financial certification does not.

We expect banks issuing financial capacity certificates to take steps appropriate to address the risk that a party receiving a financial certification (the relying party, usually a seller) would assert that the certification is really an implied promise or representation by the issuing bank that funds will be available or advanced to pay for a particular transaction. We expect issuing banks to take appropriate precautions against having their financial certificates construed as implied promises to lend. While other risk controls will be appropriate in particular cases,[47] the final rule provides that financial capacity certificates must include express disclaimers stating that the bank does not thereby promise or represent that funds will be available or advanced for a particular transaction.

If banks take necessary precautions and issue appropriately designed financial certifications, the requirements of § 7.1016 (which are designed predominantly to control credit risk) should not be required as a risk mitigation device. However, if a purported financial capacity certificate did guarantee or promise funds availability, the requirements of § 7.1016 should and will apply. Under the transparency rule in § 7.5002 of the final rule, electronic letters of credit are clearly permissible. However, in contrast to the financial certifications authorized under § 7.5005 of this final rule, electronic letters of credit are subject to § 7.1016 because they are independent undertakings.[48]

Finally, the proposed rule contemplated that verification will be provided as part of a digital certificate, *i.e.*, the certificate *itself* would contain the verified information on authority or financial capacity. However, some commenters requested that the final rule also enable banks to issue certificates that interoperate with the bank's internal systems so that the certificate is associated automatically with information in those systems related to the certificate holder. In other words, the verified information would reside not in the certificate, but in bank systems linked to the certificate. The benefit of this approach is that a system-linked certificate can provide access to information that is updated whenever the bank's systems are updated, whereas information resident on the certificate can become rapidly outdated. Thus, some comments urged that the final rule expressly authorize banks to engage in electronic authentication activities regardless of the particular technology employed.

We agree that there are significant advantages to system-linked certificates. However, such certificates also present very different risks than the certificate-based PKI systems for which the OCC has issued guidance. [49] For this reason, the final rule does not contain a general authorization for system-linked certificates. However, we are prepared to consider on a case-by-case basis how national banks may use new technologies and models, beyond PKI-based digital certificates, to provide permissible electronic verification services.

8. Data Processing (§ 7.5006)

Proposed § 7.5006(a) codified OCC interpretations confirming that a national bank may collect, process,

[46] *See* 12 CFR 7.1016.

[47] For example, the risk of confusion may be particularly great in situations where the bank is issuing a financial certification on the existence of a line of credit. Relying parties might try to assert that this certificate constitutes an implied promise that the verified credit line would be available to fund their specific transaction. Thus, in connection with such certifications, the issuing bank might not only include the disclaimer discussed above but also make available with the digital certificate the terms of the line of credit so that the relying parties may directly assess its availability for their transaction.

[48] *See* 12 CFR 7.5005(c).

[49] *See* OCC Bulletin 99–20.

transcribe, analyze, and store banking, financial, and economic data for itself and its customers as part of the business of banking.[50] Commenters were generally supportive of this aspect of the proposed rule and we are adopting it with some changes. Specifically, the final rule provides additional guidance on the scope and range of permissible banking, financial or economic data processing in two ways. First, the final rule clarifies that permissible ''processing'' of eligible data includes provision of data processing services, data transmission services, facilities (including equipment, technology, and personnel), databases and advice. It also includes providing access to such services, facilities, databases and advice. Second, the rule specifies that for purposes of this section, ''economic data'' includes anything of value in banking and financial decisions.[51]

In addition to processing of banking, financial or economic data, national banks, under their authority to conduct activities incidental to the business of banking, may also provide limited amounts of non-financial information processing to their customers to enhance marketability or use of a banking service.[52] In determining the permissible scope of this incidental processing, we typically inquire whether the processing of non-financial data is convenient or useful to the specific processing of financial data or other business of banking activities in a specific contract or relationship.

Thus, in the preamble discussing proposed § 7.5006, we requested comment on whether to codify this authority to conduct incidental non-financial data processing and specifically whether to provide that a national bank may generally derive a certain specified percentage of its total annual data processing revenue from processing non-financial data. Anecdotal evidence suggested that national banks attempting to market financial data processing services are frequently confronted with customer demands that the bank also process some non-financial data so that the customer can avoid the inconvenience of having to use two different processors for financial data and for non-financial data. Moreover, banks' competitors in the marketplace are providing these fully integrated data processing services. Thus, we asked for comments and evidence on the extent of this type of customer demand in order to determine whether it is so pervasive as to warrant authorizing the processing of non-financial data in connection with financial data processing in lieu of our current case-by-case approach.

The comments filed in response to this request supported codification of the authority to engage in incidental non-financial data processing. These comments establish that such a rule is warranted to accommodate pervasive realities of the financial data processing marketplace. Accordingly, we have decided to adopt a more flexible approach to non-financial data processing rather than a safe harbor with a specific percentage (*e.g.,* 30% or 49%). We believe that, in light of the rapidly evolving nature of bank data processing and the data processing markets in which banks compete, a fixed percentage could be inappropriately rigid.

The final rule therefore provides that, in addition to its authority to process banking, financial, and economic data, a national bank may also process additional types of data to the extent convenient or useful to the bank's ability to provide the banking, financial, and economic data processing services. This approach to permissible incidental data processing would be satisfied where providing non-financial data processing is reasonably necessary to conduct the financial data processing services on a competitive basis. The bank's total revenue from providing data processing services under this section must, however, be derived *predominantly by* from processing banking, financial, or economic data. Thus, under the final rule, a bank offering financial data processing services will also be able to offer additional processing of incidental non-financial data if it determines that, in the market it is attempting to serve, processing of some non-financial data is reasonably necessary to operate on a competitive basis and if the aggregate revenue from such incidental non-financial processing is not the predominant source of its total revenue from data processing services under this section.

We believe this approach, which is fully consistent with judicial and OCC precedent, [53] is preferable to a specific percentage-based safe harbor because it adheres to concepts that allow a component of the bank's data processing to include non-financial data processing and provides more flexibility to accommodate the evolving role in data processing in the business of banking. Banks that engage in financial or non-financial data processing will be expected to comply with all applicable supervisory requirements and guidance.[54] The OCC will develop additional guidance for examiners and bankers on data processing activity, as needed.

In addition to the authority to provide data processing under this section, national banks also have other

[50] *See, e.g.,* OCC Conditional Approval No. 289 (Oct. 2, 1998); OCC Interpretive Letter No. 805, *reprinted* in [1997–1998 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81,252 (Oct. 9, 1997). A prior OCC interpretive ruling on electronic banking specifically stated that ''as part of the business of banking and incidental thereto, a national bank may collect, transcribe, process, analyze and store for itself and others, banking, financial, or related economic data.'' 39 FR 14192, 14195 (Apr. 22, 1974). This language was deleted from former 12 CFR 7.3500 because the OCC was concerned that the specific examples of permissible activities in the ruling, such as the marketing of excess time, by-products, and the processing of ''banking, financial, or related economic data,'' had led to confusion and misinterpretation. *See* 47 FR at 46526, 46529 (Oct. 19, 1982). However, the preamble to the proposal to simplify the rule stated that ''the Office wishes to make clear that it does not intend to indicate any change in its position regarding the permissibility of data processing services.'' *Id.* Since 1982, the risk of confusion and misinterpretation of a regulation has significantly diminished due to, among other reasons, the substantial number of interpretive letters the OCC has issued on permissible data processing that can provide a context for understanding the rule.

[51] *See, e.g., Association of Data Processing Service Organizations, Inc.* v. *Board of Governors,* 745 F.2d 677, 691 (D.C. Cir. 1984).

[52] *See, e.g.,* OCC Conditional Approval No. 369 (Feb. 25, 2000).

[53] *See generally* § 7.5001(c)(2). OCC has long held that a national bank, under its incidental powers, may sell non-banking products and services when reasonably necessary to provide banking products on a competitive basis by creating a package of related services needed to satisfy consumer demand, meet market competition, and enable the bank to successfully market its banking services. Thus, for example, in OCC Interpretive Letter No. 742, *supra* note 53, OCC found offering of Internet access service was needed to successfully provide and market the bank's Internet banking service. We found limiting the bank's Internet access services, to block non-banking use, would not meet customer needs or the competing products in the marketplace. *See also* OCC Interpretive Letter No. 611, *supra* note 6 (bank selling home banking service can also provide customer access to non-banking services ''to increase the customer base and service the usage of the program''); OCC Interpretive Letter No. 653, *reprinted in* [1994–1995 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 83,601 (Dec. 22, 1994) (national banks may offer non-banking products as part of larger product or service when necessary, convenient, and useful to bank permissible activities); *cf. National Courier Ass'n* v. *Board of Governors,* 516 F.2d 1229, 1240 (D.C. Cir. 1975) (incidental powers of holding companies include providing specialized courier services when service is necessary to obtain full benefit of data processing services). *Compare National Retailers Corp.* v. *Valley Nat'l Bank,* 411 F. Supp. 308 (D. Ariz. 1976), *aff'd,* 604 F. 2d 32 (9th Cir. 1979). In light of subsequent developments, however, for the reasons stated in OCC Interpretive Letter 928 (Dec. 24, 2001) and Interpretive Letter No. 856 (Mar. 5, 1999), the OCC does not believe that courts today would accord significant weight to the *National Retailers* case.

[54] *See, e.g.,* OCC Alert No. 2001–4 (Network Security Vulnerabilities); OCC Advisory Letter No. 2001–12 (Risk Management of Outsourcing Technology); and OCC Bulletin No. 2000–14 (Infrastructure Threats-Intrusion Risks—Message to Bankers and Examiners).

authorities to process data that is non-financial. For example, banks may process data (regardless of the type) under the excess capacity doctrine and under their correspondent authority. These additional authorities are codified in other sections of the new Subpart E;[55] their rationale and concomitant limitations are independent and distinct from the authority to process banking, financial, and economic data and incidental non-financial data under § 7.5006 of the final rule. Thus, the revenue derived from non-financial data processing that may occur under these other authorities and activities is not included as non-banking, financial, or economic data processing revenue in computing the total revenue from § 7.5006 data processing services used to determine compliance with the predominantly proviso in new § 7.5006(b).

9. Correspondent Services (§ 7.5007) [56]

The proposed rule codified the OCC's longstanding interpretation that national banks may perform for other entities an array of activities called ''correspondent services'' as part of the business of banking.[57] These activities include any corporate or banking service that a national bank may perform for itself.[58] A national bank may perform these activities for any of its affiliates or for other financial institutions.[59]

This proposal also codified a number of OCC interpretations that approve certain electronic- and technology-related activities as permissible correspondent services for national banks and included these activities in the text of the regulation as examples of electronic activities that banks may offer as correspondent services. These examples included: (1) Providing computer networking packages and related hardware that meet the banking needs of financial institution customers; [60] (2) processing bank, accounting, and financial data, such as check data, other bookkeeping tasks, and general assistance of correspondents' internal operating, bookkeeping, and data processing; [61] (3) selling data processing software; [62] (4) developing, operating, managing, and marketing products and processing services for transactions conducted at electronic terminal devices including, but not limited to, ATMs, POS terminals, scrip terminals, and similar devices; [63] (5) item processing services and related software development; [64] (6) document control and record keeping through the use of electronic imaging technology; [65] (7) Internet merchant hosting services for resale to merchant customers; [66] and (8) communication support services through electronic means, such as: (i) The provision of electronic ''gateways'' in order to communicate and receive financial information and to conduct transactions; (ii) creating, leasing, and licensing communications systems, computers, analytic software, and related equipment and services for sharing information concerning financial instruments and economic information and news; and (iii) the provision of electronic information and transaction services and linkage for financial settlement services.[67]

Two commenters requested that the OCC add digital certification authority services to these examples of permissible correspondent activities. We agree that it is appropriate to add this activity to § 7.5007 because we have previously approved it in interpretive letters.[68] Accordingly, the final rule includes this activity as an additional example.

Two other commenters expressed concern that, as proposed, § 7.5007 may give the impression that the OCC considers the list of permissible correspondent activities in the regulation to be exhaustive. As indicated above, this list is a codification of existing OCC interpretations and is not intended to be restrictive. To clarify this point, we have amended § 7.5002 to specifically provide that these examples are only illustrative. We will continue to consider, on a case-by-case basis, the authorization of new electronic- and technology-related activities as correspondent services offered by national banks that may not be included in the examples provided in the regulation.

B. Location

1. Location of a National Bank Conducting Electronic Activities (§ 7.5008)

As the OCC noted in the preamble to the proposed rule, the effect of several statutes affecting national banks turns in part on where the bank in question is ''located.'' In addition, the scope of this term (or closely related statutory terms, such as ''situated'')—whether it refers only to the bank's main office, includes branches as well, or means something different—varies from statute to statute. [69] Moreover, national banks often conduct a significant portion of their operations in locations that are distinct from their main office and branches.

To remove any ambiguity on the scope of this term, the proposed rule provided that a national bank will not be considered located in a State solely because it physically maintains equipment or facilities that are necessary for the use of electronic technologies, such as a server or automated loan center, in that State, or because the bank's products or services are accessed through electronic means by customers located in the State. This interpretation of ''located'' is consistent with evolving case authority.[70] Thus, for example, these factors would not result in a bank being considered to be

[55] *See, e.g.,* §§ 7.5001(d), 7.5004, and 7.5007.

[56] We have modified the title of this section from ''correspondent banking'' to ''correspondent services'' to more accurately reflect the activity authorized by this section.

[57] *See, e.g.,* OCC Interpretive Letter No. 875, *supra* note 6; OCC Interpretive Letter No. 811, *reprinted* in [1997–1998 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81–259 (Dec. 18, 1997); OCC Corporate Decision No. 97–79 (July 11, 1997).

[58] See OCC Interpretive Letter No. 467, reprinted in [1988–1989 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,691 (Jan. 24, 1989) (national bank may offer wide range of correspondent services); Letter from Wallace S. Nathan, Regional Counsel (Dec. 3, 1982) (unpublished) (microfiche services); Letter from John E. Shockey, Chief Counsel (July 31, 1978) (unpublished) (advertising services).

[59] *See, e.g.,* OCC Interpretive Letter No. 875, *supra* note 6; OCC Interpretive Letter No. 513, *reprinted* in [1990–1991 Transfer Binder] Fed. Banking L. Rep. ¶ 83,215 (June 18, 1990).

[60] *See* OCC Interpretive Letter No. 754, *supra* note 20.

[61] *See, e.g.,* Letter from Vernon E. Fasbender, Director for Analysis, Southeastern District (Dec. 6, 1990); OCC Interpretive Letter No. 345, *reprinted in* [1985–1987 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,515 (July 9, 1985); Letter from Joe H. Selby, Deputy Comptroller (Nov. 22, 1978).

[62] *See, e.g.,* OCC Interpretive Letter No. 868, *reprinted in* [Current Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81–362 (Aug. 16, 1999).

[63] *See, e.g.,* OCC Interpretive Letter No. 890, *reprinted in* [1999–2000 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81–409 (May 15, 2000).

[64] *See, e.g.,* Letter from Vernon E. Fasbender, Director for Analysis, Southeastern District (Dec. 6, 1990); and Letter from J.T. Watson, Deputy Comptroller of the Currency (Mar. 22, 1973).

[65] *See* OCC Interpretive Letter No. 805, *supra* note 64.

[66] *See* Corporate Decision No. 2000–08 (June 1, 2000); and OCC Interpretive Letter No. 875, supra note 6.

[67] *See* OCC Interpretive Letter No. 611, *supra* note 6; OCC Interpretive Letter No. 516, supra note 6; and OCC Interpretive Letter No. 346, *reprinted* in [1985–1987 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,516 (July 31, 1985).

[68] *See* OCC Conditional Approval No. 339 (Nov. 6, 1999).

[69] *See, e.g.,* 12 U.S.C. 24 (Eighth) (charitable contributions); 12 U.S.C. 29 (authority to hold real estate); 12 U.S.C. 36 (branching); 12 U.S.C. 72 (director qualifications); 12 U.S.C. 92 (authority to act as insurance agent or broker); 12 U.S.C. 92a (trust powers); 12 U.S.C. 94 (venue); 12 U.S.C. 215 and 215a (bank consolidations and mergers); and 12 U.S.C. 548 (State taxation).

[70] *See, e.g., Amberson Holdings LLC* v. *Westside Story Newspaper,* 110 F. Supp. 2d 332 (D.N.J. 2000).

''located'' in a particular State for purposes of 12 U.S.C. 85.

Most of those who commented on this issue supported our proposal. One commenter asked that we amend this provision to state specifically that a product or service provided through electronic means shall be deemed to be offered and delivered from a single location. This suggestion raises broader issues that require additional analysis, which at this time we believe is best undertaken on a case-by-case basis rather than through this rulemaking.

Another commenter requested that we delete the word ''solely'' from the proposed provision in order to eliminate any inference that the location of a bank's technological equipment or customers may ever be considered in the determination of a bank's ''location.'' It is not our intent to remove these factors altogether from the determination of where a bank is located since the equipment may be connected to other relevant activities of the bank. Instead, the purpose of this provision is simply to make clear that these factors alone will not determine the bank's location in a State.

Accordingly, the OCC has adopted § 7.5008 as proposed.

2. Location Under 12 U.S.C. 85 of National Banks Operating Exclusively Through the Internet (§ 7.5009)

Twelve U.S.C. 85 authorizes a national bank to charge interest in accordance with the laws of the State in which it is located. In interpreting section 85, the Supreme Court has held that a national bank is ''located'' in the State where it has its main office (its home State).[71] Thus, a national bank may charge the interest rates permitted by its home State no matter where the borrower resides or what contacts with the bank occur in another State.

The OCC has chartered several national banks without physical branches that make loans or extend credit exclusively through the Internet. The proposal provided that, for purposes of 12 U.S.C. 85, the main office of a national bank that operates exclusively through the Internet is the office identified by the bank under 12 U.S.C. 22 (Second) or as relocated pursuant to 12 U.S.C. 30 or other appropriate authority.

Many commenters supported this section as proposed. We therefore are adopting this section in the final rule, with one minor technical change. Because the OCC does not always use the term ''Internet-only'' in its guidance and interpretations, we have removed that term from the title of § 7.5009.

C. Safety and Soundness

Shared Electronic Space (§ 7.5010)

In light of the increased ability of national banks to enter into joint marketing relationships with third-parties through the Internet, we proposed to extend the same general principles as set forth in 12 CFR 7.3001[72] on shared physical space to situations where banks share co-branded web sites or other electronic space with subsidiaries, affiliates, or other third-parties. The proposed rule was in part based upon our recent guidance on weblinking arrangements,[73] and was designed to reduce risk of customer confusion. To that end, the proposed rule would have required national banks to take reasonable steps to enable customers to distinguish between products and services offered by the bank and those offered by the third-party. The bank also would have been required to disclose its limited role with respect to the third-party product or service and to call attention to the fact that the bank does not provide, endorse, or guarantee any of the products or services available from the third-party.

However, many commenters expressed concern that the proposed rule was excessively prescriptive and would unduly limit industry flexibility in responding to the risks of customer confusion regarding shared electronic space. These commenters suggested that a prescriptive rule was unnecessary at this time in light of the OCC Weblinking Bulletin and that the OCC should delay action on a rule until the agency has had more opportunity to evaluate the effectiveness and impact of the Bulletin.

We have decided to adopt a shared electronic space rule, but with significant changes to the proposed rule that are responsive to comments received. In our view, a general rule on shared electronic space is needed to address broader forms of shared electronic space that are becoming increasingly prevalent, but are not covered by the OCC Weblinking Bulletin. These forms include shared web sites and bank web pages that are embedded in third-party sites. The final rule on electronic shared space will provide guidance to the industry, promote greater awareness of relevant issues, and facilitate examiner efforts to supervise this activity.

However, we have decided not to promulgate at the present time the more specific portions of the proposed rule that would have required a national bank with shared electronic space to make specific disclosures of its limited role with respect to third-party products and to advise that the bank does not provide, endorse, or guarantee any of the products or services available through the shared electronic space. In light of concerns expressed by many commenters, we believe that it would be appropriate to gain more experience in this area before codifying detailed requirements.

The final rule requires that national banks sharing electronic space with a third-party must take reasonable steps to clearly, conspicuously, and understandably distinguish between products and services offered by the bank and those offered by the third-party. In determining whether a bank has taken reasonable steps to distinguish third-party products and services available through shared electronic space, we will consider a number of factors. Among other things, we will look at web page formatting (including visual cues to the consumer), text-based or audio narrative, and compliance with other product-specific regulatory disclosure requirements. Additionally, what constitutes ''reasonable steps'' will depend upon the specific product and context; some products and contexts may require more information to be disclosed than others. Finally, the OCC Weblinking Bulletin will provide helpful guidance regarding both linking arrangements and other non-linking forms of shared electronic space.

A number of holding company commenters were concerned about how the proposed rule would apply to holding company web sites that share a common name with the bank and have web pages for a subsidiary national bank embedded in the holding company site. These commenters suggested that the final rule should not cover situations where a subsidiary bank shares its holding company's web site. However, we have consistently applied § 7.3001 to

[71] *See Marquette Nat. Bank* v. *First of Omaha Serv. Corp.,* 439 U.S. 299 (1978). The OCC also has determined that for purposes of section 85, under certain circumstances, an interstate national bank may be considered to be ''located'' in a state where it has a branch. In this situation, the bank may be required to impose interest rates in accordance with the law of the branch state. *See* OCC Interpretive Letter No. 822 (Feb. 17, 1998). A national bank that operates exclusively through the Internet and thus has no branches would not be affected by this interpretive letter.

[72] Under 12 CFR 7.3001, a national bank may lease space on bank premises to other businesses and share space jointly with other businesses subject to certain conditions. The conditions set forth in § 7.3001(c) are intended to minimize customer confusion about the nature of the products offered and promote the safe and sound operation of the bank.

[73] *See* OCC Bulletin 2001–31 (''OCC Weblinking Bulletin'').

physical space shared with affiliates. Moreover, in the physical non-electronic context, we have found that serious customer confusion potentially can arise when national banks sell holding company products and obligations, including commercial paper, on bank premises. Likewise, we are concerned that, if banks do not provide adequate disclosures in electronic space shared with affiliates, bank customers will become confused over the bank's responsibility for an affiliate's products and obligations sold through that shared space. For this reason, we have decided not to exclude affiliates from coverage by the final rule. However, the elimination of the more specific provisions of the proposed rule should largely ameliorate the concerns of the commenting holding companies.

Regulatory Flexibility Act

Pursuant to section 605(b) of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), the regulatory flexibility analysis described in section 603 of the RFA, 5 U.S.C. 603, is not required if the head of the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities and the agency publishes such a certification and a statement explaining the factual basis for such certification in the **Federal Register** along with its final rule.

On the basis of the information currently available, the Comptroller of the Currency certifies that this final rule will not have a significant impact on a substantial number of small entities within the meaning of those terms as used in the RFA. The final regulation requires a national bank that shares a co-branded website or other electronic space with a bank subsidiary or a third-party to make certain disclosures designed to enable its customers to distinguish its products and services from those of the subsidiary or third-party. We believe it will be relatively inexpensive for a bank, either internally or through a servicer, to create and display the disclosures required by this regulation. Updating a website is a fixed cost for a bank, and is a practice that is done periodically. In addition, national banks are currently required to provide similar disclosures for leased space on bank premises and when sharing space jointly with other businesses. Therefore, the OCC does not believe that this requirement will have a significant impact on a substantial number of small entities. Accordingly, a regulatory flexibility analysis is not required.

Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995, Pub. L. 104–4 (Unfunded Mandates Act) requires that an agency prepare a budgetary impact statement before promulgating a rule that includes a Federal mandate that may result in expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. If a budgetary impact statement is required, section 205 of the Unfunded Mandates Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule.

The OCC has determined that the final rule will not result in expenditures by State, local, or tribal governments or by the private sector of $100 million or more. Accordingly, the OCC has not prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

Executive Order 12866

The Comptroller of the Currency has determined that this rule does not constitute a ''significant regulatory action'' for the purposes of Executive Order 12866. Under the most conservative cost scenarios that the OCC can develop on the basis of available information, the annual effect on the economy of the final rule falls well short of the $100 million threshold established by the Executive Order.

Paperwork Reduction Act of 1995

The OCC may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), the information collection requirements contained in this rulemaking have been approved under OMB control number 1557–0225. The OCC sought comment on all aspects of the burden estimates for the information collection contained in the proposed rule (66 FR 34855, July 2, 2002). The OCC received no comments.

The information collection requirements are contained in § 7.5010. This section requires a national bank that shares a co-branded website or other electronic space with a bank subsidiary or a third-party to make certain disclosures designed to enable its customers to distinguish its products and services from those of the subsidiary or third-party.

Estimated number of respondents: 1,609.

Estimated number of responses: 1,609.

Estimated burden hours per response: 1 hour.

Estimated total burden hours: 1,609 hours.

The OCC has a continuing interest in the public's opinion regarding collections of information. Members of the public may submit comments to Jessie Dunaway, OCC Clearance Officer, 250 E Street, SW, Attention: 1557–0225, Mailstop 8–4, Washington, DC 20219. Due to the temporary delay in mail delivery, you may prefer to send your comments by electronic mail to *jessie.dunaway@occ.treas.gov,* or by fax to (202) 874–4889.

Effective Date

The Riegle Community Development and Regulatory Improvement Act of 1994 requires that any new regulation that imposes ''additional reporting, disclosure, or other requirements on insured depository institutions shall take effect on the first day of a calendar quarter which begins on or after the date on which the regulations are published in final form,'' less certain exceptions apply.[74] This rulemaking contains one section that imposes additional disclosure requirements on national banks. Section 7.5010 requires national banks that share electronic space, including a co-branded web site, with a bank subsidiary, affiliate, or another third-party to take reasonable steps to clearly, conspicuously, and understandably distinguish between products and services offered by the bank and those offered by the bank's subsidiary, affiliate, or the third-party. Accordingly, the requirement to delay the effective date until the first day of the next calendar quarter applies to § 7.5010. The remaining sections of this final rule do not impose additional reporting, disclosure, or other requirements on insured depository institutions and therefore will become effective 30 days after publication, in accordance with 5 U.S.C. 553(d).

List of Subjects in 12 CFR Part 7

Credit, Insurance, Investments, National banks, Reporting and recordkeeping requirements, Securities, Surety bonds.

Authority and Issuance

For reasons set forth in the preamble, the OCC amends part 7 of chapter I of

[74] Pub. L. 103–325, section 302(b) (Sept. 23, 1994).

title 12 of the Code of Federal Regulations as follows:

PART 7—BANK ACTIVITIES AND OPERATIONS

1. The authority citation for part 7 continues to read as follows:

Authority: 12 U.S.C. 1 *et seq.*, 92, 92a, 93, 93a, 481, 484, 1818.

2. Section 7.1002 is revised to read as follows:

§ 7.1002 National bank acting as finder.

(a) *General.* It is part of the business of banking under 12 U.S.C. 24(Seventh) for a national bank to act as a finder, bringing together interested parties to a transaction.

(b) *Permissible finder activities.* A national bank that acts as a finder may identify potential parties, make inquiries as to interest, introduce or arrange contacts or meetings of interested parties, act as an intermediary between interested parties, and otherwise bring parties together for a transaction that the parties themselves negotiate and consummate. The following list provides examples of permissible finder activities. This list is illustrative and not exclusive; the OCC may determine that other activities are permissible pursuant to a national bank's authority to act as a finder.

(1) Communicating information about providers of products and services, and proposed offering prices and terms to potential markets for these products and services;

(2) Communicating to the seller an offer to purchase or a request for information, including forwarding completed applications, application fees, and requests for information to third-party providers;

(3) Arranging for third-party providers to offer reduced rates to those customers referred by the bank;

(4) Providing administrative, clerical, and record keeping functions related to the bank's finder activity, including retaining copies of documents, instructing and assisting individuals in the completion of documents, scheduling sales calls on behalf of sellers, and conducting market research to identify potential new customers for retailers;

(5) Conveying between interested parties expressions of interest, bids, offers, orders, and confirmations relating to a transaction;

(6) Conveying other types of information between potential buyers, sellers, and other interested parties; and

(7) Establishing rules of general applicability governing the use and operation of the finder service, including rules that:

(i) Govern the submission of bids and offers by buyers, sellers, and other interested parties that use the finder service and the circumstances under which the finder service will pair bids and offers submitted by buyers, sellers, and other interested parties; and

(ii) Govern the manner in which buyers, sellers, and other interested parties may bind themselves to the terms of a specific transaction.

(c) *Limitation.* The authority to act as a finder does not enable a national bank to engage in brokerage activities that have not been found to be permissible for national banks.

(d) *Advertisement and fee.* Unless otherwise prohibited by Federal law, a national bank may advertise the availability of, and accept a fee for, the services provided pursuant to this section.

3. Section 7.1019 is removed.

4. New subpart E is added to read as follows:

Subpart E—Electronic Activities

Sec.

7.5000 Scope.
7.5001 Electronic activities that are part of, or incidental to, the business of banking.
7.5002 Furnishing of products and services by electronic means and facilities.
7.5003 Composite authority to engage in electronic activities.
7.5004 Sale of excess electronic capacity and by-products.
7.5005 National bank acting as digital certification authority.
7.5006 Data processing.
7.5007 Correspondent services.
7.5008 Location of national bank conducting electronic activities.
7.5009 Location under 12 U.S.C. 85 of national banks operating exclusively through the Internet.
7.5010 Shared electronic space.

Subpart E—Electronic Activities

§ 7.5000 Scope.

This subpart applies to a national bank's use of technology to deliver services and products consistent with safety and soundness.

§ 7.5001 Electronic activities that are part of, or incidental to, the business of banking.

(a) *Purpose.* This section identifies the criteria that the OCC uses to determine whether an electronic activity is authorized as part of, or incidental to, the business of banking under 12 U.S.C. 24 (Seventh) or other statutory authority.

(b) *Restrictions and conditions on electronic activities.* The OCC may determine that activities are permissible under 12 U.S.C. 24 (Seventh) or other statutory authority only if they are subject to standards or conditions designed to provide that the activities function as intended and are conducted safely and soundly, in accordance with other applicable statutes, regulations, or supervisory policies.

(c) *Activities that are part of the business of banking.* (1) An activity is authorized for national banks as part of the business of banking if the activity is described in 12 U.S.C. 24 (Seventh) or other statutory authority. In determining whether an electronic activity is part of the business of banking, the OCC considers the following factors:

(i) Whether the activity is the functional equivalent to, or a logical outgrowth of, a recognized banking activity;

(ii) Whether the activity strengthens the bank by benefiting its customers or its business;

(iii) Whether the activity involves risks similar in nature to those already assumed by banks; and

(iv) Whether the activity is authorized for state-chartered banks.

(2) The weight accorded each factor set out in paragraph (c)(1) of this section depends on the facts and circumstances of each case.

(d) *Activities that are incidental to the business of banking.* (1) An electronic banking activity is authorized for a national bank as incidental to the business of banking if it is convenient or useful to an activity that is specifically authorized for national banks or to an activity that is otherwise part of the business of banking. In determining whether an activity is convenient or useful to such activities, the OCC considers the following factors:

(i) Whether the activity facilitates the production or delivery of a bank's products or services, enhances the bank's ability to sell or market its products or services, or improves the effectiveness or efficiency of the bank's operations, in light of risks presented, innovations, strategies, techniques and new technologies for producing and delivering financial products and services; and

(ii) Whether the activity enables the bank to use capacity acquired for its banking operations or otherwise avoid economic loss or waste.

(2) The weight accorded each factor set out in paragraph (d)(1) of this section depends on the facts and circumstances of each case.

§ 7.5002 Furnishing of products and services by electronic means and facilities.

(a) *Use of electronic means and facilities.* A national bank may perform, provide, or deliver through electronic

means and facilities any activity, function, product, or service that it is otherwise authorized to perform, provide, or deliver, subject to § 7.5001(b) and applicable OCC guidance. The following list provides examples of permissible activities under this authority. This list is illustrative and not exclusive; the OCC may determine that other activities are permissible pursuant to this authority.

(1) Acting as an electronic finder by:

(i) Establishing, registering, and hosting commercially enabled web sites in the name of sellers;

(ii) Establishing hyperlinks between the bank's site and a third-party site, including acting as a ''virtual mall'' by providing a collection of links to web sites of third-party vendors, organized by-product type and made available to bank customers;

(iii) Hosting an electronic marketplace on the bank's Internet web site by providing links to the web sites of third-party buyers or sellers through the use of hypertext or other similar means;

(iv) Hosting on the bank's servers the Internet web site of:

(A) A buyer or seller that provides information concerning the hosted party and the products or services offered or sought and allows the submission of interest, bids, offers, orders and confirmations relating to such products or services; or

(B) A governmental entity that provides information concerning the services or benefits made available by the governmental entity, assists persons in completing applications to receive such services or benefits and permits persons to transmit their applications for such services or benefits;

(v) Operating an Internet web site that permits numerous buyers and sellers to exchange information concerning the products and services that they are willing to purchase or sell, locate potential counter-parties for transactions, aggregate orders for goods or services with those made by other parties, and enter into transactions between themselves;

(vi) Operating a telephone call center that provides permissible finder services; and

(vii) Providing electronic communications services relating to all aspects of transactions between buyers and sellers;

(2) Providing electronic bill presentment services;

(3) Offering electronic stored value systems; and

(4) Safekeeping for personal information or valuable confidential trade or business information, such as encryption keys.

(b) *Applicability of guidance and requirements not affected.* When a national bank performs, provides, or delivers through electronic means and facilities an activity, function, product, or service that it is otherwise authorized to perform, provide, or deliver, the electronic activity is not exempt from the regulatory requirements and supervisory guidance that the OCC would apply if the activity were conducted by non-electronic means or facilities.

(c) *State laws.* As a general rule, and except as provided by Federal law, State law is not applicable to a national bank's conduct of an authorized activity through electronic means or facilities if the State law, as applied to the activity, would be preempted pursuant to traditional principles of Federal preemption derived from the Supremacy Clause of the U.S. Constitution and applicable judicial precedent. Accordingly, State laws that stand as an obstacle to the ability of national banks to exercise uniformly their Federally authorized powers through electronic means or facilities, are not applicable to national banks.

§ 7.5003 Composite authority to engage in electronic activities.

Unless otherwise prohibited by Federal law, a national bank may engage in an electronic activity that is comprised of several component activities if each of the component activities is itself part of or incidental to the business of banking or is otherwise permissible under Federal law.

§ 7.5004 Sale of excess electronic capacity and by-products.

(a) A national bank may, in order to optimize the use of the bank's resources or avoid economic loss or waste, market and sell to third parties electronic capacities legitimately acquired or developed by the bank for its banking business.

(b) With respect to acquired equipment or facilities, legitimate excess electronic capacity that may be sold to others can arise in a variety of situations, including the following:

(1) Due to the characteristics of the desired equipment or facilities available in the market, the capacity of the most practical optimal equipment or facilities available to meet the bank's requirements exceeds its present needs;

(2) The acquisition and retention of additional capacity, beyond present needs, reasonably may be necessary for planned future expansion or to meet the expected future banking needs during the useful life of the equipment;

(3) Requirements for capacity fluctuate because a bank engages in batch processing of banking transactions or because a bank must have capacity to meet peak period demand with the result that the bank has periods when its capacity is underutilized; and

(4) After the initial acquisition of capacity thought to be fully needed for banking operations, the bank experiences either a decline in level of the banking operations or an increase in the efficiency of the banking operations using that capacity.

(c) Types of electronic capacity in equipment or facilities that banks may have legitimately acquired and that may be sold to third parties if excess to the bank's needs for banking purposes include:

(1) Data processing services;

(2) Production and distribution of non-financial software;

(3) Providing periodic back-up call answering services;

(4) Providing full Internet access;

(5) Providing electronic security system support services;

(6) Providing long line communications services; and

(7) Electronic imaging and storage.

(d) A national bank may sell to third parties electronic by-products legitimately acquired or developed by the bank for its banking business. Examples of electronic by-products that banks may have legitimately acquired that may be sold to third parties if excess to the bank's needs include:

(1) Software acquired (not merely licensed) or developed by the bank for banking purposes or to support its banking business; and

(2) Electronic databases, records, or media (such as electronic images) developed by the bank for or during the performance of its permissible data processing activities.

§ 7.5005 National bank acting as digital certification authority.

(a) It is part of the business of banking under 12 U.S.C. 24(Seventh) for a national bank to act as a certificate authority and to issue digital certificates verifying the identity of persons associated with a particular public/private key pair. As part of this service, the bank may also maintain a listing or repository of public keys.

(b) A national bank may issue digital certificates verifying attributes in addition to identity of persons associated with a particular public/private key pair where the attribute is one for which verification is part of or incidental to the business of banking. For example, national banks may issue digital certificates verifying certain

financial attributes of a customer as of the current or a previous date, such as account balance as of a particular date, lines of credit as of a particular date, past financial performance of the customer, and verification of customer relationship with the bank as of a particular date.

(c) When a national bank issues a digital certificate relating to financial capacity under this section, the bank shall include in that certificate an express disclaimer stating that the bank does not thereby promise or represent that funds will be available or will be advanced for any particular transaction.

§ 7.5006 Data processing.

(a) *Eligible activities.* It is part of the business of banking under 12 U.S.C. 24(Seventh) for a national bank to provide data processing, and data transmission services, facilities (including equipment, technology, and personnel), data bases, advice and access to such services, facilities, data bases and advice, for itself and for others, where the data is banking, financial, or economic data, and other types of data if the derivative or resultant product is banking, financial, or economic data. For this purpose, economic data includes anything of value in banking and financial decisions.

(b) *Other data.* A national bank also may perform the activities described in paragraph (a) of this section for itself and others with respect to additional types of data to the extent convenient or useful to provide the data processing services described in paragraph (a), including where reasonably necessary to conduct those activities on a competitive basis. The total revenue attributable to the bank's data processing activities under this section must be derived predominantly from processing the activities described in paragraph (a) of this section.

§ 7.5007 Correspondent services.

It is part of the business of banking for a national bank to offer as a correspondent service to any of its affiliates or to other financial institutions any service it may perform for itself. The following list provides examples of electronic activities that banks may offer correspondents under this authority. This list is illustrative and not exclusive; the OCC may determine that other activities are permissible pursuant to this authority.

(a) The provision of computer networking packages and related hardware;

(b) Data processing services;

(c) The sale of software that performs data processing functions;

(d) The development, operation, management, and marketing of products and processing services for transactions conducted at electronic terminal devices;

(e) Item processing services and related software;

(f) Document control and record keeping through the use of electronic imaging technology;

(g) The provision of Internet merchant hosting services for resale to merchant customers; (h) The provision of communication support services through electronic means; and

(i) Digital certification authority services.

§ 7.5008 Location of a national bank conducting electronic activities.

A national bank shall not be considered located in a State solely because it physically maintains technology, such as a server or automated loan center, in that state, or because the bank's products or services are accessed through electronic means by customers located in the state.

§ 7.5009 Location under 12 U.S.C. 85 of national banks operating exclusively through the Internet.

For purposes of 12 U.S.C. 85, the main office of a national bank that operates exclusively through the Internet is the office identified by the bank under 12 U.S.C. 22(Second) or as relocated under 12 U.S.C. 30 or other appropriate authority.

§ 7.5010 Shared electronic space.

National banks that share electronic space, including a co-branded web site, with a bank subsidiary, affiliate, or another third-party must take reasonable steps to clearly, conspicuously, and understandably distinguish between products and services offered by the bank and those offered by the bank's subsidiary, affiliate, or the third-party.

Dated: May 8, 2002.

John D. Hawke, Jr.,

Comptroller of the Currency.

[FR Doc. 02–12333 Filed 5–16–02; 8:45 am]

BILLING CODE 4810–33–P

Simple. Convenient. Secure.

The Access 360° Reloadable Prepaid Card means fast access to your cash, how and where you want – whether in stores or online – and $0 fee to open[1], $0 fee to load, and a low monthly fee.

Overview | Key Benefits | Get Started | Fee Information | FAQs

Access 360° Reloadable Prepaid Card Frequently Asked Questions

Click on the question to view the answer.

Expand All | Collapse All

About Access 360°

What is Access 360°?

Access 360° is a reloadable prepaid card that turns your cash into convenience. It gives you the ultimate control of your money. From the ability to add money at any time without incurring a "load fee" to the ability to use it virtually anywhere that MasterCard is accepted, you'll enjoy purchasing convenience and an easy way to budget.

How does an Access 360° card work?

- Get it. Open an Access 360° card at any Fifth Third Banking Center. There is no credit check required and no fee to open[6] (must deposit a minimum of $25 to open the account).
- Load it. Add money for free at any Fifth Third Banking Center, transfer money from any eligible Fifth Third account, or set up direct deposit of paychecks, government benefits, or tax refunds.
- Use it. Shop anywhere Debit MasterCard is accepted in stores or online. Plus, you can withdraw cash from thousands of Fifth Third ATMs free of charge.

How is the Access 360° card different from a debit card?

Access 360° is not connected to a checking or savings account, so you will never incur any overdraft fees.

Is the Access 360° card a credit card?

No. The Access 360° card is a prepaid card that you can load with money to spend virtually anywhere that Debit MasterCard is accepted. It is not attached to a line of credit, so you can only spend what is on the card.

EXHIBIT
K-26

How does the Access 360° card differ from a gift card?

The Access 360° is a reloadable prepaid card so you can add funds to your card as frequently as you'd like. Also, unlike most gift cards, you can receive cash from your card at ATMs.

Getting Started

How do I open an Access 360° card?

Stop in to any Fifth Third Banking Center to open up your Access 360° card. There are no fees or credit checks to open your account. A $25 minimum deposit is required. You will receive a temporary card that will allow you to instantly begin using the money on your card. A permanent card with your name on it will be mailed within 3-5 days after opening the account[6].

What are the monthly fees on an Access 360° card?

The fee is waived if you are a Fifth Third checking customer[7] or in any monthly period that $500 or more is deposited onto the card. Otherwise, a $4 monthly fee applies. Please note that if you are a joint owner of an Access 360° account and are also a Fifth Third checking customer, the other cardholder on your Access 360° account will be aware that you have a checking account with Fifth Third since a lower monthly fee will be charged.

How do I activate my Access 360° card?

After you open your account, you will be given a temporary card that you can use immediately until your personalized card comes in the mail. To activate your temporary card, please call 1-866-452-8484 and follow the prompts. You will select a PIN when activating your temporary card. Once you receive your personalized card in the mail, call 866-452-8484 and follow the prompts to activate it. Be sure to use the same PIN that you selected when activating your temporary card. Your temporary card will automatically be deactivated upon activation of your personalized card.

How do I set up my PIN?

You will select a PIN when activating your temporary card. To activate your temporary card, please call 1-866-452-8484 and follow the prompts. Once you receive your personalized card in the mail, call 1-866-452-8484 and follow the prompts to activate it. Be sure to enter the same PIN that you selected when activating your temporary card.

Do I need to activate both my temporary card and personalized Access 360° card?

Yes. You must call 1-866-452-8484 to activate your temporary card after you open your account and then again to activate your permanent personalized Access 360° card upon receipt in the mail.

What is the difference between the temporary card and the permanent card? Will I be unable to access my funds the same with the temporary card?

Although the temporary card and permanent card look different, they work the same. There is no difference in access or limits. The temporary card is a fully functional card and can be used immediately upon activation. The personalized card is embossed with your name as the cardholder and should be activated and used upon receipt.

Can I open a joint account with someone else?

Yes, single and joint accounts can be opened[7]. Please note that if you are a joint owner of an Access 360° account and are also a Fifth Third checking customer, the other cardholder on your Access 360° account will be aware that you have a checking account with Fifth Third since a lower monthly fee will be charged. At opening, all new account holders will receive a temporary card. A personalized card will be mailed to each account owner.

How old do I have to be to open an Access 360° account?

You must be at least 18 years of age to be a sole account owner. If you are at least 16 years of age, you can be a joint owner on an account with your parent or legal guardian.

Loading and Reloading your Access 360° Card

How can I load money onto my Access 360° card?

You can load money onto your card for a $0 fee in any one of these three convenient ways:

- Visit any Fifth Third Banking Center and deposit cash onto your card
- Transfer funds from an eligible Fifth Third account
  - Online with Fifth Third's Internet Banking[5]
  - Via the Fifth Third Mobile Banking App[2]
  - At most Fifth Third ATMs

  - Visit any Fifth Third Banking Center
- Direct deposit your paycheck, government benefits, and even tax refunds

Can I deposit a check onto my Access 360° card?

No. You cannot deposit a check directly onto your Access 360° card. You can cash a check at any Fifth Third Financial Center and then deposit the cashed funds directly onto the card.

How do I set up Direct Deposit?

You will receive two pre-printed Direct Deposit forms, one when you first open your account in the financial center and another when your permanent card is mailed to you. The deposit form will contain the routing number and unique account number tied to your card. Simply sign and give either form to your employer and you're all set! (Please note that some employers have their own Direct Deposit form, so be sure to check with your employer).

Is my card number the account number to be used for Direct Deposit?

No. Your 16 digit card number is not the account number you need to set up Direct Deposit. Your Direct Deposit account number will be on the pre-printed Direct Deposit forms that you receive when you open your card and again when you receive your permanent card. You can also obtain your Direct Deposit account number at any Fifth Third financial center.

What should I do if I lose my pre-printed Direct Deposit form?

If you lose or need another copy of your Direct Deposit form, simply walk into any Fifth Third Branch and ask to have it reprinted.

Getting Cash from Your Access 360° Card

How can I use my Access 360° card to get cash? Can I get cash for a $0 fee?

You can get cash for a $0 fee in any of the following ways:

1. Withdraw cash from any Fifth Third ATM
2. Withdraw cash at any Fifth Third Banking Center
3. Choose the cash back option during a PIN transaction at any merchant that supports cash back. Just press debit on the keypad and enter the PIN that you selected when activating your card. Follow the prompts to select the amount of cash you would like.

Can I use my Access 360° card to get cash at an ATM?

Yes, you can withdraw cash from any Fifth Third ATM or non-Fifth Third ATM. To get cash from an ATM, customers should select 'Checking' as the 'from' account.

Note: There is no fee to withdraw cash from any Fifth Third ATM. There is a $2 fee for ATM transactions at non-Fifth Third ATMs. You may also be charged a non-Fifth Third fee by the ATM owner.

What 'from' account should I select when withdrawing funds from an ATM?

To get cash from a Fifth Third ATM, a 'Prepaid' option will be presented.

To get cash from a non-Fifth Third ATM, you should select 'Checking' as the 'from' account.

Is there a fee for withdrawing cash from a non-Fifth Third ATM?

Yes, there is a $2 fee for ATM transactions at non-Fifth Third ATMs. You may also be charged a non-Fifth Third fee by the ATM owner.

Can I get cash back at the register when I make a purchase?

Yes, you can receive cash back when making a purchase if the merchant supports it. Just press debit on the keypad and enter the PIN that you selected when activating your card. Follow the prompts to select the amount of cash you would like.

Are there any limits on cash transactions?

You can withdraw up to $500 per day from an ATM. You may withdraw cash at any financial center for up to $2,500 per day.

Making Purchases Using Your Access 360° Card

Where can I make purchases using my Access 360° card?

You can make purchases wherever Debit MasterCard is accepted in stores and online. You can also use it to withdraw funds from thousands of Fifth Third ATMs at no charge.

How do I make purchases with my Access 360° card?

- Swipe your card
- Choose one:
  - Select debit. Enter your PIN that you selected when activating your card
  - Select credit. Sign the receipt.

Note: If you wish to get cash back when making a purchase, you must press debit on the keypad. Then, enter the PIN that you selected when activating your card. Follow the prompts to select the amount of cash you would like.

When making a purchase, should I select 'credit' or 'debit'?

You are free to choose either 'credit' or 'debit' when making purchases. If you choose credit, you will not need to enter your PIN, but you may need to sign the receipt. If you choose debit, you will need to enter your PIN.

Note: In order to get cash back with your purchase, you will need to choose debit.

Can I use my Access 360° card to pay bills?

Yes, you can use your Access 360° card number at biller sites where MasterCard payments are accepted.

Will my Access 360° card work when I travel internationally? Is there a cost or fee for using it internationally?

Yes, your Access 360° card can be used internationally anywhere Debit MasterCard is accepted. If the purchase is not completed in U.S. Dollars, it will be converted or exchanged to U.S. Dollars. A 3% exchange rate adjustment fee and a .20% currency conversion fee will be added to the converted amount.

Can I use my Access 360° card to purchase gas?

Yes, the Access 360° card can be used at a gas station to pay for gas. You cannot use your card to pay at the pump. You will need to go inside and give your card to the cashier in order to purchase gas.

Are there any limits on purchase transactions?

You may make purchases, including cash withdrawals made at branches, for up to $2,500 per day.

Managing Your Access 360° Card

How can I check the available balance on my card?

You can check your balance in the following ways:

1. Through a balance inquiry at a Fifth-Third ATM
2. By using the Fifth Third Mobile Banking App[2]
3. By logging onto Fifth Third's Internet Banking[5]
4. By calling 1-866-452-8484 and pressing the balance inquiry prompt
5. By setting up a mobile text alert[2]
6. By inquiry at a Fifth Third Financial Center
7. By texting BAL to 535353[2]

Will I get a statement that shows my card activity?

Yes, statement and transaction history can be viewed online in Fifth Third's Internet Banking. A printed statement is available upon request. You can also use Internet Banking to view the account balance and activity daily.

How do I set up mobile text alerts?

To enroll your mobile device[2], follow the instructions below:

- Login to Internet Banking[5]
- Go to Service Center
- Click the "Register your Phone" link
- Select: "Mobile Account Alerts" checkbox to enable text alerts
- Accept the disclosures.
- Enter your cell phone number and select your carrier.

- Enter the PIN number sent to your phone.
- Once your phone is registered simply select the alerts you would like to receive.

Once your mobile device is enrolled, you can text BAL to 535353 at any time to check your current balance[2].

Security

What should I do if my Access 360° card is lost or stolen? Am I protected against any unauthorized charges?

Call Customer Service at 1-866-452-8484 immediately to report your card as lost or stolen. The card will immediately be deactivated and a new one will be sent to you within 3-5 business days. Your Access 360° card comes with MasterCard Zero Liability Protection[4]. This means that you will have no liability for "unauthorized purchases" made using your Access 360° card. See the MasterCard Zero Liability Policy in the Access 360° Card Terms and Conditions for complete details.

Are the funds on my Access 360° card FDIC insured?

Yes, funds credited to your account are covered by FDIC insurance up to the base coverage amount of $250,000 per depositor for combined deposits at Fifth Third Bank.

Always Know Your Card's Balance.

With just a quick text[2], you can check the current balance on your Access 360° Card. Register your phone for text banking today!

Learn More

Protect Yourself from ID Theft

Help us in safeguarding your accounts and your identity.

View Details

Disclosures

*A $2 service fee applies for non-Fifth Third ATM transactions. Other ATM network owners may also assess a usage fee.

MasterCard is a registered trademark of MasterCard International Incorporated.

Access 360° is a registered trademark of Fifth Third Bancorp. Cash Version 2.0. is a service mark of Fifth Third Bancorp.

Access 360° Terms and Conditions

Copyright © 2015 Fifth Third Bank, All Rights Reserved.

Member FDIC, Equal Housing Lender

Simple. Convenient. Secure.

The Access 360° Reloadable Prepaid Card means fast access to your cash, how and where you want – whether in stores or online – and $0 fee to open[1], $0 fee to load, and a low monthly fee.

Overview | Key Benefits | Get Started | Fee Information | FAQs

Get it.

It couldn't be easier to make quick, secure access to your cash possible.

- COME IN. Visit your nearest Fifth Third Banking Center.
- No credit checks required.

Load it.

Easily add money – any time – for $0 fee.

Use it.

Shop anywhere Debit MasterCard® is accepted – online, on the phone, on vacation.

Love it.

Enjoy extended warranties and protection from unauthorized purchases if your card is ever lost or stolen[3,4]. Plus, check your balance any time, anywhere, when it's convenient for you[2].

Always Know Your Card's Balance.

With just a quick text[2], you can check the current balance on your Access 360° Card. Register your phone for text banking today!

Protect Yourself from ID Theft

Help us in safeguarding your accounts and your identity.

View Details

EXHIBIT
K-27

Learn More

Disclosures

*A $2 service fee applies for non-Fifth Third ATM transactions. Other ATM network owners may also assess a usage fee.

MasterCard is a registered trademark of MasterCard International Incorporated.

Access 360° is a registered trademark of Fifth Third Bancorp. Cash Version 2.0. is a service mark of Fifth Third Bancorp.

Access 360° Terms and Conditions

Copyright © 2015 Fifth Third Bank, All Rights Reserved.

Wells Fargo Launches Simplified Person-to-Person Money Transfer Service Nationwide

You no longer need an account number to pay someone electronically: a mobile phone number or email address enables Wells Fargo customers to make payments leveraging clearXchange℠

SAN FRANCISCO - May 24, 2012

Wells Fargo & Company (NYSE:WFC) today announced the launch of Send & Receive Money, a new service that simplifies Wells Fargo customers' payments to other Wells Fargo and Bank of America customers through online and mobile banking using an email address or mobile phone number. Wells Fargo customers no longer need to know their recipient's account number at Wells Fargo or Bank of America. Wells Fargo is the first bank to roll out nationally the *clearXchange* service for person-to-person-payments.

"Customers want options and convenience," said Brett Pitts, senior vice president at Wells Fargo's Internet Services Group. "With Send & Receive Money customers can send payments electronically to others without having to know their sensitive financial information, such as bank account numbers. As mobile money transfer becomes more common, remembering multiple account numbers will be harder. Send & Receive Money allows customers to pay another person using information they typically either know or have programmed on their phone."

Customers can use their recipient's mobile phone number or email address to initiate a person-to-person payment via *clearXchange*, which was formed to facilitate the movement of funds between bank customers to better meet their needs. Wells Fargo is an owner of *clearXchange*.

"This is a great step in the vision we have for *clearXchange*," said Mike Kennedy, executive vice president and head of Innovation and Payments Strategy at Wells Fargo and board chairman of *clearXchange*. "The ability to easily move money between family and friends across financial institutions is something asked for by our customers. We are happy to now provide the service."

Over time, Wells Fargo's Send & Receive Money service will be expanded, and Wells Fargo customers will be able to send money to and receive money from customers at banks other than Bank of America.

Wells Fargo customers have been able to use an account number to make transfers to each other online since 2003. The service was extended through the mobile banking URL wf.com in 2007, made available on new mobile banking applications for the iPhone and iPod touch in 2009, and on new applications for Android, BlackBerry and Palm in 2010.

All Send & Receive Money transactions are covered by Wells Fargo's Online Security Guarantee. Learn more about how Wells Fargo's Online Security Guarantee works at https://www.wellsfargo.com/privacy_security/online/guarantee. Mobile Banking is also covered by the Online Security Guarantee.

The service is available to all Wells Fargo customers with a checking or savings account and online banking. Customers can sign up for Send & Receive Money during an online banking session or via Wells Fargo's mobile apps or at wf.com. Transfers take up to one business day between Wells Fargo customers and up to three business days between customers of different financial institutions. The service currently has no fee.

Watch the educational video "Send & Receive Money – payments on the go" on Wells Fargo's YouTube channel at http://www.youtube.com/watch?v=1yc1XC98mbc. For more information about online banking, visit https://www.wellsfargo.com/wfonline, or to learn more about Wells Fargo's mobile banking features visit https://www.wellsfargo.com/mobile.

About Wells Fargo Online, Mobile and Text Banking
Wells Fargo is a leading provider of online and mobile financial services for individual consumers, small and middle market businesses, and large corporations with a full range of banking, money movement, investing, asset management, and other financial and risk management products. Wells Fargo was recognized by *Bank Technology News* on "The Innovators" list for its online banking services (May 2012). Keynote's Mobile Banking Scorecard named Wells Fargo winner in two categories: Privacy & Security and Quality & Availability (2012). Wells Fargo was named a 2011 Compuware Best of the Web award winner. Wells Fargo was honored as the 2011 Gold award winner for the Check Account Details Transaction category in Retail Banking, which benchmarks three key Web performance metrics – Response Time, Availability and Consistency (2011).

About Wells Fargo
Wells Fargo & Company (NYSE: WFC) is a nationwide, diversified, community-based financial services company with $1.3 trillion in assets. Founded in 1852 and headquartered in San Francisco, Wells Fargo provides banking, insurance, investments, mortgage, and consumer and commercial finance through more than 9,000 stores, 12,000 ATMs, the Internet (wellsfargo.com), and other distribution channels across North America and internationally. With more than 270,000 team members, Wells Fargo serves one in three households in America. Wells Fargo & Company was ranked No. 23 on *Fortune's* 2011 rankings of America's largest corporations. Wells Fargo's vision is to satisfy all our customers' financial needs and help them succeed financially.

Media
Andrea Mahoney
415-222-4722

Investors
Jim Rowe
415-396-8216

EXHIBIT
K-28

Related topics: News Releases

© 1999 - 2015 Wells Fargo. All rights reserved. NMLSR ID 399801

');
Personal </bbtdotcom/start.page> > Banking </bbtdotcom/banking/default.page> > Cards </bbtdotcom/banking/cards/default.page> > Prepaid Debit Card

Questions? Start Chat

Prepaid Debit Card

Enjoy the unrivaled purchasing power of Visa® with a prepaid, reloadable BB&T MoneyAccount®. It's the smart way to manage and protect your money.

- Apply in minutes—no separate bank account or minimum credit score is required
- Spend only the money available in your account
- Make purchases, pay bills online and more
- Use direct deposit to avoid check-cashing fees

Benefits

The BB&T MoneyAccount combines the features of a checking account with the convenience of a prepaid, reloadable, Visa debit card.

- Enjoy hassle-free spending around town, while traveling or shopping online
- Add security to your online purchases by linking your card to Visa Checkout </sites/bbtdotcom/sp/visacheckout/1407/default.jsp?intcmp=3275>
- Establish financial responsibility—since you can only spend available funds, you'll never overdraw your account
- Learn or sharpen budgeting skills
- Share joint accounts with your spouse, child, relative or friend

Adding Funds

It's easy to add money to your BB&T MoneyAccount:

- Deposit cash, BB&T checks or government–issued checks at any BB&T financial center </bbtdotcom/locator/search.page> location
- Enroll in Direct Deposit </bbtdotcom/banking/checking/direct-deposit.page> to automatically deposit your paycheck, tax refund or US government benefits
- Transfer funds to and from other BB&T accounts
- Load funds where you shop. Use the Visa ReadyLink <http://usa.visa.com/locators/readylink-locations.jsp > reload network at any participating merchant location <http://usa.visa.com/locators/readylink-locations.jsp >

EXHIBIT
K-29

- Use the Ingo Money app to load approved checks directly into your MoneyAccount by taking a photo with your iPhone® or Android™ mobile device. You can download the free app from Google® play or the Apple App Store.

Managing Your Account

Bank on your terms—anytime, anywhere, with BB&T online banking—our FREE Internet banking service. It's safe, easy and convenient.

With BB&T online banking, you get access to:

- Online Bill Payment </bbtdotcom/online-services/online-banking/online-bill-payment.page>—schedule free, secure payments when they're most convenient for you
- BB&T Mobile </bbtdotcom/online-services/mobile-banking/default.page>—perform banking transactions right from your mobile phone[1]
- Alerts </bbtdotcom/online-services/online-banking/alerts.page>—receive account-related email or text messages on your mobile device[1]

Pricing

BB&T MoneyAccount fees are straightforward and affordable and, because your account is prepaid, you never have to worry about overdraft fees.

Standard monthly maintenance fee:

- $5 per month (BB&T will reduce this fee to $3 for any month in which you have total deposits/loads of at least $1,000.)

ATM withdrawal fees:

- Free cash withdrawals at any BB&T ATM
- $2.50 at ATMs outside of the BB&T network[2]
- $5.00 at international ATMs[2]

Each month, you'll receive free online statements and a single paper statement at no charge. A fee of $3 applies to additional paper statements.

View the complete list of fees and free services </bbtdotcom/banking/cards/prepaid-debit-card-pricing.page>.

FAQ

Here are the answers to some frequently asked questions about the BB&T MoneyAccount.

GENERAL INFORMATION

What are the advantages of a BB&T MoneyAccount?

Your BB&T MoneyAccount card can be used just like any Visa debit card, and is accepted at millions of places worldwide, online or by phone. You can easily get cash or add money to your account, and enjoy 100% Visa fraud protection with FDIC insurance BB&T Online® Banking </bbtdotcom/online-services/online-banking/bbt-online.page> account access anytime, anywhere you have an Internet connection.

Who should get the BB&T MoneyAccount?

The BB&T MoneyAccount is ideal if you want the spending power of a Visa debit card but don't want to pay a lot in fees or risk overdrawing your account:

- **Budget-minded clients** can enjoy the convenience and safety a Visa debit card provides while limiting spending to only the money they have available.
- **Students and young adults** can use MoneyAccount to establish financial responsibility.
- **New customers** with no prior banking relationships can be approved for MoneyAccount—no minimum credit score required.

Can I get a BB&T MoneyAccount card for another family member?

BB&T MoneyAccount cards are issued only to the person submitting the application.

Can I get a joint BB&T MoneyAccount?

Yes. You may apply with your spouse, child or anyone else that you would like to have as a co-applicant.

Can I get more than one card for my BB&T MoneyAccount?

One card is issued for an individually owned BB&T MoneyAccount, and up to two cards can be issued for a joint account. Lost or stolen cards can be replaced for a nominal fee.

GETTING STARTED

How do I sign up for a BB&T MoneyAccount?

Our BB&T MoneyAccount application process is quick and easy, and you'll get an online decision in minutes. Before you begin, gather the Social Security number, driver's license information, date of birth and current home address of any applicants, then apply online <https://www.bbt.com/pma/>.

Will you pull my credit report?

Yes. We'll review your credit report to help us prevent fraud and identity theft. However, your credit score or lack of credit history will not prevent you from opening a BB&T MoneyAccount.

Do I need to have a checking account?

No, neither a checking account nor a previous relationship with BB&T (or any other financial institution) is required.

How do I set up direct deposit?

After you apply <https://www.bbt.com/pma/> for the BB&T MoneyAccount, print out the Direct Deposit form. (We'll even pre-fill most of the form for you.) Then, complete, sign, and deliver it to your company/employer's payroll department.

You'll need Adobe Acrobat Reader to view and print your Direct Deposit form. If you don't currently have Acrobat Reader installed, you may download <http://www.adobe.com/products/acrobat/readstep2.html> it for free at your convenience.

Can I have my government benefits deposited to the account?

Yes, your Social Security, SSI, VA Compensation and Pension or other federal benefit payments can be deposited directly into your BB&T MoneyAccount. Once your MoneyAccount has been opened, visit Go Direct® <http://www.godirect.org/> to have your federal benefits deposited directly.

How can I find a BB&T Financial Center?

Our online locator </bbtdotcom/locator/search.page> allows you to quickly find your nearest BB&T financial center.

LOADING FUNDS

What is a "prepaid" card? Is that different from a "reloadable" card?

A prepaid debit card allows you to spend only the amount of money in your account. Certain prepaid cards, such as gift cards, cannot be used after the prepaid money has been spent. A reloadable card, such as the BB&T MoneyAccount card, is a debit card that allows you to spend only the amount of money in your account but also add (reload) money whenever you need to, so that you can continue using the same card.

How can I add money to my BB&T MoneyAccount?

Adding money to your BB&T MoneyAccount is easy. You can set up direct deposit, add funds at any BB&T financial center </bbtdotcom/locator/search.page>, transfer money from other BB&T accounts, use the Ingo Money app to load approved checks using your mobile device, or visit any merchant participating in the Visa ReadyLink reload network.

What is Visa ReadyLink? How can I find a Visa ReadyLink location?

Visa ReadyLink offers a fast and easy way to load money into your BB&T MoneyAccount account. Visit Visa ReadyLink <http://usa.visa.com/locators/readylink-locations.jsp> to find the nearest of more than 50,000 locations.

USING YOUR BB&T MONEYACCOUNT CARD

Where can I use my BB&T MoneyAccount card?

Your MoneyAccount card can be used wherever Visa debit cards are accepted. You can make purchases or payments in stores, online or by phone.

Can I use the account to pay bills?

Yes, you can use the BB&T MoneyAccount to pay bills in person, over the phone or with BB&T online bill payment </bbtdotcom/online-services/online-banking/online-bill-payment.page>.

Can I use the card to shop online?

Yes, your BB&T MoneyAccount card can be used for online purchases, wherever Visa debit cards are accepted.

Can I withdraw funds from any ATM?

You can withdraw funds from any ATM that displays the Visa or Plus logo. If you use one of 2,400 ATMs within the BB&T network </bbtdotcom/locator/search.page>, there are no transaction or service fees.

If you would like to withdraw funds from an ATM outside of the BB&T network </bbtdotcom/locator/search.page>, you may incur fees. Please note that these fees may be listed in your account statements as "foreign ATM fees."

Can I get cash back from my BB&T MoneyAccount?

Yes, you can get cash back at participating merchant locations, such as grocery stores and drug stores.

What should I know about transactions made at gas stations, hotels, restaurants and car-rental agencies?

Transactions where the final purchase amount is not known at the time you present your card are processed differently than most other purchases. These special transactions may be handled differently by different merchants. If you are unsure of a merchant's policy, it's best to ask before presenting your card.

- Gas stations will accept the BB&T MoneyAccount card to prepay for fuel inside the station, but "pay at the pump" transactions are not allowed.
- Restaurants, Hotels, Car rental agencies may authorize more than final purchase amount.

CHECKING YOUR BALANCE

What's the best way to monitor my BB&T MoneyAccount?

Sign up for online banking </bbtdotcom/online-services/online-banking/bbt-online.page>, our free, easy-to-use online banking service. You can also get balance information by calling **877-762-9931.**

What are account alerts?

BB&T alerts </bbtdotcom/online-services/online-banking/alerts.page> are messages from BB&T that you can get by email or through your mobile device. You can set up alerts to keep tabs on your account or to notify you when important account activities occur.[1]

What is BB&T online banking?

BB&T online banking </bbtdotcom/online-services/online-banking/bbt-online.page> is a safe and convenient Internet banking service. You can bank online from anywhere you have Internet access, including your mobile phone. Use online banking to check balances, transfer funds, pay bills and set up alerts.[1]

What is mobile banking?

BB&T Mobile </bbtdotcom/online-services/mobile-banking/default.page> is a way for you to bank anytime, anywhere, from your mobile device. BB&T offers three convenient mobile banking options: Mobile App </bbtdotcom/online-services/mobile-banking/mobile-app.page>, Mobile Web </bbtdotcom/online-services/mobile-banking/mobile-web.page> and Mobile Text </bbtdotcom/online-services/mobile-banking/mobile-text.page>.[1]

Can I accidentally spend more than the balance on my card?

No. The BB&T MoneyAccount has been designed to allow you to spend only the amount of money you've deposited.

Can my card ever have a negative balance?

It's possible that a Visa merchant may put an item through without prior authorization. For example, a restaurant may automatically add an 18% gratuity to your bill's total, and BB&T would be obligated to pay for such an item. If the amount of the transaction exceeds the amount in your account, this may result in a negative balance.

In the unlikely event of such a situation, the amount of the negative balance will automatically be deducted from the next deposit that is made to your BB&T MoneyAccount, and you would not be charged an overdraft fee.

SECURITY

What if my BB&T MoneyAccount card is lost or stolen?

If your MoneyAccount card gets lost or stolen—or if the account number is misused by someone else—you will be reimbursed for 100 percent of any unauthorized transactions.

Your BB&T MoneyAccount card comes with 24-hour support. If your card is lost or stolen, call **877-762-9931** immediately.

Are the funds in my account FDIC insured?

Yes. All BB&T MoneyAccount funds are FDIC insured. Learn more </assets/docs/html/bbt-com/2011/fdic-limit-increase/default.html> about FDIC Insurance coverage and limits.

PRICING

Is it possible to incur overdraft fees with this account?

No. The BB&T MoneyAccount has been designed so that you'll never incur overdraft fees.

Are there any fees associated with the BB&T MoneyAccount?

Yes, there is a standard monthly maintenance fee of $5 ($3 if you load $1,000 during a month). Additional fees, such as those for ATM withdrawals outside of the BB&T network, may apply depending on your activity. See your Fee Schedule </assets/docs/pdf/bbt-com/banking/cards/standard-pricing.pdf> for full details.

What is a foreign ATM fee?

A foreign ATM fee (also known as a foreign transaction fee) is a fee charged to a cardholder for using an ATM outside of a bank's network. You can avoid this fee by using one of the more than 2,400 BB&T ATMs </bbtdotcom/locator/search.page> located across 12 states and Washington, DC.

© 2015, Branch Banking and Trust Company. All Rights Reserved.

BBVA Compass

Contact Us Locations Security Center Privacy En Español

Personal Banking | Small Business Banking | Commercial Banking | Global Wealth | About BBVA Compass | Customer Service | Search

Personal Banking ▶ Checking Accounts ▶ Safespend Prepaid Visa Card

SafeSpend: Visa® Prepaid Card

A smart, simple, safe solution to manage your money.

Forget the worry of bounced checks and overdraft fees – the SafeSpend Card helps you manage your money responsibly and affordably.

Benefits

How it works

Funding

Direct Deposit

Limits/Fees

The BBVA Compass SafeSpend Card is a reloadable Prepaid Visa Debit card. Gain control of your money by converting cash to your card today, and take advantage of the convenience and safety of Prepaid Visa Debit.

No Overdraft Fees

Get funds more quickly with Direct Deposit

Great for College Students

Avoid Check Cashing Lines/Fees

The BBVA Compass SafeSpend Card also includes:

FREE Online Banking
FREE email or text* balance alerts
Zero Liability** if card is lost or stolen
FDIC Insured

*BBVA Compass does not charge for text message alerts, however message and data rates may apply. Please check with your wireless carrier about such fees.

**Visa® Zero Liability covers U.S.-issued cards only and does not apply to ATM transactions, PIN transactions not processed by Visa, or certain commercial card transactions. Cardholder must notify BBVA Compass promptly of any unauthorized use. Consult BBVA Compass for additional details or visit visa.com/security. See your Visa Cardholder Agreement for further details.

1. **Sign up for your Card online** with our instant approval process

Get Started

I have a BBVA Compass Check Card
Apply Online Now

All Others
Apply Online Now

SafeSpend Demo

Visa® Acceptance

Use everywhere Visa is accepted online, over-the-phone, and at many ATM's.

SafeSpend Card

FAQs

ReadyLink Reload Locations

EXHIBIT
K-30

No Credit Check

No Issuance Fees

2. **Activate your SafeSpend Card** and add funds – there's just a $4 fee for the initial loading of funds.

   Get instant access to your paycheck, download Direct Deposit Form

   Transfer funds from your BBVA Compass debit card to your SafeSpend Card

   Add cash at participating Visa ReadyLink retail merchant locations – find a ReadyLink location near you

3. **Use your card anywhere Visa is accepted**

   Transact worry free with no risk of overdraft fees

Add Funds To Your Card

Multiple ways to reload (add funds) to your SafeSpend Card.

Direct Deposit: Gain access to your funds quicker by direct depositing all or part of your paycheck to your card. Direct Deposit payroll funds will be available on your Card as of the check's payment received date – and pay no reload fee.

Swipe your card at the register of any participating Visa ReadyLink retail merchant location. Find a ReadyLink location near you.

Online Card-to-Card Transfer (from BBVA Compass debit cards only): Add money online from your BBVA Compass debit card with no reload fee. A great tool to provide funds for your teen or college age student.

Manage Your Money Online

Know what's going on with your account is just a click away.

Stay on plan: Easily view purchases and detailed account summary online to remain aware of what you've spent and what you have left to spend. Alert yourself to low balances with email and text alerts* so you know when it's time to put money back on your card.

Manage your funds: order a second card to share with a student or spouse. Fund your student's Card and help them stay on track and avoid trouble by tracking their spending online.

*BBVA Compass does not charge for text message alerts, however message and data rates may apply. Please check with your wireless carrier about such fees.

Sign up for Direct Deposit and your pay check, social security, or other income can be deposited directly to your SafeSpend Card.

Features and Benefits

Convenient – Easier than cashing your check at a bank or check cashing location.

Fast – Immediate access to your money from the time of the deposit.

Safe – Checks can be lost, delayed or stolen. Direct Deposit helps protect you from these risks.

Automatic Payment – Your money is automatically deposited onto your SafeSpend Card.

How to Sign Up

To set up this service simply download and complete our Payroll Direct Deposit Form, or use the prefilled form provided with your SafeSpend Card shipment and take it to your employer's payroll or Human Resources Department. They can take care of the rest.

Note: If you receive Social Security or other government payroll payments, you may call the number listed at the bottom of the Payroll Direct Deposit form to set up direct deposit

Limits

SafeSpend Card Load (Funding) Limits		
	Ordered SafeSpend Card without BBVA Compass Debit Card	**Ordered SafeSpend Card with BBVA Compass Debit Card**
Maximum balance of funds on card	$3,000	$6,500
Maximum amount of all loads	$1,600 during any 15-day period	$3,500 during any 15-day period
Maximum number of loads	3 during any 7-day period	3 during any 7-day period
Maximum for Visa ReadyLink Loads	$500/load $500 during any 7-day period 3 loads during any 7-day period	$600/load $1,500 during any 7-day period 3 loads during any 7-day period
Maximum amount of any direct deposit	$1,600	$3,500
Maximum amount of any transfer from your BBVAC debit card	n/a	$2,500
Minimum load amount	$20	$20

SafeSpend Card Transaction Limits		
	Ordered SafeSpend Card without BBVA Compass Debit Card	**Ordered SafeSpend Card with BBVA Compass Debit Card**
Daily limit for transactions to obtain cash from a Visa ATM	$400/transaction	$600/transaction
	$400/day	$600/day
Daily limit for all other kinds of transactions, including purchases at Visa Merchants	$1,500/transaction	$1,500/transaction
	$1,500/day	$1,500/day
Daily limit for all transactions	$1,500/day	$1,500/day

Schedule of Fees

New Card	No Charge
Card Activation	No Charge
Initial Loading of Funds	$4
Monthly Maintenance	$4/month
Reloading of Funds	No Charge by BBVA Compass
Card Reissued after Expiration	No Charge
Replacement of Lost/Stolen Card	No Charge
Card for Authorized User	$4
Email/Text Message Alerts	No Charge by BBVA Compass*
Paper Statements	$4/month

Copy of Statement	$4/statement
Check for Funds	$15 (charged only if you terminate use of Card)
Balance Inquiry	
Domestic ATM	No Charge by BBVA Compass
Foreign ATM	$1
Withdrawal	
Domestic ATM	$1**
Foreign ATM	$3**
Foreign Transactions	
Withdrawal at Foreign ATM	1% of the U.S. dollar amount of the withdrawal
All other Foreign Transactions	3% of the U.S. dollar amount of the transaction

*Message and data rates may apply. Please check with your wireless carrier about such fees.

** BBVA Compass will not charge a fee for the first withdrawal from an ATM each month regardless of whether that withdrawal occurs at a domestic or foreign ATM.

SafeSpend Terms & Conditions

Links to third party sites are provided for your convenience. These sites are not within our control and may not have the same privacy, security or accessibility standards. Third parties are completely and solely responsible for the content and availability of their sites.

Like 89k Follow @bbvacompass 7,916 followers

banking built for you.

© 2015 BBVA Compass Bancshares, Inc. Compass Bank is a Member FDIC and an Equal Housing Lender. BBVA Compass is a trade name of Compass Bank, a member of the BBVA Group.

BBVA Compass

Contact Us Locations Security Center Privacy En Español

Personal Banking | Small Business Banking | Commercial Banking | Global Wealth | About BBVA Compass | Customer Service | Search

Personal Banking ▶ Checking Accounts ▶ Safespend Prepaid Visa Card

SafeSpend: Visa® Prepaid Card

A smart, simple, safe solution to manage your money.

Forget the worry of bounced checks and overdraft fees – the SafeSpend Card helps you manage your money responsibly and affordably.

Benefits

How it works

Funding

Direct Deposit

Limits/Fees

The BBVA Compass SafeSpend Card is a reloadable Prepaid Visa Debit card. Gain control of your money by converting cash to your card today, and take advantage of the convenience and safety of Prepaid Visa Debit.

No Overdraft Fees

Get funds more quickly with Direct Deposit

Great for College Students

Avoid Check Cashing Lines/Fees

The BBVA Compass SafeSpend Card also includes:

FREE Online Banking
FREE email or text* balance alerts
Zero Liability** if card is lost or stolen
FDIC Insured

*BBVA Compass does not charge for text message alerts, however message and data rates may apply. Please check with your wireless carrier about such fees.

**Visa® Zero Liability covers U.S.-issued cards only and does not apply to ATM transactions, PIN transactions not processed by Visa, or certain commercial card transactions. Cardholder must notify BBVA Compass promptly of any unauthorized use. Consult BBVA Compass for additional details or visit visa.com/security. See your Visa Cardholder Agreement for further details.

1. **Sign up for your Card online** with our instant approval process

Get Started

I have a BBVA Compass Check Card
Apply Online Now

All Others
Apply Online Now

SafeSpend Demo

Visa® Acceptance

Use everywhere Visa is accepted online, over-the-phone, and at many ATM's.

SafeSpend Card

FAQs

ReadyLink Reload Locations

EXHIBIT
K-31

No Credit Check

No Issuance Fees

2. **Activate your SafeSpend Card** and add funds – there's just a $4 fee for the initial loading of funds.

   Get instant access to your paycheck, download Direct Deposit Form

   Transfer funds from your BBVA Compass debit card to your SafeSpend Card

   Add cash at participating Visa ReadyLink retail merchant locations – find a ReadyLink location near you

3. **Use your card anywhere Visa is accepted**

   Transact worry free with no risk of overdraft fees

Add Funds To Your Card

Multiple ways to reload (add funds) to your SafeSpend Card.

Direct Deposit: Gain access to your funds quicker by direct depositing all or part of your paycheck to your card. Direct Deposit payroll funds will be available on your Card as of the check's payment received date – and pay no reload fee.

Swipe your card at the register of any participating Visa ReadyLink retail merchant location. Find a ReadyLink location near you.

Online Card-to-Card Transfer (from BBVA Compass debit cards only): Add money online from your BBVA Compass debit card with no reload fee. A great tool to provide funds for your teen or college age student.

Manage Your Money Online

Know what's going on with your account is just a click away.

Stay on plan: Easily view purchases and detailed account summary online to remain aware of what you've spent and what you have left to spend. Alert yourself to low balances with email and text alerts* so you know when it's time to put money back on your card.

Manage your funds: order a second card to share with a student or spouse. Fund your student's Card and help them stay on track and avoid trouble by tracking their spending online.

*BBVA Compass does not charge for text message alerts, however message and data rates may apply. Please check with your wireless carrier about such fees.

Sign up for Direct Deposit and your pay check, social security, or other income can be deposited directly to your SafeSpend Card.

Features and Benefits

Convenient – Easier than cashing your check at a bank or check cashing location.

Fast – Immediate access to your money from the time of the deposit.

Safe – Checks can be lost, delayed or stolen. Direct Deposit helps protect you from these risks.

Automatic Payment – Your money is automatically deposited onto your SafeSpend Card.

How to Sign Up

To set up this service simply download and complete our Payroll Direct Deposit Form, or use the prefilled form provided with your SafeSpend Card shipment and take it to your employer's payroll or Human Resources Department. They can take care of the rest.

Note: If you receive Social Security or other government payroll payments, you may call the number listed at the bottom of the Payroll Direct Deposit form to set up direct deposit

Limits

SafeSpend Card Load (Funding) Limits		
	Ordered SafeSpend Card without BBVA Compass Debit Card	**Ordered SafeSpend Card with BBVA Compass Debit Card**
Maximum balance of funds on card	$3,000	$6,500
Maximum amount of all loads	$1,600 during any 15-day period	$3,500 during any 15-day period
Maximum number of loads	3 during any 7-day period	3 during any 7-day period
Maximum for Visa ReadyLink Loads	$500/load $500 during any 7-day period 3 loads during any 7-day period	$600/load $1,500 during any 7-day period 3 loads during any 7-day period
Maximum amount of any direct deposit	$1,600	$3,500
Maximum amount of any transfer from your BBVAC debit card	n/a	$2,500
Minimum load amount	$20	$20

SafeSpend Card Transaction Limits		
	Ordered SafeSpend Card without BBVA Compass Debit Card	**Ordered SafeSpend Card with BBVA Compass Debit Card**
Daily limit for transactions to obtain cash from a Visa ATM	$400/transaction	$600/transaction
	$400/day	$600/day
Daily limit for all other kinds of transactions, including purchases at Visa Merchants	$1,500/transaction	$1,500/transaction
	$1,500/day	$1,500/day
Daily limit for all transactions	$1,500/day	$1,500/day

Schedule of Fees

New Card	No Charge
Card Activation	No Charge
Initial Loading of Funds	$4
Monthly Maintenance	$4/month
Reloading of Funds	No Charge by BBVA Compass
Card Reissued after Expiration	No Charge
Replacement of Lost/Stolen Card	No Charge
Card for Authorized User	$4
Email/Text Message Alerts	No Charge by BBVA Compass*
Paper Statements	$4/month

Copy of Statement	$4/statement
Check for Funds	$15 (charged only if you terminate use of Card)
Balance Inquiry	
Domestic ATM	No Charge by BBVA Compass
Foreign ATM	$1
Withdrawal	
Domestic ATM	$1**
Foreign ATM	$3**
Foreign Transactions	
Withdrawal at Foreign ATM	1% of the U.S. dollar amount of the withdrawal
All other Foreign Transactions	3% of the U.S. dollar amount of the transaction

*Message and data rates may apply. Please check with your wireless carrier about such fees.

** BBVA Compass will not charge a fee for the first withdrawal from an ATM each month regardless of whether that withdrawal occurs at a domestic or foreign ATM.

SafeSpend Terms & Conditions

Links to third party sites are provided for your convenience. These sites are not within our control and may not have the same privacy, security or accessibility standards. Third parties are completely and solely responsible for the content and availability of their sites.

Like 89k Follow @bbvacompass 7,916 followers

banking built for you.

© 2015 BBVA Compass Bancshares, Inc. Compass Bank is a Member FDIC and an Equal Housing Lender. BBVA Compass is a trade name of Compass Bank, a member of the BBVA Group.

Bank of America Online Banking

Get Answers

How to send money online to friends and family

Whether you're sending money to a neighbor across town or helping out relatives overseas, there are a number of easy ways to send money. Here's an overview of your options.

At one time or another, most people need to send money to an individual, family member or friend. Maybe you need to top off the account of a child away at college, pay your son's piano teacher or help support relatives abroad. Whatever the reason, there are several ways to send money, each with its own advantages.

1. Online transfer using an email address or mobile number. Some banks, including Bank of America, now offer account holders the ability to send money securely using just the email or mobile phone number of the recipient. This lets you easily send money to someone else's account, which makes it a great way to transfer money to a student away at school or someone you pay often, like a babysitter. You can even send money via mobile transfer to split a bill or as a birthday gift. Just enter the amount to transfer and the recipient will receive a text or email with instructions on how to receive it.

- **Fees:** Most standard transfers are no-cost to Bank of America account holders
- **Delivery time:** Less than a day
- **Security:** High

2. Online transfer using an account number and routing number. This lets you easily send money online to someone else's account, and is also a great way to transfer money between your own accounts with Bank of America or at other financial institutions. To perform a transfer, sign in to your account and select **Transfers** from the navigation menu. You'll need to know the account number and transit routing number of the recipient.

What's a transit routing number? A transit routing number—also known as a check routing number, ABA number or routing transit number (RTN) —is a 9-digit code that identifies the bank, its branch and location. Bank of America Online Banking customers can find their routing numbers by signing into Online Banking, selecting your desired account and going to the **Information & Services** tab of the specific account. Or, if you know the state your account was opened in, use the dropdown menu on our routing numbers from Bank of America FAQ page.

- **Fees:** Some banks charge a fee
- **Delivery time:** Varies, but can take 2-4 days
- **Security:** High

3. Checks. If you're wondering how to send money to someone who can't receive a transfer through online banking, checks sent via the mail are a straightforward alternative.

- **Fees:** Writing and cashing checks may have no cost or carry a small service charge depending on your account. Contact your bank to find out.
- **Delivery time:** Domestic mail takes 1-3 days. The recipient will then have to deposit the check. For cashier's checks, recipients receive the money immediately, but for regular checks they may have to wait several days before accessing the money.
- **Security:** Though it's rare, some checks do get lost in the mail. Ask your bank the procedure you should follow if this happens.

4. Wire transfers. For sending a large amount of money, wire transfers can be a solution. Keep in mind that there's typically a fee for wire transfers. To make a wire transfer, call or visit your bank or a wire transfer company, or make an online transaction with a trusted source.

- **Fees:** Often
- **Delivery time:** Funds are often transferred the same day
- **Security:** High

5. Money orders. You can purchase money orders from your bank or the U.S. Postal Service and mail them to people in the U.S. or around the world.

- **Fees:** For U.S. Postal Service money orders, you pay $1.20 for a money order up to $500 and $1.60 for a money order between $500 and $1,000 in the U.S. If you're sending money internationally, the fee is $4.50 for a money order up to $700. For bank money orders, check the fees with your branch.
- **Delivery time:** It will take 1-3 days to mail domestically and longer internationally. Domestic recipients can cash money orders at either the post office or their bank.
- **Security:** You may be able to have money orders replaced if they're lost, stolen or damaged.

EXHIBIT
K-32

With so many ways to send money to family and friends, there is sure to be a method that offers the delivery times, fees and security that work best for you.

Learn

more about this topic

- Email and mobile transfers FAQ
- Mobile Banking
- Online Banking Service Agreement
- Online Banking Security Guarantee

More in **Get Answers**

Talk

to a solutions expert

For more information on Bank of America products and services

866.736.2205

Mon–Fri 7 a.m.–10 p.m.
Sat–Sun 8 a.m.–5 p.m.

To make an appointment online to meet with a personal banker

Visit

Schedule an appointment

Find

our related products

Transfer money

Easily send money using only the recipient's email address or mobile number.

Learn more

Service Agreement
eCommunications Disclosure
Online Banking Security Guarantee
Alerts
Statements
BankAmeriDeals®
Transfers
Quicken

Apple, the Apple logo, iPhone, iPad, Mac and MacBookAir are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc.

Some accounts, services and fees vary from state to state. Please review the Personal Schedule of Fees for your state, also available at your local Banking Center.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2015 Bank of America Corporation. All rights reserved.

Overview	Features	Getting Started	Common Costs & FAQs

See how simple Chase Liquid can be.

Get Chase Liquid at your local branch, with no fees to open or activate. You'll leave the branch with a fully functioning card. Just a $25 initial load to get started.

EXHIBIT
K-33

Load cash and checks at any Chase DepositFriendly℠ ATM, load checks using Chase QuickDeposit℠[1] or Direct Deposit, or transfer funds from accounts. Available 24/7, with no hassles.

Use Chase Liquid virtually anywhere VISA® debit cards are accepted[2] and withdraw cash at any Chase ATM or branch without paying a fee. Plus, track your balance with text banking[3] and mobile banking.

Reload easily without any fees with Direct Deposit or at more than 11,500 Chase DepositFriendly℠ ATMs.

Use your Chase Liquid Card to make everyday purchases virtually anywhere Visa® debit cards are accepted.[2]

Learn more »

Check your balance, deposit a check, and get Account Alerts all in the palm of your hand with the free Chase Mobile® App.[4]

Learn more about Chase Mobile »

A chip transaction adds another layer of security to cards by requiring the chip to produce a single-use code to validate the transactic

Learn more »

[1]Chase QuickDeposit℠ is available for select mobile devices. Enroll in Chase Online℠ and download the Chase Mobile® App. Message and data rates may apply. Subject to eligibility and further review. Deposits are subject to verification and not available for immediate withdrawal. Deposit limits and other restrictions apply. See Chase.com/QuickDeposit for details and eligible mobile devices.

[2]Excluding rentals (e.g., cars, equipment, furniture).

[3]**Account Alerts:** There is no charge from Chase, but message and data rates may apply. Delivery of alerts may be delayed for various reasons, including service outages affecting your phone, wireless, or Internet provider; technology failures; and system capacity limitations. Any time you review your balance, keep in mind it may not reflect all transactions, including recent prepaid card transactions.

[4]Chase Mobile® App is available for select mobile devices. Enroll in Chase Online℠ and download the Chase Mobile® App. There is no charge from Chase, but message and data rates may apply.

A Monthly Service Fee applies. Deposited Item Returned Fees, Non-Chase ATM Fees, and other fees may apply.

Deposit products provided by JPMorgan Chase Bank, N.A. Member FDIC.

© 2015 JPMorgan Chase & Co.

The reloadable card that's filled with features, not fees.

Withdraw cash

With a Chase Liquid Card, your cash is more accessible. Take advantage of 24/7 access at over 18,000 Chase ATMs (withdraw up to $500 per day). You can also withdraw cash by obtaining a cash advance from any Chase Teller. These cash advances, along with purchases, have a total daily limit of up to $3,000 per day.

Load your card

Loading money to your Chase Liquid Card is quick and easy. You can automatically load your paycheck, government benefit check, or tax refund onto your card by enrolling in Direct Deposit. You can load checks using Chase QuickDeposit℠ on your mobile device[5] , load cash or checks to your card at over 11,500 Chase DepositFriendly℠ ATMs, 24/7, or load money at any Chase branch. Cash loads are limited to $4,000 per month. Direct deposits, check deposits at ATM/Teller and transfers from a Chase checking or savings account are unlimited.

EXHIBIT
K-34

Monitor your balance

With Chase Liquid, there are many ways to monitor your balance, all without paying a fee:

- Sign up for online banking on Chase.com to check balances and see purchase history online.
- Download the Chase Mobile® App[4] to check balances and see purchase history on your mobile device.
- Sign up for customized email or text alerts[3] to allow you to see when your balance reaches certain limits. Once enrolled, you will also be able to text "bal" to Chase at 24273 for a text message of your available balance.

Make purchases

Chase Liquid Card can be used for purchases virtually anywhere VISA® debit cards are accepted, including online purchases, excluding rentals (e.g., cars, equipment, furniture), without worrying about additional fees. Purchases, along with cash advances have a total daily limit up to $3,000 per day.

Pay bills

You can use Chase Liquid to pay phone, electric, cable and any other bill at merchant sites where VISA® debit cards are accepted.[2] Whether it's online or over the phone, you can pay with your card and the amount will be deducted from your balance.

Save on fees

With one flat monthly fee of $4.95, there's no confusion. Load your card at any Chase DepositFriendly℠ ATM without fees or the hassles of refill packs. Enjoy no fee cash withdrawals at any Chase ATM. Plus, since you spend only what you load, you won't have to worry about overdraft fees.

Chase on your side

Take advantage of the added benefits of being with Chase through Chase Liquid:

- Your funds are FDIC insured,[7] so you can load government benefit checks and tax refunds to your card.
- Zero Liability Protection for any unauthorized card transactions when you notify us promptly. Certain limitations apply.[8]
- Guaranteed Reimbursement for any unauthorized purchases and withdrawals.[9] The money is back in your account by end of the next business day.

Service and support

You can get service and support through Chase.com, by calling our customer service line at 1-877-712-0088, or by visiting your local branch. No matter which you choose, you won't pay a fee for customer service.

Use your Chase Liquid Card to make everyday purchases virtually anywhere Visa® debit cards are accepted.[2]

Learn more »

Check your balance, deposit a check, and get Account Alerts all in the palm of your hand with the free Chase Mobile® App.[4]

Learn more about Chase Mobile »

A chip transaction adds another layer of security to cards by requiring the chip to produce a single-use code to validate the transactic

Learn more »

[1]Chase QuickDeposit℠ is available for select mobile devices. Enroll in Chase Online℠ and download the Chase Mobile® App. Message and data rates may apply. Subject to eligibility and further review. Deposits are subject to verification and not available for immediate withdrawal. Deposit limits and other restrictions apply. See Chase.com/QuickDeposit for details and eligible mobile devices.

[2]Excluding rentals (e.g., cars, equipment, furniture).

[3]**Account Alerts:** There is no charge from Chase, but message and data rates may apply. Delivery of alerts may be delayed for various reasons, including service outages affecting your phone, wireless, or Internet provider; technology failures; and system capacity limitations. Any time you review your balance, keep in mind it may not reflect all transactions, including recent prepaid card transactions.

[4]Chase Mobile® App is available for select mobile devices. Enroll in Chase Online℠ and download the Chase Mobile® App. There is no charge from Chase, but message and data rates may apply.

A Monthly Service Fee applies. Deposited Item Returned Fees, Non-Chase ATM Fees, and other fees may apply.

Deposit products provided by JPMorgan Chase Bank, N.A. Member FDIC.

© 2015 JPMorgan Chase & Co.

SERVICES

WAYS TO BANK

Online Banking
Mobile & Tablet Banking
Mobile Check Deposit
Citi Mobile Apps
Citi Mobile for Smartphones
Citi Text Banking
Citi Tablet Apps
Worldwide ATM Network
Citibank Branches
CitiPhone® Banking
Citibank en Espanol

MANAGE YOUR ACCOUNT

Account Alerts
Linking Citi Accounts
Citi® Financial Tools
Online Bank Statements
Online Check Images
eBills
Citibank® Debit Card
Deposits
Auto Save
Split Tax Refund

MOVE YOUR MONEY

Online Bill Payment
Transfers
Inter Institution Transfers
Wire Transfers
Citibank Global Transfers
Popmoney
MasterCard PayPass

PROTECT YOUR MONEY

Online & Mobile Fraud Protection
Citi Identity Theft Solutions

Popmoney®

A whole new way to send money.

Welcome to Popmoney® – the new way to "Pay Other People" directly from your Citibank account. Popmoney is right for you if:

• You want to make a Person-to-Person payment

• You're a Small Business owner and are looking for an easy-to-use electronic payments and invoicing system

Right for you if:

Person-to-Person

You send money to kids at college

You send anyone the gift of cash

You want to square up with your friends

Small Business

You send payments to vendors

You send payments to employees

You send invoices to customers

You receive payments from customers or vendors

NOT A CUSTOMER? OPEN AN ACCOUNT

Call us at 1-800-374-9700
Text Telephone (TTY) 1-800-788-0002

Sign on to use Popmoney®

What You Get

Person-to-Person

Popmoney® is the exciting new way to make payments. You can use your existing Citibank checking, savings or money market account to send or deposit payments. Use Popmoney® to:

Send money to your child at college
Send the gift of money to anyone
Pay back friends when you split the bill
Send your gift to a wedding when you can't attend

Small Business

Popmoney® for Small Business is a comprehensive electronic and payments invoicing system designed specifically for small businesses. With Popmoney you can easily:

Send electronic payments to vendors
Send electronic payments to employees
Invoice customers
Receive electronic payments against your invoices

How It Works

Send Money

Person-to-Person

To send money, simply sign on to Citi Online and go to Payments or Transfers. Or sign on to the Citi mobile app and from Payments or Transfers go to Pay Other People.

Works With These Products

Person-to-Person
Checking Accounts

Savings Accounts

Money Market Accounts

Small Business
Business Checking Accounts

Business Savings Accounts

Business Money Market Accounts

EXHIBIT
K-35

Safety Check

OVERDRAFT PROTECTION

Checking Plus

Safety Check

GLOBAL CLIENT BANKING

Relocating to/from the US

Moving to the US

Leaving the US

Traveling Abroad

Purchasing Property in the US

Moving Money Internationally

Citibank Global Transfers

Wire Transfers

Banking Services

Once you are enrolled, you can send money to anyone in the US with a bank account by using his or her email address or bank account information.

Your Popmoney® transaction may be completed in as few as 3 business days—we'll notify you when the transaction is complete.[1]

Small Business

To pay vendors, employees and invoice customers, simply sign on to Citi Online and go to Payments or Transfers. Once you are enrolled, you can add contacts (payees), and quickly send payments to vendors and employees in the US with a bank account by using his her email address or bank account information.[2]

Receive Money

Person-to-Person

You'll receive an email or text message that someone is sending you money. Sign on to Citi Online to enroll with Popmoney®, and set up Auto Deposit. The money will be sent to your account and deposited.

Small Business

You'll receive an email notification that one of your customers or vendors is paying an invoice. The money will be automatically sent to your account and deposited.

APPLY ONLINE FIND A BRANCH Or, call us at 1-800-374-9700 (TTY 1-800-788-0002) to open an account or learn more.

1. For complete details, see the Popmoney Terms & Conditions.

2. For complete details see the Popmoney for Small Business Terms & Conditions.

Terms, conditions and fees of accounts, products and services are subject to change.

Norton SECURED AdChoices

This page of citi.com contains information about U.S. domestic financial services provided by the Citigroup family of companies and is intended for use domestically in the U.S.

Copyright © 2015 Citigroup Inc
jfp/prap26-srv2/jfp
BANKRIAWebEnglish/Pop Money

(/payments/)

clearXchange Member Banks

clearXchange is the leading bank-focused person-to-person payments network in the United States. Because of clearXchange's security, convenience, and ease of use, banks representing over 100 million online banking customers have joined the network, allowing their customers to send money to anyone with a U.S. bank account. If you're a customer of one of the member banks listed above, you will either register at your bank's online or mobile site, or through clearXchange.com, depending on how your bank has implemented the network. And if you bank at a non-network bank, you can always register at clearXchange.com. Either way, you can start the registration process here (/payments/get-started).

©2015 clearXchange Intellectual Property. All rights reserved.

EXHIBIT
K-36

ABOUT SSL CERTIFICATES

(https://www.symantec.com/ssl-certificates)

Popmoney

Overview Demo

A simple way to send & receive money

What is Popmoney®?

An online person to person payment service that lets you send, request and receive money to or from friends, family or just about anyone.

Why use Popmoney?

Popmoney provides you the convenience of sending money to virtually anyone you know or owe directly from your bank account. You no longer need to visit an ATM to get cash or write a check to make a payment.

Popmoney Features & Benefits

- Uses the same systems and security you rely on today
- Links over 1,400 banks and more than 35 million registered users

EXHIBIT
K-37

Send or receive funds in as little as one business day*
Personalize emails with eGreetings
Import your contacts from popular email services
Schedule future-dated payments and recurring payments

How Popmoney works

Sending Money

Log in to online banking and select the "Pay People" tab
Select the "Send Money" tab, enter an email address or mobile phone number and the amount you want to send
A text or email will be sent to your recipient with simple instructions on how to deposit the money online

Receiving Money

You receive an email or text message letting you know you have a payment waiting for you
Log in to online banking and select the "Pay People" tab, click the “Overview” tab, then choose the FirstMerit account where the money will go

Requesting Money

Log in to online banking and select the "Pay People" tab
Select the "Request Money" tab, enter the contact's information and the amount you would like to request
A text or email will be sent to your recipient with instructions on how to send money to your account

Not yet enrolled in online banking? Enroll Today!

Let’s Talk

Call: **888-554-4362**
Visit your nearest FirstMerit branch

Let’s Talk

Call: 888-554-4362

Find a Branch

Common uses:

Paying your portion of
a group dinner
Paying the rent
Paying a babysitter
Sending money to
your child at college

Watch Demo

Use Popmoney

* Payment availability is based on selected delivery speed, when recipient accepts payment and the recipient bank's funds availability policy. A delivery or request fee may apply. For more detailed information: view our Popmoney fees and limits.

View our Popmoney Terms & Conditions.

Personal

Banking

Checking Accounts

Savings Accounts & CDs

Credit Card Comparision

Online Banking & Mobile Banking

Online Banking

Online Bill Pay

Account & Security Alerts

Mobile Banking

Mobile Banking Deposit

Popmoney

Loans & Lines

Brokerage, Insurance & Advisory Services

Planning Resources & Calculators

Follow Us

Facebook

LinkedIn
Twitter

YouTube

Personal
Business
Commercial
PrivateBank

About Us
Careers
Investors
Security

Customer Service

Access Your Accounts

Planning Calculators

Locations

Privacy & Disclosures | Terms of Use | Site Map |

CRA | Browser Requirements

© 2015 FirstMerit Corporation. All rights reserved.

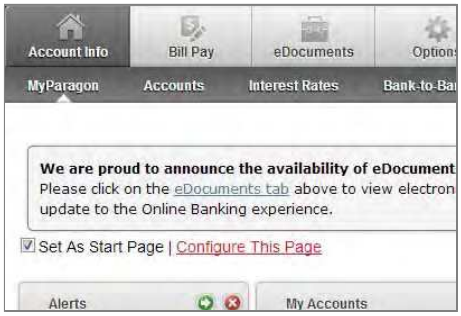
Member
FDIC

Person-to-Person Payments

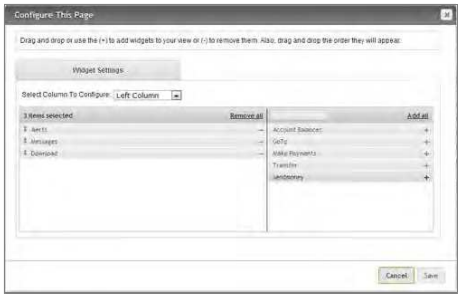
Out to dinner with friends and forget your wallet? No cash to pay the babysitter? Person-to-Person Payments allows you to send money to an individual simply by entering their e-mail address.

See the step by step process to use P2P Payments below!

To begin using P2P Payments, the **sendmoney** widget needs to be added to your **MyParagon** page by clicking **Configure This Page** in the top left of the page.



The widget configuration options will appear. Click on the **plus symbol** next to **sendmoney** in the right column, and be sure to click **Save**. The widget will now appear on your MyParagon page.



Now you can send money to someone by clicking **Click Here** within the sendmoney widget.

Your first time accessing the P2P feature will be unique. You'll have to select the one account from which all P2P transactions are paid. Please choose wisely as this selection cannot

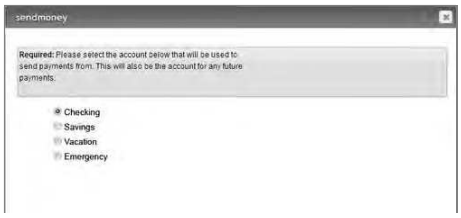
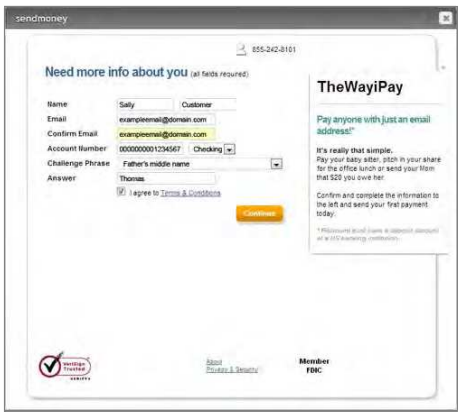


EXHIBIT
K-38

be changed without the assistance of Paragon. If you do end up needing this changed at any time, simply contact us at 901.273.2900.

You'll need to complete the personal information form and agree to the terms and conditions to proceed.



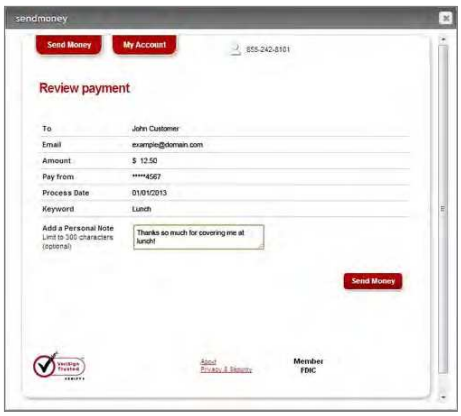
The name and email address of your first payee will need to be entered. You'll also create a keyword. This keyword is extremely important as the payee will need it to complete the verification of their account and complete the funds transfer.

Once you've created the payee, the system will need to verify that the request is indeed legitimate. You'll be provi choice of phone call, text message, or email.

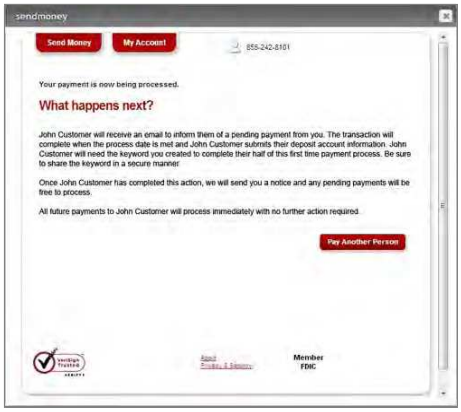
Once you receive the activation code, you'll be required to enter it into the

field. The new payee creation will then be complete.

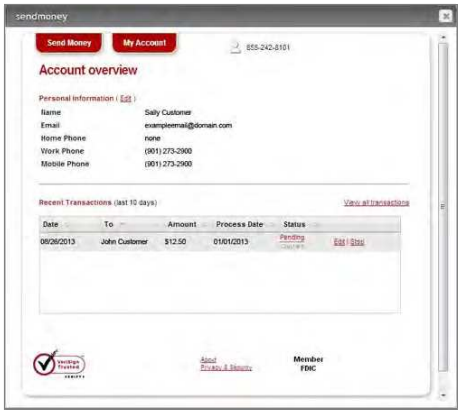
Finally, you'll be able to review the payment information and even include a personal note. The personal note can be used to thank the recipient or simply tell them the reason for which the payment is being made.



You'll then be given the recipient's required steps to finish the transfer. The recipient will receive an email informing them of a pending payment. Again, they'll need the keyword to complete their half of this first-time payment. Once completed, we'll send you a notice and the pending payments will be processed. All future payments to this payee will process immediately and require no further action.



You can click the My Account tab to view payment history, status, and more. You can also edit or even stop a pending payment.



P.O. Box 2022 | Memphis, TN 38101-2022 | Phone: 901.273.2900 | Fax: 901.273.2908 | info@bankparagon.com
Privacy Policy | ©2013 Paragon Bank | All Rights Reserved | Member FDIC | An Equal Housing Lender

Bank of America

Discover an easier way to send money

All you need is a recipient's email or mobile number.

Now through Online and Mobile Banking you can securely send and receive money using an email address or mobile number.[1]

Overview | How to Register | How to Send Money | FAQs

How to Send Money

Easily and securely send money to account holders at banks nationwide using their email address or mobile number.

To make a transfer to someone else:

1. After signing in to Online or Mobile Banking, locate the **Transfers** tab.
2. In the **Send Money To Someone** drop down, select **Using their email address or mobile number.**
3. Click **Add email or mobile recipient**, and after filling out your recipient's info and answering a security question, click **Add Recipient**. This info will be saved for future transfers.
4. When you're ready to transfer money, select your recipient and enter the amount. After making sure everything looks good, click **Make transfer.**

Your recipient will then receive a notification when the money has been sent. If the recipient is already registered, the money will be directly deposited into their account. If not, the recipient will need to complete the one-time registration process to receive their funds through their bank or with clearXchange.

Sign in and get started

Watch this video to see how simple it is to make transfers using a recipient's email address or mobile number.

[1] Requires enrollment in service. Email and Mobile Transfers must be made from a Bank of America consumer checking or savings account to a US-based bank account. Recipients have 14 days to register to receive money or transfer will be cancelled. Dollar and frequency limits apply. See the Online Banking Service Agreement for details, including cut-off and delivery times. Wireless carrier charges may apply.

[2]

EXHIBIT
K-39

You are not liable for fraudulent Online Banking transactions when you notify the bank within 60 days of the transaction first appearing on your statement and comply with security responsibilities. See our Online Banking Service Agreement for full terms and conditions.

[3] To access Online or Mobile Banking, you must enroll in the service. Once enrolled, the same Online ID and passcode can be used to access both Online and Mobile Banking. View the Online Banking Service Agreement for more information. Data connection required. Wireless carrier fees may apply. Enrollment not available through the Mobile App on all devices.

Privacy & Security

Bank of America, N.A. Member FDCI. Equal Housing Lender

© 2014 Bank of America Corporation. All rights reserved.

ARCSV5H4/K31I3I

Search Search …

Mascoma Savings Bank

With Person-To-Person payments all you need to send money is an email address.

Home » **Person To Person Payment**

PERSON-TO-PERSON PAYMENT

EXHIBIT 40

Send money to anyone with a bank account in the United States with just an email address. All you need to send money is your friend, child, or associate's email address. Whether you are "settling up" or providing spending money, sending money just got infinitely easier. Go to your Mascoma Internet Banking page and click the "send money" icon, and your recipient can deposit the money right into a bank account. No account numbers are exchanged so your banking information is kept private.

How to set up payment

First, add the sendmoney widget to your "My NetTeller" page in Internet Banking then configure to the Net Teller page.

Learn More

How to send a payment

Go to "My NetTeller" (if it is not your default start page.) Click on the SendMoney Widget and follow instructions.

Learn More

How to receive a payment

You will be contacted by the person sending you a payment.

Learn More

Person 2 Person Payments
How to Send a Payment

Mascoma Savings Bank

Go to "My NetTeller" (if it is not your default start page.)

Click on the ***SendMoney*** Widget.

This will bring you to the P2P Widget Window.

Enter in the Name of the Recipient (First and Last Name),

the Payee's Email address,

amount of the payment,

select a Process date (today is the default),

make up a Keyword:

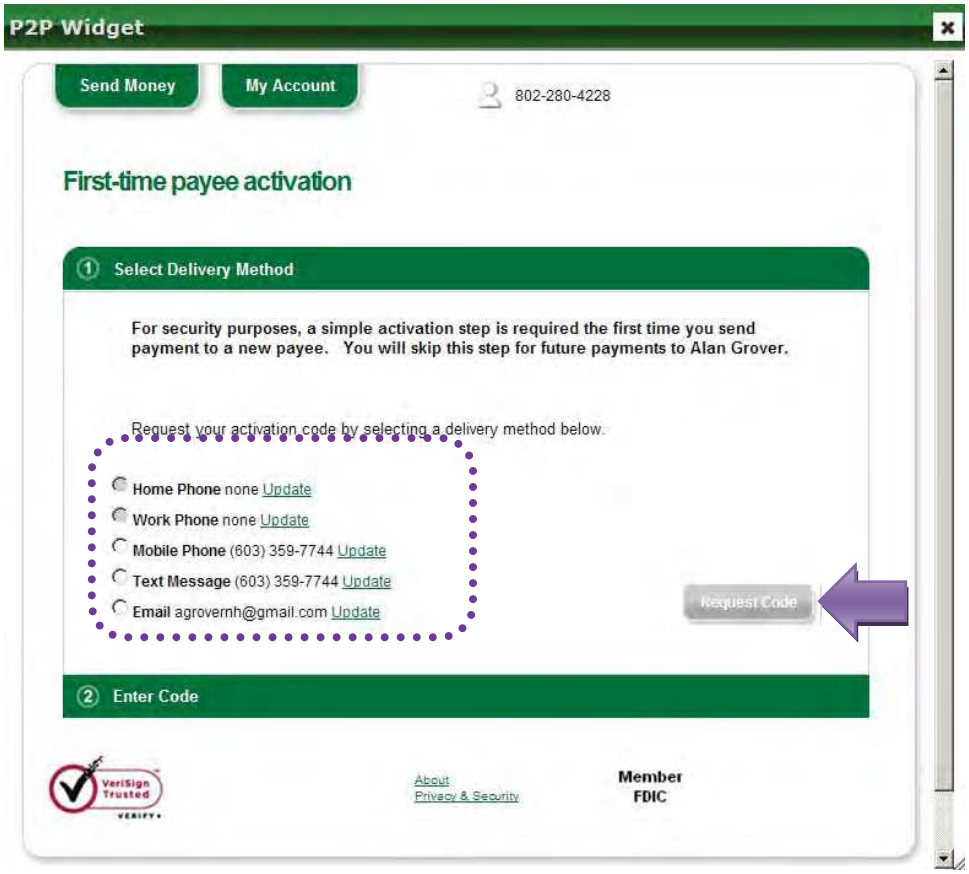
The Keyword will need to be communicated to the recipient via a secure method (such as calling them on the phone and telling them their Keyword). The recipient will need the Keyword to complete their portion of payment process. This process only happens one time, all future payments to the same recipient will bypass this process.

When done click **Continue**.

EXHIBIT 41

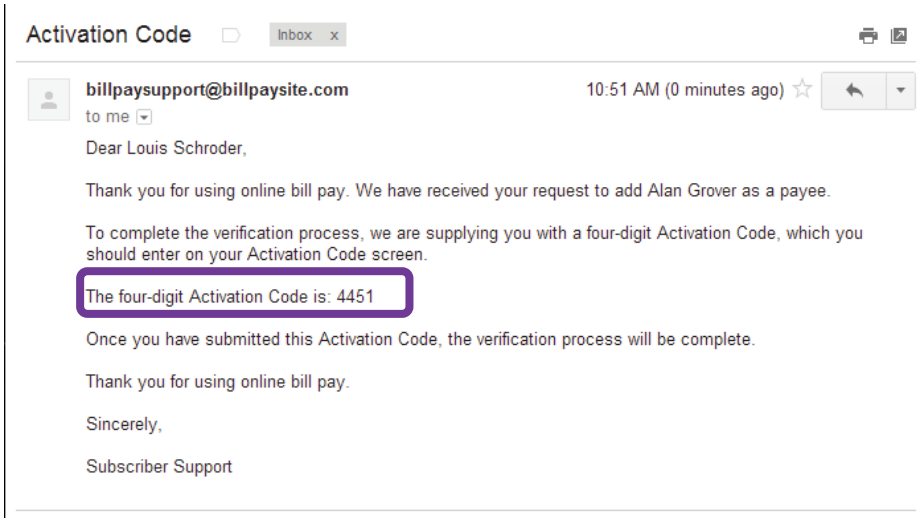
For security purposes, you will need an activation code to set up any person you want to make a payment to. Select from the radio buttons how you would like to receive the one-time activation code.

After you select your method, click the **Request Code** button.



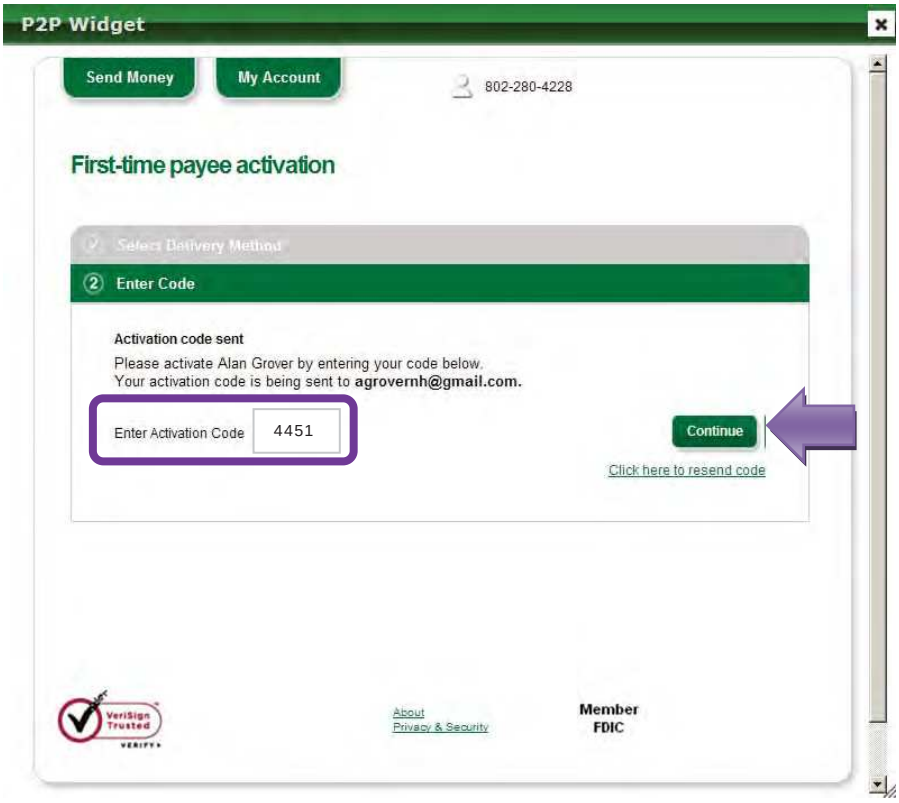
The code will be sent by the method that you chose. Go to the method that you requested for the code. If you requested email, do not close the P2P Widget, open a new Tab or Web Browser session to get the code. For this example I chose E-mail:

Here is the code I will enter into the P2P Widget.



Enter in the Activation Code:

Then Click **Continue**:

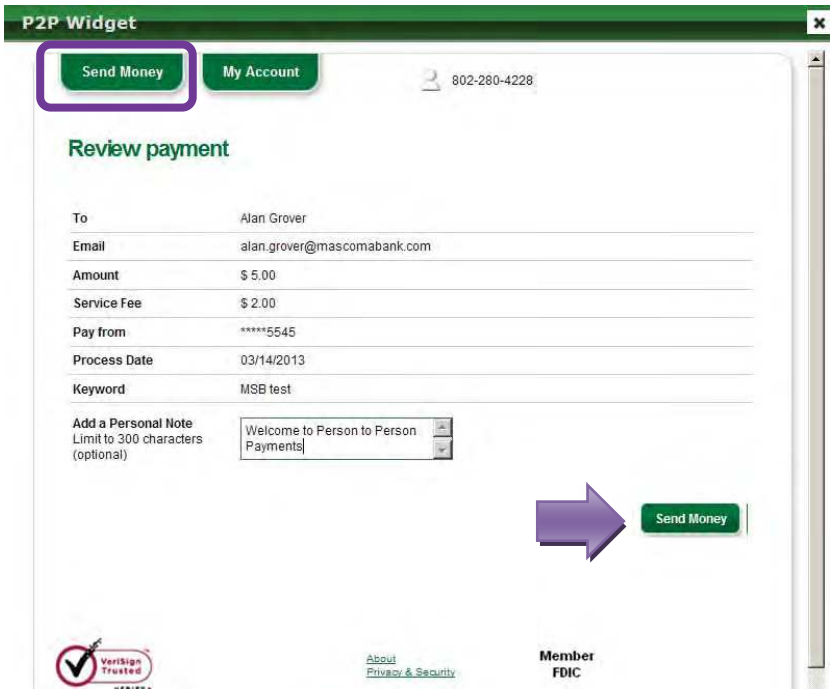


Person 2 Person Payments
How to Send a Payment

Review the payment
If something is not correct you will need to click on the **Send Money tab** and refill in the correct information.

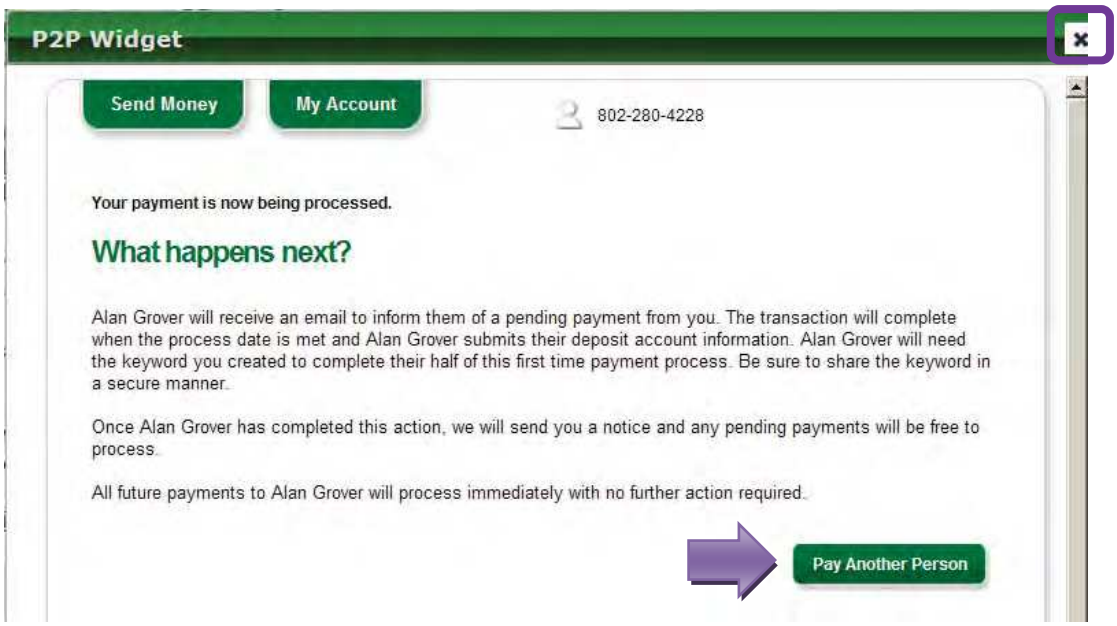
You can add a personal note to the payee of up to 300 characters.

To complete the payment click **Send Money.**



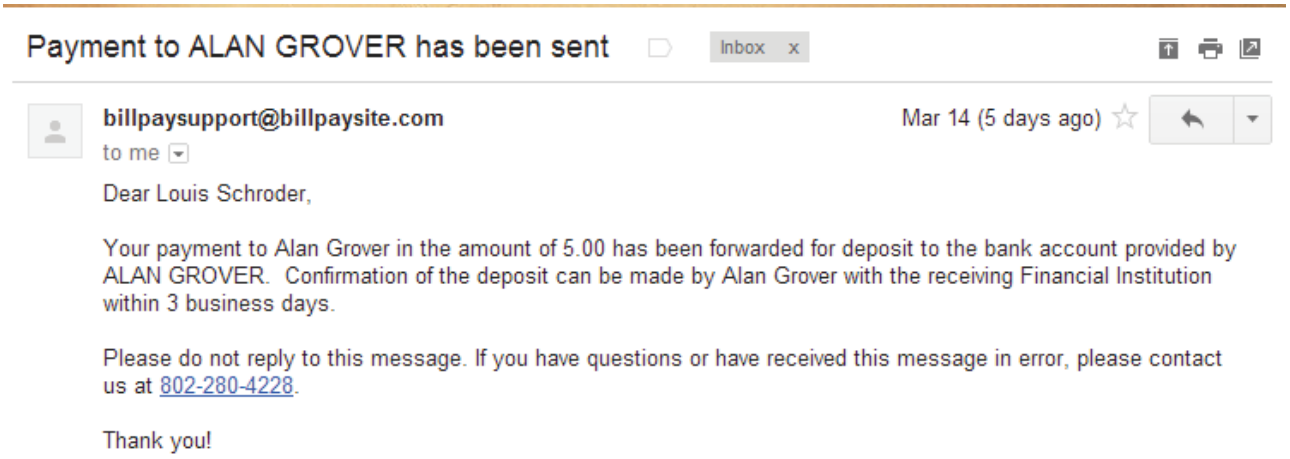
You will receive a notice that the payment is now being processed and the steps that the recipient will need to do. Important Notice: The payment will not process until the recipient has completed their setup in the payment system. Once the recipient completes that you will receive an email that this has occurred and that the payment is now in process.

Future payments to this payee will not require additional actions by the recipient.



You have the option to pay another person or if you are done click the **X** in the upper right hand corner of the widget.

When the recipient has completed their part of the signup you will receive an email (example below) letting you know the payment has gone out.



Person-to-Person Payments

Summary

TheWayiPay®

Send payments from your Northeast Bank checking account to anyone with an account at a U.S. financial institution and a valid email address.

Details:

Send payments to practically anyone 24/7, including weekends and holidays
Enjoy the convenience of paying your family and friends without the hassle of writing a check or carrying cash
Save time by not having to write and mail checks – service is more efficient than writing checks and less expensive than sending a wire transfer.
Easy to use — access by adding the SendMoney widget in NetTeller online banking, send your payment in minutes
Safe and secure process to add new payees — with multiple verification steps built in
Protect your financial information as well as the payee's information
Start using P2P payments now to:
Pay a friend back for lunch or a movie
Send money to your kids at college
Pay the babysitter
Send a gift to a family member or friend
Easy to get started - follow the instructions in this guide to get started using the service
$1.00 charge per P2P payment
See our frequently asked questions, including limits on payments and how to use.

Northeast Bank
Copyright © 2015, All rights reserved.

Google+

EXHIBIT
K-42

Northeast Bank

Strength of a Leader. Hand of a Friend.

TheWayiPay® Person-to-Person (P2P) Payments FAQ

What is TheWayiPay® payment service?

How much do TheWayiPay payments cost?

How do I sign up for TheWayiPay payment service?

How does TheWayiPay work?

How do I send a TheWayiPay payment?

Are there limits for TheWayiPay payments?

When can I use TheWayiPay?

How long do the TheWayiPay payments take?

Will TheWayiPay payments work on my smartphone?

What is TheWayiPay® payment service?

TheWayiPay® is a secure online person-to-person payment service that allows you to electronically send money to virtually anyone who has a valid email address and a personal deposit account at a U.S. financial institution. The recipient confirms the payment by providing the "keyword" and their account information in a safe and confidential transmission. Enjoy the convenience of paying your family and friends without the hassle of writing a check or having cash. Payments are convenient, easy and secure with TheWayiPay.

- Pay a friend for dinner or a movie.
- Send money to kids in college.
- Give a gift to a family member or friend.
- Pay the babysitter, house cleaner, etc.
- Enjoy the convenience of making payments 24 hours a day, even weekends and holidays.

Payments accepted by the recipient by 2 p.m. Central Time are processed that business day. Weekend and holiday deposits will be processed the next business day.

How much do TheWayiPay payments cost?

The fee for TheWayiPay is $1.00 per payment. This fee will be charged to your account each time you make a payment with TheWayiPay service.

How do I sign up for TheWayiPay payment service?

Enrollment is easy. If you are an existing Northeast Bank customer with personal NetTeller Online Banking, you will need to add TheWayiPay to your My NetTeller online banking page.

- Login to your NetTeller Online Banking account through an internet browser.
- Click on My NetTeller, if you do not already use that for your landing page.
- Click on "Configure This Page". Your widget settings will be displayed.

EXHIBIT
K-43

- The widget you need for TheWayiPay is called "SENDMONEY". Click to add SENDMONEY to your widget settings.
- You can also configure the order that your widget appears by clicking on the widget and dragging it up or down in the list.
- Save the changes to exit.
- Click on "Click Here" on the SENDMONEY widget and follow the prompts to set up your profile and review and agree to TheWayiPay Service Agreement.

Then you are ready to make your first payment.

If you do not have NetTeller Online Banking, enroll now by calling Northeast Bank at 612-379-8811 and asking for a Personal Banker.

During and after enrollment, please check your email account to make sure your TheWayiPay notifications reach your inbox (and are not blocked or sent to your "junk mail" folder). Otherwise, you may not be able to complete enrollment and start receiving notifications about TheWayiPay.

How does TheWayiPay work?

Upon enrollment, TheWayiPay allows you to send payments to virtually anyone with an email address and a bank account at a U.S. financial institution.

Payees are added by creating a new payee and then going through a safe and secure payee enrollment process. You will be required to enter their name and email address, as well as a short confirmation code before a new payee can receive payments. New payees are required to follow a secure link from an email that will be sent to the email address provided requiring them to enter a security phrase that you will create and provide them to confirm their authority to receive payments, and then to enter their account information for the account into which they would like to receive payment. Once the new payee is added all you have to do is enter the payee's name in the "To" field for future payments.

How do I send a TheWayiPay payment?

To make a TheWayiPay Payment to a payee for the first time, follow these steps:

1. Login to NetTeller Online Banking. Select "My NetTeller".
2. Click on the "SENDMONEY" (TheWayiPay) widget.
3. Fill in name and email address of the person you want to pay (payee).
4. Fill in the dollar amount of the payment.
5. Select the process date.
6. Enter the Keyword (A special word that only you and your payee will know. Your payee will need this word to complete the transaction.)
7. Select the delivery method to receive your request code.
8. Input your request code.
9. Add a personal note (optional).
10. Click "Send Money".

The payee will receive an email to inform them of a pending payment from you. The transaction will be completed when the process date is met and the payee submits their deposit account information. The

payee will need the keyword you created to complete their half of this first time payment process. Be sure to share the keyword in a secure manner.

To make a TheWayiPay payment to an existing payee, follow these steps:

1. Log in to NetTeller Online Banking. Select “My NetTeller”.
2. Click on the “SENDMONEY” widget.
3. Type the name of the payee and enter. Their email address should auto-populate.
4. Fill in the dollar amount of the payment.
5. Select the process date.
6. Add a personal note (optional).
7. Click “Send Money” and your payment will process on the date indicated.

You can also review and watch the progress of your TheWayiPay payments for the last 30 days by selecting “My Account” inside the “SENDMONEY” widget.

Are there limits for TheWayiPay payments?

Yes, the general limits for TheWayiPay payments are:

- Per payment – $2,000; or
- Not to exceed $2,500 per day

Lower limits may apply. You may request higher limits by calling Northeast Bank at 612-379-8811 and asking for an Electronic Banking Specialist.

When can I use TheWayiPay?

You can use TheWayiPay® 24 hours a day, including weekends and holidays. For faster payments, make sure you input your payment before the 2 p.m. Central Time each business day.

How long do the TheWayiPay payments take?

TheWayiPay uses the ACH network to send money to the recipient. Payments can take up to three (3) business days for new payees. New payee setup is a one-time occurrence so subsequent payments often take less time. The sender will typically see the funds withdrawn from their account one business day before they are deposited into the account of the recipient. For faster payments, make sure you input your payment before the 2 p.m. Central Time each business day. Note: the fastest way to get a payment to another person somewhere else is still usually via sending a wire transfer.

Will TheWayiPay payments work on my smartphone?

Once you have signed up for TheWayiPay payments, you can access NetTeller Online Banking through your browser on your smartphone; and then select the “SENDMONEY” widget. The display size on smartphones (e.g., iPhone®) may hinder complete use of all functions of TheWayiPay. Also wireless message and data rates may apply when accessing the service from your device. Please check with your wireless service provider for access rates, texting charges, and other applicable fees. TheWayiPay is not currently integrated into our mobile banking applications.

NB Needham Bank

April 14, 2015 10:30am EST Main Offic

Home Co

Branch / ATM Locations

Search

NB PERSONAL BANKING
Personal Checking, Savings, and CD Accounts.

NB BUSINESS BANKING
Run your business more efficiently with NB Business Banking!

NB RESIDENTIAL LOANS
Residential Loans powered by Needham Bank

NB COMMERCIAL LOANS
Commercial loans to help you run your business.

CUSTOMER SUPPORT

COMMUNITY INVOLV

PERSONAL BANKING LOGIN

Customer ID

Password

Login

Enroll Help

BUSINESS BANKING LOGIN

REMOTE DEPOSIT LOGIN

SERVICES

NB PERSONAL CHECKING

NB PERSONAL SAVINGS

NB CDS & IRAS

FEATURES

NB ONLINE BANKING

NB ATM/NB DEBIT MASTERCARD®

NB MOBILE BANKING

NB PERSON TO PERSON PAYMENTS

Receiving NB Person to Person Payments

DEPOSIT RATES

SWITCH PORTAL

CALCULATORS & TOOLS

NB Person to Person Payments

Send money from your bank account to anyone at any bank in the U.S.

Make deposits into your child's account, conveniently repay friends for event tickets, or effortlessly split bills with roommates using NB Person to Person.

If you have NB Online Banking, you have access to NB Person to Person and can send money without any fees.

To send a person to person payment, you will be prompted to enter the name and then either an account number, email address, or cell phone number of the recipient.

Select the amount of money you would like to send and confirm the recipient's name and contact information.

For faster transfers, provide the recipient's name, routing number, and account number (all available from one of their personal checks) and the funds will be deposited directly into the specified account without any additional action from the recipient.

If you've set up your recipient with a cell phone number or email address, the recipient will receive an email or text message outlining the transfer, and the brief steps they need to follow to receive the transfer.

Additional Information on NB Person to Person:

Receiving Money
Popmoney and Funds Transfer Agreement

SCHEDULE AN APPC

Receiving NB Person to I

If a Needham Bank custom money using your cell phor email address, please see retrieving your money. If...

Learn More

Home Branch / ATM Locations Contact Us Career Opportunities Account Support & Safety Email Signup Our Ad Campaigns

© Copyright 2015 Needham Bank. All rights reserved. Privacy Statement

powered by getfused

MEMBER FDI
MEMBER SIF

EXHIBIT
K-44

PNC *Smart*Access®
Prepaid Visa® Card

Looking for a secure, easy way to access and manage your money? The PNC *Smart***Access** card lets you deposit money, make purchases, pay bills, get cash and more.

Apply for a card today

Complete your application online.

APPLY NOW

Have a Card?

Or, if you have not yet enrolled your card

Sign In

Want access to your tax refund sooner?
Your PNC *Smart*Access Prepaid Visa Card can help.

Find out how »

Key Features

Easy access to your money

You can use your card at millions of places where Visa is accepted.

No overdraft fees

Spend the funds on your card and never worry about overdraft fees.

It's safe and secure

It's more secure than carrying cash.

EXHIBIT
K-45

Features and Benefits

Easy to add money

- Set up direct deposit and get access to your paycheck right away
- Deposit cash at any PNC Branch[1]
- Deposit cash at any participating Visa ReadyLink retail location[2]
- Load cash at select PNC DepositEasy℠ ATMs[3] using the Prepaid Load option

Direct Deposit: It's free and easy to set up

- Set up direct deposit for your paycheck or government benefit payments
- Complete the Direct Deposit Form (or the one provided by your employer)

More secure than carrying cash

- If your card (or its number) is lost or stolen, your money will be replaced if you notify us promptly of its unauthorized use.[4]

Get easy access to your money

- Withdraw your money for free at over 7,300 PNC ATMs.
- Make purchases at millions of places that accept Visa debit cards
- Pay bills quickly and easily with your card on the billers' websites or by calling your billers directly[5]

Track your balance and spending virtually anytime, anywhere

- **Text and email alerts** - Set up alerts for recent deposits, recent purchases and even for low balances, delivered right to your phone or email inbox.[6]
- **PNC *Smart*Access Mobile App** - Keep tabs on your balance and view purchases right from your mobile device. Download now for your iPhone or Android device:[7]
- **Online banking** - Check your balance, view your purchases, manage your alerts and more.

See How It Works

Step 1: Activate your card

- Call 1-866-304-2818
- Go Online

Step 2: Load money

- Add cash anytime at a PNC branch[1], select PNC DepositEasy ATMs[3] or Visa ReadyLink[2]

Step 3: Use your card

- Make purchases where Visa debit cards are accepted
- Pay bills and more

What's New?

How to Apply

Ways to Apply

What You Need to Apply

Frequently Asked Questions

Getting started

Loading money on your card

Making purchases with your card

Security

Additional Card Features and Benefits

Customer Service Questions

PNC Online Banking

PNC *Smart*Access Mobile Services

Standard message and data rates may apply.

Important Legal Disclosures and Information

1. Primary cardholder only.
2. Visa ReadyLink merchants may charge a fee for this service.
3. Cash deposits for *Smart***Access** cards are only available at select PNC ATMs equipped with currency validation technology.
4. Please refer to the *Smart***Access** Terms and Conditions for full information.
5. Although PNC does not charge for these payments your biller may. Be sure to check with your biller before making payments.
6. Standard message and data rates may apply.
7. PNC does not charge a fee for the *Smart***Access** Mobile App. However, third party message and data rates may apply. These include fees your wireless carrier may charge you for data usage and text messaging services. Check with your wireless carrier for details regarding your specific wireless plan and any data usage or text messaging

charges that may apply. Also, a supported mobile device is needed to use the *Smart***Access** Mobile App. Certain other restrictions apply. See the *Smart***Access** Mobile Service Terms and Conditions for details.

Apple, iPod, and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. iPhone and Apple Pay are trademarks of Apple Inc. App Store is a service mark of Apple Inc.

Android and Google Play are trademarks of Google Inc.

FormFree® is a registered trademark of Moneygram International, Inc.

CVS/pharmacy® is a registered trademark of CVS Pharmacy, Inc.

PNC *Smart***Access** and *Smart***Access** are registered trademarks of The PNC Financial Services Group, Inc.

Visa is a registered trademark of Visa International Service Association and used under license.

Bank deposit products and services provided by PNC Bank, National Association. **Member FDIC**

©2015 The PNC Financial Services Group, Inc. All rights reserved.

Transfer Funds

Move your money with ease - to where you need it when you need it.

Move money between your PNC accounts, between your PNC accounts and accounts you own elsewhere, even send money to your friends and family[1]. No checks, no cash, not even a trip to the bank.

Features and Benefits

Between your PNC accounts

Move money between your PNC accounts (checking, savings, loans, credit card and select investment accounts) right from your home computer or mobile device. Make a one-time transfer or set up a recurring transfer and have the money automatically transferred at a frequency you choose. Update or modify your transfer whenever you need to right from the convenience of your home.

Between your PNC and non-PNC accounts

Move money from your accounts elsewhere to your PNC (checking, savings, or money market) account without leaving the house. You can move money in and out of the your account in as little as 3 business days, make a one-time transfer or even set up a recurring transfer for up to a year in advance.

Between you and other people with popmoney

Send money and a personalized message to friends and family with just their email address or mobile phone number[2]! It's the perfect last minute gift, an easy way to tell someone you're thinking of them, and the simplest way to pay your friends and family.

Get Started

Already using Online Banking?

- Log in to Online Banking »
- Then, click on the "Transfer Funds" tab.

New to Online Banking?
Get Started Now »

EXHIBIT
K-46

Important Legal Disclosures and Information

1. Federal regulation prohibits you from making more than a total of 6 transfers each month to other accounts from a savings or money market account (including transfers to another account for overdraft protection) or to third parties each month by check, through point-of-sale purchase transactions with a banking card, by preauthorized or automatic agreements, telephone, or online. See your account agreement for more information. Other limits may apply to your account. Excessive transactions may result in changing your Money Market or Savings account to a non-interest bearing checking account.

Popmoney and the Popmoney Logo are registered marks of CashEdge, Inc. Now part of Fiserv.

All online banking services are subject to and conditional upon adherence to the terms and conditions of the PNC Online Banking Service Agreement.

Bank deposit products and services provided by PNC Bank, National Association. **Member FDIC**

©2015 The PNC Financial Services Group, Inc. All rights reserved.

Frequently Asked Questions
Rewards FAQs
Checking & Savings FAQs
Card Product FAQs
Loans & Credit FAQs
Regions Online Banking FAQs
- Getting Started
- Online Statements
- Account Access
- Transfers
- Bill Payment
- Personal Pay
- Mobile Banking
- Mobile Deposit
- Customer Service
- Browser & Security
- Western Union® Transfer
- Same Day Payment
- My GreenInsights

Customer Service FAQs
How do I?

Regions Personal Pay℠ FAQs

What is Regions Personal Pay?
How does a Personal Pay payment work?
How do I sign up for Personal Pay?
How do I send my first payment to someone?
When does the payment come out of my account?
What do I need to do when I receive my first payment from someone?
How much does this service cost?
How quickly will a payment be received?
What is the maximum amount I can send?
Can I cancel a payment after I send it? If so, how?
What type of confirmation do I get that my payment has been received and accepted?
How long does someone have to claim a payment?
How safe is Personal Pay compared with other similar online payment services or writing a check?
Will the recipient be able to see my account information? Or vice versa?
How is Personal Pay different than using Regions Online Banking Payment Center to pay someone?
Can I use Personal Pay for payments outside of the United States?
How will payments appear on my account statement?
What browsers work best with Personal Pay?
Are there JavaScript concerns I need to be aware of?

What is Regions Personal Pay? [back to top]

Regions Personal Pay is a secure way to send money from your eligible Regions deposit account to anyone with a bank account in the United States.

How does a Personal Pay payment work? [back to top]

As a Regions Online Banking customer, all you need to send a personal payment is the email address or mobile phone number of the person to whom you wish to send funds. After you schedule a payment, the recipient is sent an email or text message with instructions to claim the funds. If the recipient is already enrolled in the Popmoney network, the funds can be deposited into their account in as little as one business day.

For more information regarding terms and conditions of use please see the Electronic Banking Agreement & Disclosure Statement and the Personal Pay Addendum.

How do I sign up for Personal Pay? [back to top]

If you are an Online Banking customer of Regions, you already have access to Personal Pay. If money is sent to you and it matches the email address you have on file at Regions, the funds will be deposited into your checking or money market account. To send money, simply select the "Personal Pay" links from within Online Banking.

Note: To verify that your correct email address is on file, select "Personal Pay" in Online Banking, then select "Preferences."

How do I send my first payment to someone? [back to top]

Log in to Regions Online Banking, and select "Personal Pay" from the Payments tab. Enter the amount you wish to send. Send to the recipient's email or mobile phone, or directly to their bank account. You may also include a short message to the recipient if you wish. Once completed, a message goes out to the recipient's email or mobile phone stating that you have sent them money. The money is debited from your account the day payment is sent. If the recipient does not claim the money within 10 days, the money will be credited back to your account.

EXHIBIT
K-47

When does the payment come out of my account? [back to top]

Any time you send a Personal Pay payment, the money is debited from your account the day the payment is sent. If the recipient does not claim the money within 10 days, the money will be credited back to your account.

What do I need to do when I receive my first payment from someone? [back to top]

If you are a Regions Online Banking customer with an eligible deposit account and a valid email address on file, you are automatically enrolled in the service and the funds will be deposited directly into your account.

If you do not have an email address on file, or the email address/mobile number does not match the email address/mobile number to which the payment was sent, you will simply need log in to Online Banking, select "Personal Pay" from the Payments tab, then select "Preferences" and add the email address or mobile number. Once the email address or mobile number has been added, your payment will automatically be deposited into your account.

How much does this service cost? [back to top]

There is a charge of $1 each time you send a Personal Pay payment. There is no cost to you when you receive funds through the service. The $1 fee will be charged to the sender at the time the payment is sent to the recipient. The fee will be added to the amount of the payment and appear as one transaction in your Online Banking transaction history and monthly statement.

How quickly will a payment be received? [back to top]

If the recipient is enrolled in the Popmoney network, money can be deposited into their checking account in as little as one business day. If they are not in the network, the money can be received in 1-3 business days after enrolling and claiming the funds. The recipient has 10 days to claim the funds. If funds are not claimed within 10 days, a refund of the payment will be issued to the sender.

What is the maximum amount I can send? [back to top]

Daily payment limits vary from customer-to-customer, depending on their credit history, account balance and length of relationship with Regions Bank. To access the payment limits, simply select the help icon next to the "Amount" field. **Note:** This icon only appears after you select your "Pay From" account when scheduling a payment.

Can I cancel a payment after I send it? If so, how? [back to top]

Yes, you may cancel a payment anytime before or on the send date. Your contact will be notified if you cancel a payment after notification has been sent.

What type of confirmation do I get that my payment has been received and accepted? [back to top]

You will receive a payment receipt by email or text stating the date, amount and details documenting that your funds were sent. You may also see if the payment has been claimed by logging to Online Banking and selecting "Personal Pay" under the Payments tab, and then selecting Activity.

How long does someone have to claim a payment? [back to top]

Payments expire after 10 days. The recipient will get an email or text reminder on the third day and again on the seventh to remind them to claim the payment.

How safe is Personal Pay compared with other similar online payment services or writing a check? [back to top]

For maximum safety and security, Regions Online Banking uses SSL (secure sockets layer) and 128-bit encryption. With Personal Pay, there is no go-between or middle person. There is no paper trail, no check or cash to lose or misplace.

Will the recipient be able to see my account information? Or vice versa? [back to top]

No, The recipient will not be able to see any corresponding personal information from the sender including email address or bank account information.

How is Personal Pay different than using Regions Online Banking Payment Center to pay someone? [back to top]

The Bill Pay service within Regions Online Banking is generally designed for paying bills like utilities, services, mortgages and so on. Sending a payment to an individual using the traditional Bill Pay service can take up to five business days to arrive to the recipient because it is sent by check. Regions Personal Pay allows you to send funds electronically using only an email address, mobile number, or bank account information of the person you wish to pay.

Can I use Personal Pay for payments outside of the United States? [back to top]

No, it can only be used between bank accounts in the United States at this time.

How will payments appear on my account statement? [back to top]

Personal Pay payments you make to others will generally appear as electronic withdrawals, similar to the way ATM withdrawals appear and the fee will be combined with the payment amount. Personal Pay payments received will appear as deposits on your account statement.

What browsers work best with Personal Pay? [back to top]

Personal Pay works across many platforms, but we recommend the following to provide the best combination of security and functionality:

Microsoft Internet Explorer 8 (Windows XP, Vista, and 7)
Microsoft Internet Explorer 7 (Windows XP)
Firefox 3.5 (Windows XP)
Apple Safari 4 (OS X 10.5 and 10.6)

Are there JavaScript concerns I need to be aware of? [back to top]

We suggest you enable JavaScript in your browser since it is necessary for some Personal Pay functions.

Member FDIC
© 2015 Regions Financial Corporation. All rights reserved.

Regions Personal Pay[SM]

Filling the gap between writing a check and setting up online bill payments, Regions Personal Pay is the perfect personal payment solution to easily pay for items like dinners with friends, gifts, team dues, fundraisers, even paying the babysitter.

Personal Pay Advantages

- Safe, secure electronic personal payments.
- Powered by Popmoney, a personal payment service that links over 1,400 banks and more than 35 million registered users.
- Faster than the postal service — and just $1* each time you send money.
- Send or receive funds in as little as one business day.
- Personalize emails to your friends and family with eGreetings
- Import contacts from popular email services such as Hotmail, Yahoo! and Gmail
- Schedule future-dated payments and recurring payments

Simple to Start!
If you are a **Regions Online Banking** customer, there's no enrollment necessary! Simply select the Personal Pay link from the Payments tab to send money today or to change the settings for your account. If you don't use Regions Online Banking, **enroll today**.

Log in to Online Banking.

Select "Personal Pay" under the Payment tab.

Enter the email or mobile number, or account number of the person and how much you want to send.

Have questions? View our Regions Personal Pay **FAQs** for more answers.

popmoney

How Regions Personal Pay Works

1. Send money in as little as one business day to your family and friends with only an email address or mobile phone number, or account number.
2. They receive an email or text message to let them know that you have sent them a payment.
3. If they are also enrolled in Regions Personal Pay, they can receive the payment into their bank account. Non-Regions customers can simply go online to popmoney.com to claim their funds.
4. You receive confirmation of payment by email. That's all there is to it!

Have additional questions? View our FAQs.

Share

*The $1.00 fee will be charged to the sender at the time payment processing is initiated. The payment transaction amount that appears in your Online Banking transaction history statement will include the fee.

For more information regarding terms and conditions of use please see the Electronic Banking Agreements & Disclosure Statement and the Personal Pay Addendum.

Member FDIC
© 2015 Regions Financial Corporation. All rights reserved.

EXHIBIT
K-48

ONLINE & MOBILE BANKING

- Online Banking / Billpay
- Mobile Banking
- Mobile Apps
- Make a Deposit
- Bank to Bank Transfers
- Person to Person Payments
- eStatements
- My Finance
- Deposits, Payments and Transfers
- Client Care

PERSON TO PERSON PAYMENTS

Send money to friends and family with just their email address and mobile phone number. With State Bank's Person to Person Payments, you can send money to virtually any individual from your computer or mobile phone.

The solutions you need. The personal service you want.

- Send money to anyone from my computer or mobile phone

State Bank Online Banking and Bill Pay Solutions

- State Bank Online Banking – Person to Person Payments

Take Action

If you have Online Banking and Bill Pay then you automatically have Person to Person Payments

» Contact Us

Open your new account online

Convenience, freedom and control begin with State Bank's free online banking. Wherever you have Internet access, whenever you need to access your accounts, online banking is available right here through our Web site.

Start Today ›

EXHIBIT K-49

800.414.4177

© 2015 State Bank and Trust Company.
All rights reserved.

Member FDIC. Equal Housing Lender
NMLS#441508

SunTrust Prepaid MasterCard®

Pay with Confidence

If you're looking for a convenient and secure alternative to using cash, money orders or paper checks, the SunTrust Prepaid MasterCard may be the solution you're looking for. It's totally funded by you, and you don't need a credit check to get one. Purchase a card at a SunTrust branch, load the funds on the card, and you're ready to go.

Why choose a SunTrust Prepaid MasterCard?

Flexible and Secure | **Convenient for Managing Your Money**

Prepaid cards are more convenient and safer than cash.

Your balance is stored on the card, and you can reload it. Your SunTrust Prepaid MasterCard card can be used to make purchases everywhere MasterCard is accepted, so it's perfect for shopping online, at the grocery store, or anywhere you'd prefer not to pay with cash. You can even use it to get cash at ATMs.[1]

Please visit our Card Center at www.suntrust.com/myprepaidcard and discover an easy and convenient way to check your balance, view your transactions, verify your funding as well as sign up for text alerts.

Contact Us

To reach SunTrust's Prepaid MasterCard Service Center:

888.968.7061

Email Us

Related Links

Financial Education Resources

Building A Budget

Money And Your Marriage

Plan for Future Security

Fee Schedule

Disclaimer

1 Non- SunTrust ATM fee/ATM owner fees may apply. Non-SunTrust Bank ATM Withdrawals $2 per withdrawal. ATMs owned by non-SunTrust institutions may also add a surcharge to the amount of the withdrawal or charge a fee for a balance inquiry even if the withdrawal is not completed. You can not withdraw cash from international ATMs.

2 A qualifying Direct Deposit is a Direct Deposit of your salary, pension, Social Security or other regular monthly income of $500 or more per deposit electronically deposited to your SunTrust Prepaid MasterCard each month by your employer or an outside agency. Card reloads made at a SunTrust branch location or via MasterCard® rePOWER Network do not qualify as a Direct Deposit. SunTrust does not charge a fee for reloads via MasterCard® rePOWER Network. However, applicable merchant fees may apply.

EXHIBIT
K-50

©2013 MasterCard. MasterCard and the MasterCard Brand Marks are trademarks of MasterCard International Incorporated

SunTrust Bank, Member FDIC. ©2013 SunTrust Banks, Inc. SunTrust is a federally registered service mark of SunTrust Banks, Inc.

Person-to-Person Payments

Flexible ways to send and receive money

At TD Bank, it's never been easier to send money to friends, family or anyone at all.

Our Online Banking customers can sign up for Popmoney® to make person-to-person payments, simply and securely, with several delivery options.

Quick and easy setup of recipients

Once enrolled, you'll be able set up your contacts with any (or all) of these delivery methods enabled:

- e-mail address
- mobile phone number (for text message delivery)
- account number

For text and e-mail delivery, the recipient will receive built-in directions on how to claim the money you've sent. You can add a personal message or even an electronic greeting card to accompany the money you're sending.

Receiving money is easy too

Suppose you're splitting a dinner check with friends. Instead of worrying about cash, change or multiple cards, you can send a text or e-mail prompting them to pay directly from their accounts.

They'll get your personal message, plus instructions for making a quick and easy electronic payment.

At TD Bank, person-to-person payments are easy and convenient.

Enroll today

You might also be interested in:

- Personal checking accounts
- Personal savings and money market accounts
- Mobile banking

Log in to Online Banking

Access your accounts anytime

Log in

Not enrolled? **Enroll Now**

View the demo

Person-to-Person Payments (Popmoney) are available for most personal checking and money market accounts. To use these services you must have an Online Banking profile with a U.S. address, a unique U.S. phone number, an active unique e-mail address, and a Social Security Number. Your eligible personal deposit account must be active and enabled for ACH transactions and Online Banking transfers. Fees may apply depending on delivery options.

EXHIBIT
K-51

For more information, read the Terms & Conditions.

Person-to-Person Payments are only available in English in secure Online Banking at this time.

U.S. Bank Contour® Card

Order online
Purchase at a U.S. Bank Branch
Log In to your Card Account

Put more time into your life and more life into your money with Contour! No bank account or credit check is required to enroll[1], and since spending is limited to the amount of money deposited to the card, you can't incur overdraft fees.

Simple to Use

Shop everywhere Visa® Debit Cards are accepted.
Pay bills online at merchant websites, over the phone or in person.
Add a joint account and up to 5 sub account for others in your life or to help you budget.
Make free cash withdrawals at U.S. Bank and MoneyPass® ATMs.

Easy to Add Money

Free cash deposits at any U.S. Bank branch.
Free direct deposit of your payroll or government benefits check for instant access to your money. View Visa's direct deposit video.
Add funds to your card at any Visa ReadyLink location.

Smart Tools

Sign up online for free text and email alerts (remember that standard messaging charges may apply from your mobile carrier).
Free online account management.

Contour is a great payment solution to help meet your financial needs. Purchase your reloadable card today at any **U.S. Bank branch** or **online** for just $4.00. No minimum balance is required[2].

The Contour Card is issued by U.S. Bank National Association pursuant to a license from Visa. U.S.A., Inc. Member FDIC © 2013 U.S. Bank.

1. Successful identity verification required. To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. If necessary, we may also ask to see your driver's license or other identifying documents.

   Back to Text

2. Monthly service fee and other fees may apply. See **cardholder agreement and fee schedule** for details.

   Back to Text

Contact Us

Visit Us: Find a Branch
Call Us: 800-720-BANK

Manage Your Prepaid Card

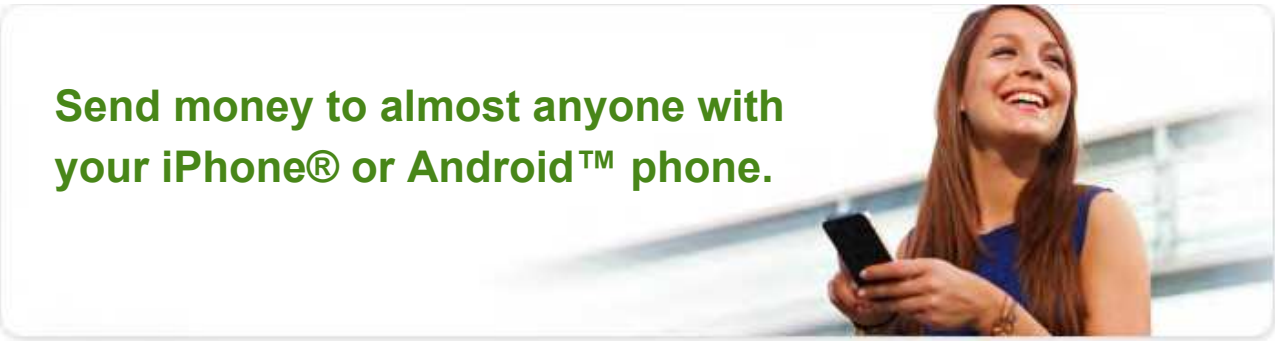
U.S. Bank Contour Account
U.S. Bank Visa Gift Card Account

EXHIBIT
K-52

© 2015 U.S. Bank National Association.

Send Money

- MOBILE BANKING
- MOBILE INVESTING
- MOBILE INSURANCE
- AUTO ON THE GO
- PROPERTY
- ACCESS METHODS



How It Works | Member Reviews

Send money securely from your mobile phone.

This innovative feature lets you send money to a person or business using just your mobile phone.

- No trips to the bank or ATM.
- No check writing.
- No revealing of sensitive bank account information.

"Send Money" is available exclusively on the USAA Mobile Apps for iPhone and Android.

EXHIBIT
K-53

Sending money is easy ...

1. **Tell us how much to send and who to send it to.**
   Use the USAA Mobile App to enter the recipient's email address or mobile phone number as well as the amount you want to send domestically.

2. **Your recipient gets the money instantly.**
   If your recipient is a USAA Bank member, use the phone number or email address that they have on file with USAA and we'll deposit the funds directly into their account. Then we'll let them know by email or text.

   For money sent to anyone else, PayPal will send an email or text to your recipient letting them know their money is available. They can log on to their existing PayPal account or set one up for free to get the money. It's available immediately. (They don't have to have a PayPal account before you send the money.)

   PayPal recipients have the option of transferring the funds to their bank account, requesting a check or spending the money with thousands of online merchants that accept PayPal.

   » USAA Federal Savings Bank Send Money Service Agreement

Download our App

Get the right app for your smart phone.

Learn More

Explore mobile.usaa.com

Text the word "mobile" to **MyUSAA (698722)** and we'll send you a link to mobile.usaa.com

We can't send to international numbers,
including Puerto Rico and Canada.

Sign Up for Text Messaging

Get instant account information and transfer funds with a simple text message.

Sign Up and Manage

Share. Connect. Explore.
Visit the Member Community.

Switch to mobile site

Copyright © 2015 USAA.

System availability, account access and trade executions may vary due to network availability, market volatility and other factors.

Investments/Insurance: Not FDIC Insured • Not Bank Issued, Guaranteed or Underwritten • May Lose Value

USAA means United Services Automobile Association and its insurance, banking, investment and other companies. Banks Member FDIC. Investments provided by USAA Investment Management Company and USAA Financial Advisors Inc., both

registered broker dealers.

The trademarks, logos and names of other companies, products and services are the property of their respective owners.

Your phone carrier's data charges may apply.

209488-1014
691770

About Our Ads

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

Intrust Financial Corporation, Opposer, v. nTrust Corp., Applicant.	))))))))))	Opposition No. 91204456 Application Serial No.: 85/250992 Mark: NTRUST

Opposer's Second Rebuttal Notice of Reliance

Opposer Intrust Financial Corporation ("Intrust"), pursuant to 37 C.F.R. §§ 2.121 and 2.122 of the Trademark Rules of Practice, hereby gives notice that it introduces as evidence and intends to rely upon the documents and testimony identified herein, true and accurate copies of which are filed herewith and incorporated as Exhibits L-1 through L-21. Nothing submitted herein concedes any point or waives any rights or arguments of Opposer concerning the admissibility of any documents or testimony submitted by Applicant.

Except where expressly noted, the internet materials attached hereto display the date accessed and printed and the source URL in accordance with Trademark Rules and *Safer, Inc. v. OMS Investments, Inc*., 94 U.S.P.Q.2d 1031, 1039 (Trademark Tr. & App. Bd. Feb. 23, 2010). Exhibits L-1 through L-3 and L-20 through L-21 are additionally admissible as website printouts of government reports, which are self-authenticating. *Safer*, U.S.P.Q.2d at 1039; 37 C.F.R. § 2.122(e).

Rebuttal Trademark Registrations

Exhibits L-1 through L-3 are records from the United States Patent and Trademark Office that show that the Entrust Administration, Inc., Entrust Bankcard, and NTrust Wealth Management

trademarks are dead or abandoned. These Exhibits are offered in rebuttal to those offered by Applicant as Exhibits I-14, J-4 through J-5, J-8 through J-10, and J-20 through J-21.

Rebuttal Websites

Exhibits L-4 through L-19 are offered in rebuttal to the exhibits offered by Applicant through Categories I and J. These materials constitute web pages from entities identified in Applicant's Categories I and J, and are relevant to show how the appearance, services, trade channels, customer base, and/or markets of these entities distinguish them from Intrust, or to show that the entity no longer operates or maintains a website or web presence.

Rebuttal Secretary of State Registrations

Exhibits L-20 and L-21 are printouts from websites operated by the California Secretary of State and the Massachusetts Secretary of State. Exhibit L-20 shows that MTrust Networks, Inc. has surrendered its business status. This is relevant to show that the entity identified in Applicant's Exhibit I-12 is no longer in operation. Exhibit L-21 shows that in addition to having an expired service mark registration, NTRUST FINANCIAL is not licensed to operate in the state in which it obtained a service mark registration. *See* Applicant's Exhibit I-13.

Respectfully submitted,

Dated: April 17, 2015

Michael J. Norton, KS #18732
William P. Matthews, KS #18237
FOULSTON SIEFKIN LLP
1551 N. Waterfront Parkway, Suite 100
Wichita, Kansas 67206-4466
Telephone: 316-291-9743
Facsimile: 866-346-2031
Attorneys for Opposer

Certificate of Service

I certify that a copy of **Opposer's Second Rebuttal Notice of Reliance** was sent via email to counsel of record as follows:

James D. Nguyen
JimmyNguyen@dwt.com
Davis Wright Tremaine LLP
Suite 2400
865 S Figueroa Street
Los Angeles CA 90017
Attorney for Applicant

on this 17th day of April, 2015.

Michael J. Norton, KS #18732

United States Patent and Trademark Office

Home | Site Index | Search | FAQ | Glossary | Guides | Contacts | eBusiness | eBiz alerts | News | Help

Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Mon Apr 13 03:21:44 EDT 2015

TESS Home | New User | Structured | Free Form | Browse Dict | SEARCH OG | Bottom | HELP

Logout Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

TSDR | ASSIGN Status | TTAB Status ***(Use the "Back" button of the Internet Browser to return to TESS)***

Entrust Administration, Inc.

Word Mark	**ENTRUST ADMINISTRATION**, INC.
Goods and Services	(CANCELLED) IC 036. US 100 101 102. G & S: Financial services, namely, third party management and record keeping of self-directed tax-deferred or tax-free retirement plans, retirement accounts, and trusts. FIRST USE: 19920500. FIRST USE IN COMMERCE: 19920500
Mark Drawing Code	(3) DESIGN PLUS WORDS, LETTERS, AND/OR NUMBERS
Design Search Code	26.09.02 - Plain single line squares; Squares, plain single line 26.09.12 - Squares with bars, bands and lines 26.09.21 - Squares that are completely or partially shaded 26.11.12 - Rectangles with bars, bands and lines 26.11.13 - Rectangles (exactly two rectangles); Two rectangles 26.11.16 - Rectangles touching or intersecting 26.11.21 - Rectangles that are completely or partially shaded
Trademark Search Facility Classification Code	NOTATION-SYMBOLS Notation Symbols such as Non-Latin characters,punctuation and mathematical signs,zodiac signs,prescription marks SHAPES-BAR-BANDS Designs with bar, bands or lines SHAPES-GEOMETRIC Geometric figures and solids including squares, rectangles, quadrilaterals and polygons
Serial Number	78209669
Filing Date	January 31, 2003
Current Basis	1A
Original Filing Basis	1A
Published for Opposition	August 28, 2007
Registration Number	3334386
	November 13, 2007

EXHIBIT L-1

Registration Date	
Owner	(REGISTRANT) Entrust Administration, Inc. CORPORATION CALIFORNIA 555 12th Street, Suite 1250 Oakland CALIFORNIA 94607 (LAST LISTED OWNER) THE ENTRUST GROUP, INC. CORPORATION DELAWARE 555 12TH STREET SUITE 1250 OAKLAND CALIFORNIA 94607
Assignment Recorded	ASSIGNMENT RECORDED
Attorney of Record	Nicole H. Chiu
Disclaimer	NO CLAIM IS MADE TO THE EXCLUSIVE RIGHT TO USE "ADMINISTRATION, INC." APART FROM THE MARK AS SHOWN
Description of Mark	Color is not claimed as a feature of the mark. The lining in the drawing is a feature of the mark and does not indicate color.
Type of Mark	SERVICE MARK
Register	PRINCIPAL
Live/Dead Indicator	DEAD
Cancellation Date	June 20, 2014

United States Patent and Trademark Office

Home | Site Index | Search | FAQ | Glossary | Guides | Contacts | eBusiness | eBiz alerts | News | Help

Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Mon Apr 13 03:21:44 EDT 2015

TESS Home | New User | Structured | Free Form | Browse Dict | SEARCH OG | Bottom | HELP

Logout Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

TSDR | ASSIGN Status | TTAB Status ***(Use the "Back" button of the Internet Browser to return to TESS)***

ENTRUST BANKCARD

Word Mark	**ENTRUST BANKCARD**
Goods and Services	(ABANDONED) IC 009. US 021 023 026 036 038. G & S: Magnetic coded gift cards. FIRST USE: 20101116. FIRST USE IN COMMERCE: 20101116 (ABANDONED) IC 035. US 100 101 102. G & S: Incentive award programs to promote the sale of products and services of others. FIRST USE: 20101116. FIRST USE IN COMMERCE: 20101116 (ABANDONED) IC 036. US 100 101 102. G & S: Credit and debit card payment processing services; Financial transaction services, namely, providing secure commercial transactions and payment options using a mobile device at a point of sale; Loyalty program payment processing services. FIRST USE: 20101116. FIRST USE IN COMMERCE: 20101116
Mark Drawing Code	(3) DESIGN PLUS WORDS, LETTERS, AND/OR NUMBERS
Design Search Code	26.17.01 - Bands, straight; Bars, straight; Lines, straight; Straight line(s), band(s) or bar(s) 26.17.05 - Bands, horizontal; Bars, horizontal; Horizontal line(s), band(s) or bar(s); Lines, horizontal 27.03.01 - Geometric figures forming letters, numerals or punctuation
Serial Number	85277145
Filing Date	March 25, 2011
Current Basis	1A
Original Filing Basis	1A
Owner	(APPLICANT) Entrust Companies, LLC LIMITED LIABILITY COMPANY ARIZONA 1255 West Baseline Road, Suite A200 Mesa ARIZONA 85202
Attorney of Record	Danielle D. Janitch
Description of Mark	Color is not claimed as a feature of the mark. The mark consists of the words ENTRUST BANKCARD. The letter "E" in the word ENTRUST is stylized in the form of three horizontal lines

EXHIBIT L-2

	and the TRUST portion of the word appears in bold font. The word BANKCARD appears in smaller letters beneath the TRUST portion of ENTRUST.
Type of Mark	TRADEMARK. SERVICE MARK
Register	PRINCIPAL
Live/Dead Indicator	DEAD
Abandonment Date	March 12, 2013

United States Patent and Trademark Office

Home | Site Index | Search | FAQ | Glossary | Guides | Contacts | eBusiness | eBiz alerts | News | Help

Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Mon Apr 13 03:21:44 EDT 2015

TESS Home | New User | Structured | Free Form | Browse Dict | SEARCH OG | Bottom | HELP

Logout Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

TSDR | ASSIGN Status | TTAB Status ***(Use the "Back" button of the Internet Browser to return to TESS)***

Word Mark	**NTRUST WEALTH MANAGEMENT**
Goods and Services	(ABANDONED) IC 036. US 100 101 102. G & S: Financial services, namely, financial research and analysis; insurance information and consultancy; insurance brokerage; investment consultation, advice, and management; financial planning; account and investment administration; mortgage planning; financial planning for retirement; financial administration of retirement plans. FIRST USE: 20090529. FIRST USE IN COMMERCE: 20090529
Mark Drawing Code	(3) DESIGN PLUS WORDS, LETTERS, AND/OR NUMBERS
Design Search Code	07.03.09 - Lighthouses 26.01.29 - DNA helix; Helixes
Serial Number	77781329
Filing Date	July 15, 2009
Current Basis	1A
Original Filing Basis	1A
Owner	(APPLICANT) At the Beach Inc. CORPORATION VIRGINIA 780 Lynnhaven Parkway, Suite 190 Virginia Beach VIRGINIA 23452
Attorney of Record	Peter A. Shaddock II
Description of Mark	The color(s) red and blue is/are claimed as a feature of the mark. The mark consists of an image of a lighthouse having a helix of blue stripes adjacent the words "NTRUST" and "WEALTH MANAGEMENT", wherein the letter "N" in "NTRUST" and the words "WEALTH MANAGEMENT" appear in blue and the letters "TRUST" in "NTRUST" appear in red.
Type of Mark	SERVICE MARK
Register	PRINCIPAL
Live/Dead Indicator	DEAD

EXHIBIT L-3

Abandonment Date April 19, 2010

Contact Us

Contact Information

Speak With An Advisor:
(805) 371-8020

How can we help you?

Alliance Entrust
3390 Auto Mall Drive
Westlake Village, CA 91362

Phone
805.371.8020

Fax
805.371.8008

Email
info@allianceadvisory.com

©2011 **Alliance Entrust.** Alliance Entrust® is a Trademark of Alliance Advisory & Securities, Inc. A Registered Investment Advisor/Member FINRA & SIPC

Alliance Entrust
3390 Auto Mall Drive
Westlake Village, CA 91362
O: (805) 371-8020
F: (805) 371-8008

EXHIBIT
L-4

The Entrust Group myDirection Card

Already a card holder? Log into your account

ALL NEW - Introducing The Entrust Group myDirection Visa® Prepaid Cards For Self-Directed Investors and Retirees

Investors

The Entrust Group myDirection Card for Asset Management

Highlights

- Lower the cost of maintaining your assets
- Eliminate check request fees
- Make deposits or purchases on the spot

EXHIBIT
L-5

- Pay for IRA-owned asset maintenance, such as property taxes, property management fees, and upgrades
- Report self-directed IRA transactions online

Learn More

Retirees

The Entrust Group myDirection Card for Distributions

Highlights

- Save money by eliminating check request fees
- Take your distributions without hassle and skip all the paperwork
- Your retirement funds are automatically added to your card
- Use your card in the U.S. or abroad; anywhere Visa® debit cards are accepted
- Convenient support, 24/7

Learn More

©2015 The Entrust Group, Inc.. All rights reserved.
555 12th Street, Suite 1250 Oakland, CA 94607

Disclaimer | Privacy | Sitemap

The Entrust Group myDirection Card

Already a card holder? Log into your account

The Entrust Group myDirection Visa® Prepaid Card
The card for self-directed investors.

One card, many benefits. Discover The Entrust Group myDirection Card for self-directed investors.

Invest online:
The Entrust Group myDirection Card gives you instant access to your Entrust account funds. You can use the card to purchase investments such as stocks, bonds, and precious metals online.

Make faster investment transactions:
Purchase tax liens or make a deposit on real estate on the spot. You can invest when and where you want with a swipe of your card.

Save money on transactions:
You no longer need to request a check be mailed to you or a vendor. You can automatically add funds to your card and pay your vendors.

Request a card today!

Existing Entrust Client > New to Entrust >

EXHIBIT
L-6

Frequently Asked Questions

Download our frequently asked questions guide to help you gain a better understanding of The Entrust Group myDirection Card. Discover the full benefits and how you can make the most of your retirement savings.

Download Now

An Innovative Way to Direct Your Future™

- Low $3.00 monthly maintenance fee
- One-time only set-up fee of $25.00
- Automatically add funds to your card
- Convenient support, 24/7
- Online account access

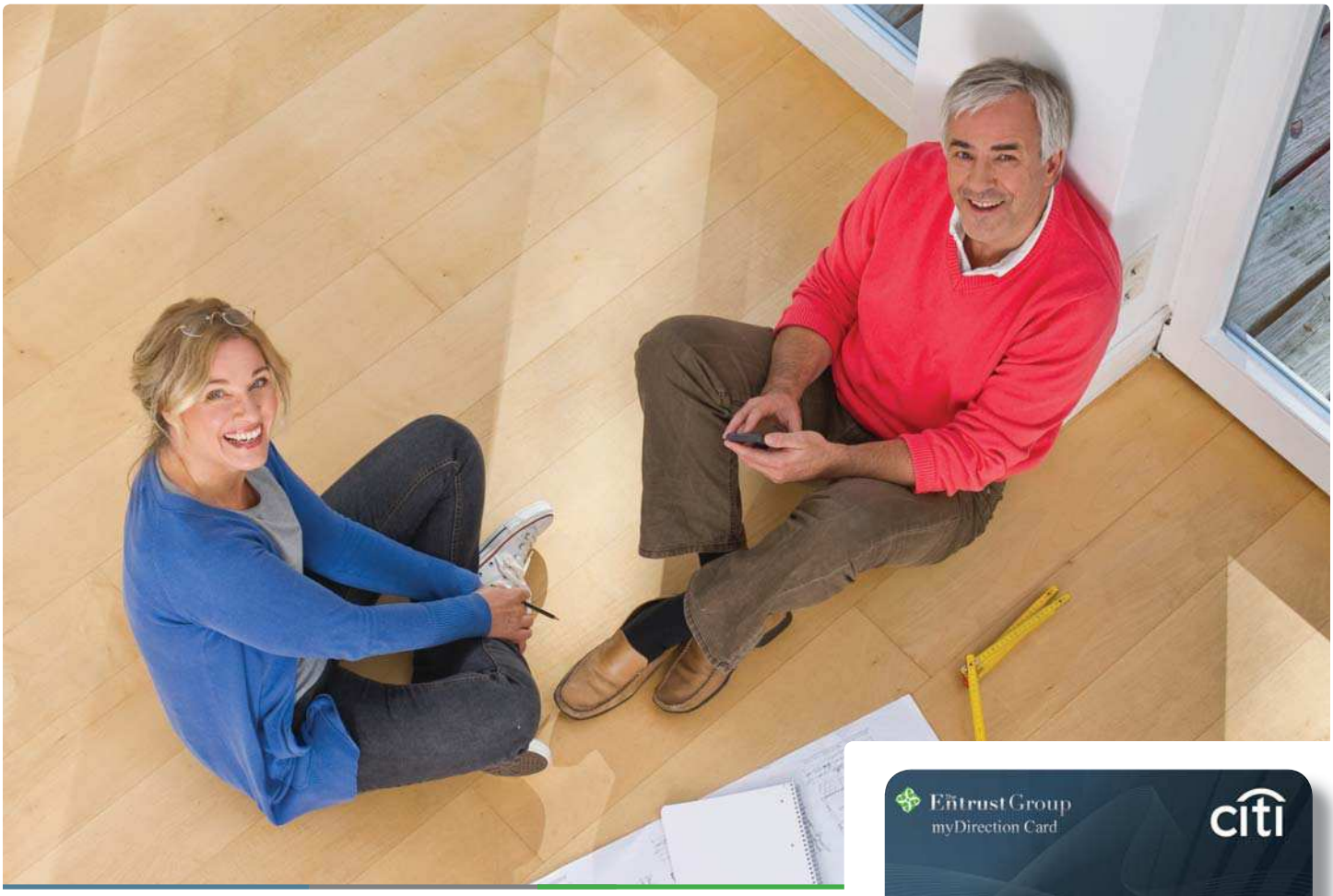
Available for IRAs, ESAs, and HSAs.

©2015 The Entrust Group, Inc.. All rights reserved.
555 12th Street, Suite 1250 Oakland, CA 94607

Disclaimer | Privacy | Sitemap

The Entrust Group

Direct Your Future™



The Entrust Group myDirection Visa® Prepaid Card

Asset Transaction Card FAQs

EXHIBIT
L-7

Cards are issued by Citibank, N.A. pursuant to a license from Visa U.S.A. Inc. and managed by Citi Prepaid Services. This card can be used everywhere Visa debit cards are accepted.

TheEntrustGroup.com/myDirection

Asset Transaction Card FAQs

General

1. Is an Entrust account required to request The Entrust Group myDirection Card?

Yes. The Entrust Group myDirection Card must be linked to an Entrust account. If you do not have an account, you can open one at TheEntrustGroup.com, or by calling 800-392-9653.

2. How do I request The Entrust Group myDirection Card?

Complete The Entrust Group myDirection Visa® Prepaid Card Application. Use this form to request the card and indicate the initial amount you would like to transfer to your card ($100 minimum).

3. How long does it take to receive The Entrust Group myDirection Card?

It takes 7-10 business days to receive The Entrust Group myDirection Card. You must have an open and funded Entrust account before the card can be ordered.

4. Can the card be sent to any address I request?

The Entrust Group myDirection Card will be sent to the address indicated on the The Entrust Group myDirection Visa® Prepaid Card Application. For security purposes, the address indicated must match an address on file with Entrust and must be a United States address. Due to banking regulations, cards cannot be shipped overseas, though they can be used anywhere Visa® Debit cards are accepted.

5. What is the maximum value The Entrust Group myDirection Card can have?

Currently, for security purposes to protect your account from loss, twenty-five thousand dollars ($25,000) is the maximum value allowed on The Entrust Group myDirection Card. In certain circumstances, exceptions can be made. Please contact Entrust for any card limit exceptions.

6. Do the funds on The Entrust Group myDirection Card ever expire?

No. The funds will remain on your The Entrust Group myDirection Card and are considered part of your account assets until they are used. Any The Entrust Group myDirection Card transactions not completed before midnight (PST) on December 31 of the respective year will be counted towards the following year.

7. Is there a limit on the number of times I can transfer funds to The Entrust Group myDirection Card?

No. You can transfer funds to The Entrust Group myDirection Card as often as you would like, using The Entrust Group myDirection Visa® Prepaid Card Maintenance Form. Please keep in mind that your request to add funds to The Entrust Group myDirection Card must be completed through Entrust.

8. Can I use The Entrust Group myDirection Card for a rollover or transfer?

No. You cannot make rollover or transfer contributions directly to The Entrust Group myDirection Card. All monies must be deposited to Entrust for the benefit of your account, and then may be transferred to your card.

Asset Transaction Card FAQs

General

9. What would constitute a Prohibited Transaction using The Entrust Group myDirection Card?

Some types of transactions violate the basic intent of your account. Transactions that can be interpreted as providing immediate financial gain to the account holder or other disqualified parties are not allowed. The Entrust Group myDirection Card protects you from unknowingly conducting a prohibited transaction because all transactions are considered distributions, until or unless you provide information that the purchase was for the benefit of the account. If you have provided information that the purchase was for an asset or improvement of an existing asset within the account, and the purchase is actually for personal use, this could be considered a prohibited transaction. Entrust will rely on the information and documentation you provide within the specified time limits, as well as your guarantee that you have not committed a prohibited transaction.

Using Your Card

1. Does The Entrust Group myDirection Card have daily limits?

Yes. The Entrust Group myDirection Card has a daily ATM limit of $1,000 per business day for domestic and international withdrawals. For point of sale purchases, the daily limit is $10,000. Please see The Entrust Group myDirection Visa® Prepaid Card Application for all applicable limits. To fund a large transaction above the daily limit, please contact Entrust in advance.

2. What can I use The Entrust Group myDirection Card for?

The Entrust Group myDirection Card can be used to purchase assets, goods, and services for the IRA, ESA, or HSA.

Example: Asset purchase - You can purchase tax liens at auction using your card.

Example: Purchase assets or services for your account - Your account owns real property. The property may need a repair. It is necessary to use the account's funds for the repair. The Entrust Group myDirection Card is a way to access the cash in the account to pay for the supplies and labor associated with the improvements or repairs to the property.

3. Can The Entrust Group myDirection Card be used for PIN based transactions at a point of purchase?

No. The Entrust Group myDirection Card needs to be used as signature based (sign a receipt) for all transactions. You must use the "Credit" button at a point of sale. The "Debit" button will decline the transaction. Your PIN can only be used at ATMs.

4. Can I use The Entrust Group myDirection Card in another country?

Yes. You can use The Entrust Group myDirection Card wherever Visa® debit cards are accepted. You can also use it at any ATM worldwide.

5. Are there fees associated with The Entrust Group myDirection Card?

Yes. Please see The Entrust Group myDirection Visa® Prepaid Card Application for all applicable fees.

6. Can I use The Entrust Group myDirection Card to spend more money than I have in my account?

No. The Entrust Group myDirection Card does not have overdraft or credit privileges. The amount that you can spend using the card will be limited to the amount of money that you transfer from the undirected cash in your account to your card. This may not exceed the amount of available funds within your account. There is a fee for a declined transaction. Please see The Entrust Group myDirection Visa® Prepaid Card application for all applicable fees.

Asset Transaction Card FAQs

Maintaining Your Card

1. Can I view my balance and transaction history online?

Yes. For balance and transaction information, please visit TheEntrustGroup.com/myDirection.

2. How are transactions with The Entrust Group myDirection Card reported?

All transactions using The Entrust Group myDirection Card are considered a distribution until they are certified online or the proper documentation is submitted to Entrust verifying or validating the transaction was for the benefit of your Entrust account. You have 30 days to certify the transactions online or to complete and submit The Entrust Group myDirection Visa® Prepaid Card Transaction Form.

3. Can I use The Entrust Group myDirection Card to maintain assets that are not owned 100% by my Entrust account?

Yes. However, the expense must be proportionate to the percentage of your Entrust account's ownership. Transactions will be recorded as being properly completed in this manner.

Example: Your Entrust Traditional IRA owns 50% of a property and you own the other 50% personally. A repair is needed and costs $1,000. You should use The Entrust Group myDirection Card to pay for $500 (50%), and personal funds to pay the remaining $500.

All transactions should be certified online accordingly. See question 4 below, for more information on certifying transactions.

4. What do I need to provide to ensure my purchase is not counted as a distribution, if the purchase is intended to be for the benefit of the account?

If your transaction is for the benefit of your Entrust account, you can certify the transactions online or by submitting the necessary paperwork (with receipts) to Entrust.

To certify the transactions online, visit TheEntrustGroup.com/myDirection and follow the steps below:

1. Log in to view your accounts.
2. Select the appropriate card (if applicable).
3. Type in the dollar amount that applies to your Entrust asset for each transaction.
4. Indicate if the asset is existing or new (if the transaction is a new asset, remember to complete the necessary Buy Direction Letter (BDL) and submit it to Entrust).
5. Select the asset the transaction applies to from the drop down menu.
6. Click the Transaction Certification Policy and then click SUBMIT.

To certify transactions via mail, fax, or email follow the steps below:

1. Complete and sign The Entrust Group myDirection Visa® Prepaid Card Transaction Form explaining the nature of the expenditure and how it relates to the asset(s) in your Entrust account.
2. Attach the sales receipt for the expenditure and the credit card slip with your signature. Retain a copy for your records.
3. Send these items to Entrust for review within 30 days of the transaction. If the information adequately demonstrates that the card use was for the benefit of the account or asset(s) held by the account, then the transaction will not be reported as a distribution.

Asset Transaction Card FAQs

Maintaining Your Card

If The Entrust Group myDirection Visa® Prepaid Card Transaction Form and accompanying documents are not submitted, or if they do not adequately reflect that the expenditure was for the benefit of your Entrust account, then Entrust will file reports with the IRS that show that the amount of the transaction was a distribution from your Entrust account. The amount distributed to you may be subject to taxes and/or penalties.

5. How do I add funds to my card?

To add funds to The Entrust Group myDirection Card, complete the The Entrust Group myDirection Visa® Prepaid Card Maintenance Form. Requests to add funds to your The Entrust Group myDirection Card can only be executed on business days, during regular business hours. Please allow up to two business days from the date of request before the changes are reflected on The Entrust Group myDirection Card.

6. Can I make deposits directly to The Entrust Group myDirection Card?

No. You cannot make deposits directly to The Entrust Group myDirection Card. All monies must be transferred from your Entrust account to your card.

7. Can I add personal funds to The Entrust Group myDirection Card?

No. You cannot commingle personal funds with funds on The Entrust Group myDirection Card.

8. Can the funds on The Entrust Group myDirection Card be transferred back to my Entrust account?

Yes. Complete The Entrust Group myDirection Visa® Prepaid Card Maintenance Form to transfer funds from The Entrust Group myDirection Card to your Entrust account. Once Entrust has confirmed the balance of the transfer and the balance on your card, the transfer will be processed.

9. Can I have more than one of my Entrust accounts linked to The Entrust Group myDirection Card?

No. To ensure proper record keeping and reporting, you will need one card for each Entrust account.

10. What should I do if my card is lost or stolen?

To report a lost or stolen card, call **Citibank at 877-855-7201**, 24 hours a day, 7 days a week.

11. What happens if I need to return an item I purchased with The Entrust Group myDirection Card?

You can return the item to the merchant it was purchased from. The merchant processes a credit adjustment and a credit will by applied to The Entrust Group myDirection Card. Cash refunds should not be given to you for purchases made with the myDirection Card. Receiving cash back from the merchant would be considered a distribution from your account. You will need to complete a The Entrust Group myDirection Visa® Prepaid Card Maintenance Form.

12. Can I customize my PIN number for ATM transactions?

Yes. Call the number listed on the sticker on the front your card to select your custom PIN. This PIN can only be used for ATMs.

Asset Transaction Card FAQs

Maintaining Your Card

13. What if I withdrew more money at the ATM than I intended?

If you withdrew more money than you intended, you will need to send a personal check along with the Entrust Rollover Certification Form* to deposit the funds into your Entrust account. Please visit our website at TheEntrustGroup.com for more information on rollovers.

14. How are the transactions listed online?

The transactions are listed in date order, with the newest transaction appearing first (on top). You will need to scroll or page to view older transactions. Please remember that transactions need to be certified within 30 days of the transaction date.

*Rollover rules apply.

The Entrust Group myDirection Card

Already a card holder? Log into your account

The Entrust Group myDirection Visa® Prepaid Card
The card for retirees.

Taking Distributions is Now as Easy as Swiping a Card

Save money with convenience

- No monthly fee
- No check request fees
- No set-up fee

Take your distributions without hassle

- No waiting for checks in the mail
- No more waiting in line at a bank
- No time-consuming paperwork

Benefits that provide peace of mind

- FDIC insured
- Automatically add funds to your card
- Convenient support, 24/7
- Online account access

Request a card today!

EXHIBIT
L-8

Existing Entrust Client >

New to Entrust >

Frequently Asked Questions

Download our frequently asked questions guide to help you gain a better understanding of The Entrust Group myDirection Card for retirees. Discover the full benefits of using The Entrust Group myDirection Card for taking distributions and how you can maximize your retirement.

Download Now

An Innovative Way to Direct Your Future™

- NO monthly fee
- NO set-up fee
- Automatically add funds to your card
- Convenient support, 24/7
- Online account access

This card is available for IRA, HSA or ESA distributions.

©2015 The Entrust Group, Inc.. All rights reserved.
555 12th Street, Suite 1250 Oakland, CA 94607

Disclaimer | Privacy | Sitemap

The Entrust Group

Direct Your Future™

The Entrust Group myDirection Visa® Prepaid Card

Distribution Card FAQs

EXHIBIT
L-9

Cards are issued by Citibank, N.A. pursuant to a license from Visa U.S.A. Inc. and managed by Citi Prepaid Services. This card can be used everywhere Visa debit cards are accepted.

TheEntrustGroup.com/myDirection

Distribution Card FAQs

General

1. Is an Entrust account required to request The Entrust Group myDirection Card?

Yes. The Entrust Group myDirection Card must be linked to an Entrust account. If you do not have an account, you can apply for one at TheEntrustGroup.com, or by calling 800-392-9653.

2. How do I request The Entrust Group myDirection Card?

Complete the The Entrust Group myDirection Visa® Prepaid Card Application. Use this form to request the card and the initial amount you would like to transfer to your card ($100 minimum). Visit TheEntrustgroup.com/myDirection for this form.

3. How long does it take to receive The Entrust Group myDirection Card?

It takes 7-10 business days to receive The Entrust Group myDirection Card. You must have an open and funded Entrust account before the card can be ordered.

4. Can the card be sent to any address I request?

The Entrust Group myDirection Card will be sent to the address indicated on the The Entrust Group myDirection Visa® Prepaid Card Application. For security purposes, the address indicated must match the address on file with Entrust and must be a United States address. Due to banking regulations, cards cannot be shipped overseas, though they can be used anywhere Visa® Debt cards are accepted.

5. What is the maximum value The Entrust Group myDirection Card can have?

Currently, for security purposes to protect your account from loss, twenty-five thousand dollars ($25,000) is the maximum value allowed on The Entrust Group myDirection Card. In certain circumstances, exceptions may be made. Please contact Entrust for any card limit exceptions.

6. Do the funds on The Entrust Group myDirection Card ever expire?

No. The funds will remain on The Entrust Group myDirection Card until they are used.

7. Is there a limit on the number of times I can transfer funds to The Entrust Group myDirection Card?

No. You can transfer funds to The Entrust Group myDirection Card as often as you would like, using The Entrust Group myDirection Visa® Prepaid Card Maintenance Form. Please keep in mind that your request to add funds to The Entrust Group myDirection Card must be completed through Entrust. There is no charge for transferring funds to your card.

8. Can I use The Entrust Group myDirection Card for a rollover or transfer?

No. The Entrust Group myDirection Card is for taking distributions from your Entrust account(s) only.

Distribution Card FAQs

General

9. Can I use The Entrust Group myDirection Card to satisfy my Required Minimum Distribution (RMD) for the year?

Yes. The Entrust Group myDirection Card can be used for RMDs or any other type of distribution.

10. What would constitute a prohibited transaction using The Entrust Group myDirection Card?

Since the funds are being distributed to you at the time they are credited to The Entrust Group myDirection Card, the IRA prohibited transactions rules do not apply.

Using Your Card

1. Does The Entrust Group myDirection Card have daily limits?

Yes. The Entrust Group myDirection Card has a daily ATM limit of $1,000 per business day for domestic and international withdrawals. For point of sale purchases, the daily limit is $10,000. Please see The Entrust Group myDirection Visa® Prepaid Card Application for all applicable limits. To fund a large transaction above the daily limit, please contact Entrust in advance.

2. Can The Entrust Group myDirection Card be used for PIN-based transactions at point of purchase?

No. The Entrust Group myDirection Card needs to be used as signature-based (sign a receipt) for all transactions. **You must use the "Credit" button at a point of sale. The "Debit" button will decline the transaction. Your PIN can only be used at ATMs.**

3. Can I use The Entrust Group myDirection Card in another country?

Yes. You can use The Entrust Group myDirection Card wherever Visa® debit cards are accepted. You can also use it at any ATM worldwide.

4. Are there fees associated with The Entrust Group myDirection Card?

Yes. Please see The Entrust Group myDirection Visa ®Prepaid Card Application for all applicable fees.

5. Can I use The Entrust Group myDirection Card to spend more money than I have in my account?

No. The Entrust Group myDirection Card does not have overdraft or credit privileges. The amount that you can spend using your card will be limited to the amount of money that you transfer from the undirected cash in your account to The Entrust Group myDirection Card. This may not exceed the amount of available funds within your account. There is a fee for a declined transaction. Please see The Entrust Group myDirection Visa® Prepaid Card Application for all applicable fees.

Distribution Card FAQs

Maintaining Your Card

1. How are transactions with The Entrust Group myDirection Card reported?

When your card is funded by your Entrust account, it is considered a distribution and is reported to the IRS. Since the funds are being distributed to you at the time they are credited to your card, the transactions do not need to be reported.

2. Can I view my balance and transaction history online?

Yes. For balance and transaction information, please login to TheEntrustGroup.com/myDirection.

3. How do I add funds to my card?

To add funds to The Entrust Group myDirection Card, complete The Entrust Group myDirection Visa® Prepaid Card Maintenance Form. Requests to add funds to The Entrust Group myDirection Card can only be executed on business days, during regular business hours. Please allow up to two business days from the date of request before the changes are reflected on The Entrust Group myDirection Card.

4. Can I make deposits directly to The Entrust Group myDirection Card?

No. You cannot make deposits directly to The Entrust Group myDirection Card. All monies must be transferred from your Entrust account to your card.

5. Can I add personal funds to The Entrust Group myDirection Card?

No. You cannot commingle personal funds with funds on The Entrust Group myDirection Card.

6. Can the funds on The Entrust Group myDirection Card be transferred back to my Entrust account?

No. Since the funds are being reported as a distribution, you cannot transfer them back to your Entrust account.

7. Can I have more than one of my Entrust accounts linked to The Entrust Group myDirection Card?

Since The Entrust Group myDirection Card is being used solely for distribution purposes, you may use one card for all Entrust accounts. The distribution requests will be reported to the IRS as such, and may or may not be taxable.

8. What should I do if my card is lost or stolen?

To report a lost or stolen card, call **Citibank at 877-855-7201**, 24 hours a day, 7 days a week.

9. What happens if I need to return an item I purchased with The Entrust Group myDirection Card?

You can return the item to the merchant it was purchased from. The merchant processes a credit adjustment and a credit will by applied to The Entrust Group myDirection Card.

10. Can I customize my PIN number for ATM transactions?

Yes. Call the number listed on the sticker on the front your card to select or change your PIN. This PIN can only be used at ATMs.

Merchant Login

To access your control panel, please enter your username and password in the fields below.

* Username

* Password

Login

EXHIBIT
L-10

The webpage cannot be found

HTTP 404

Most likely causes:

- There might be a typing error in the address.
- If you clicked on a link, it may be out of date.

What you can try:

- Retype the address.
- Go back to the previous page.
- Go to and look for the information you want.

More information

EXHIBIT
L-11

We provide world-class investment strategies tailored specifically for your lifestyle and support our recommendations with advanced planning.

Who Do We Help?

We limit our practice to successful women and their families for whom we can make a major impact.

Successful women today control more than half of the wealth in the world. And the wealth of these women is growing.

Successful women may have earned their wealth, they may have inherited their wealth, or they might have been awarded their wealth in a settlement. Successful women want to delegate the details of their financial security, so they can focus on what they love.

We partner with you using a consultative approach. We use a consultative approach to assure that we are doing the right thing for you. We want to be sure that you are comfortable every step of the way.

Entrust Financial, LLC®
Wayne, PA | Phone: 610-687-3515 | Fax: 610-687-3595
Serving in Pennsylvania: Montgomery, Chester, Philadelphia and Delaware Counties

Certified Financial Planner Board of Standards, Inc. owns the certification marks CFP®, CERTIFIED FINANCIAL PLANNER™ and federally registered CFP, which it awards to individuals who successfully complete initial and ongoing certification requirements. Disclosure (/disclosure/)

Certified Financial Planner Board of Standards, Inc

Portfolio Access
When you link to the websites provided here, you are leaving this site.

EXHIBIT
L-12

Charles Schwab & Co., Inc. (http://www.entrustfinancial.com/charles-schwab-co-inc/)

(https://investor.lincolninvestment.com/)

(https://www.netxinvestor.com/web/netxinvestor/login)

© Copyright 2015 Entrust Financial, All Rights Reserved

Contact us today and start the conversation.

Contact Us

To Discover How we Might Help You

Entrust Financial, LLC
West Valley Business Center
940 West Valley Road, Suite 1902
Wayne, PA 19087

610-687-3515 | 610-687-3595 (fax)
info@entrustfinancial.com
(mailto:info@entrustfinancial.com)

Fill out the form below and we will contact you shortly.

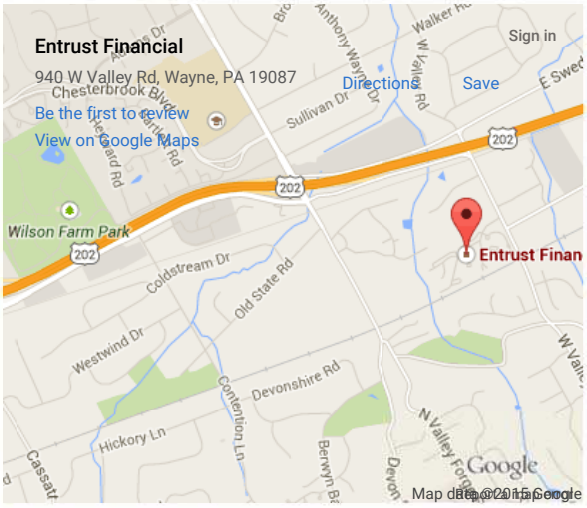
Name:*

Email:*

Phone:

Your Message:*

SUBMIT



View Larger Map (https://maps.google.com/maps?f=q&source=embed&hl=en&geocode=&q=Entrust+Financial,+940+West+Valley+Road,+Suite+1902,+Wayne,+PA+19087&ll=40.074.724323&sspn=7.455378,11.733398&t=m&ie=UTF8&hq=Entrust+Financial,+940+West+Valley+Road,+Suite+1902,+Wayne,+PA+19087&ll=40.075.434103&spn=0.01642,0.05064&z=14)

Directions To Our Office

From Philadelphia
I 76 West (the Schuylkill Expressway) past the Gulph Mills exit. The road soon widens to 4 lanes as it approaches the King of Prussia Mall. Note the signs for Pottstown/Swedesford Road; they will continue to draw you to the far right lane. Exit at the double lane with the Swedesford sign and remain in the right lane. As the highway widens, continue keeping to the right following the signs to exit at Swedesford Road.

As you approach the traffic light prepare to make a left turn on to Swedesford Road. You will encounter 4 more traffic lights, the last of which is West Valley Road—turn left. On your right, just past the U.S. Post Office & Processing Center—turn right at the West Valley Business Center. Bear right as you drive through the Center, and park as soon as you see the building marked 1900 –1902. That's us!

From the Southern and Western Suburbs
Proceed on I 476 (the Blue Route) and exit at I 76 West. Go past the Gulph Mills exit. The road soon widens to 4 lanes as it approaches the King of Prussia Mall. Note the signs for Pottstown/Swedesford Road; they will continue to draw you to the far right lane. Exit at the double lane with the Swedesford sign

EXHIBIT
L-13

and remain in the right lane. As the highway widens, continue keeping to the right following the signs to exit at Swedesford Road.

As you approach the traffic light prepare to make a left turn on to Swedesford Road. You will encounter 4 more traffic lights, the last of which is West Valley Road—turn left. On your right, just past the U.S. Post Office & Processing Center—turn right at the West Valley Business Center. Bear right as you drive through the Center, and park as soon as you see the building marked 1900 –1902. That's us!

From the Northern and Eastern Suburbs
Proceed on the Pennsylvania Turnpike and exit at Valley Forge. Choose a toll booth on the right because you will exit to the right soon after the toll. Note the signs for Pottstown/Swedesford Road; they will draw you to the right lane where you will use Exit 328A. As the highway widens, continue keeping to the right following the signs to exit at Swedesford Road.

As you approach the traffic light prepare to make a left turn on to Swedesford Road. You will encounter 4 more traffic lights, the last of which is West Valley Road—turn left. On your right, just past the U.S. Post Office & Processing Center—turn right at the West Valley Business Center. Bear right as you drive through the Center, and park as soon as you see the building marked 1900 –1902. That's us!

From West Chester and Downingtown
Access Route 202 North. When you enter the newly rebuilt section of 202, look for the exit marked Valley Forge Road/West Valley Road. DO NOT take the next exit marked South Valley Forge Road. In about 100 yards, exit at the sign marked North Valley Forge Road/West Valley Road. Move to the far right as you come down the exit ramp.

Turn right at the traffic light onto West Valley Road. On your right, just past the U.S. Post Office & Processing Center—turn right at the West Valley Business Center. Bear right as you drive through the Center, and park as soon as you see the building marked 1900–1902. That's us!

From Western Philadelphia (avoiding the expressway)
Haverford Avenue becomes Haverford Road when it crosses City Line and enters Montgomery County. Following Haverford Road, its name changes to County Line Road as you cross Bryn Mawr Avenue at the hospital. After you pass Bryn Mawr Hospital, the next traffic light presents a "half left" turn on to Conestoga Road. Follow Conestoga Road until you reach Lancaster Avenue (route 30.) Turn left.

Turn right at the very next traffic light on to Old Eagle School Road. Turn left at the next traffic light on to Upper Gulph Road. Be alert for an IMMEDIATE right turn (at the school building) onto West Valley Road. At the bottom of a long, winding hill there is a new bridge over a single track railroad. Make the first available left turn (after the bridge) at the sign for West Valley Business Center. Bear right as you drive through the Center. Park as soon as you see the building marked 1900–1902. That's us!

Entrust Financial, LLC®
Wayne, PA | Phone: 610-687-3515 | Fax: 610-687-3595
Serving in Pennsylvania: Montgomery, Chester, Philadelphia and Delaware Counties

Portfolio Access
When you link to the websites provided here, you are leaving this site.

Certified Financial Planner Board of Standards, Inc. owns the certification marks CFP®, CERTIFIED FINANCIAL PLANNER™ and federally registered CFP, which it awards to individuals who successfully complete initial and ongoing certification requirements. Disclosure (/disclosure/)

Certified Financial Planner Board of Standards, Inc

Charles Schwab & Co., Inc.
(http://www.entrustfinancial.com/charles-schwab-co-inc/)

LINCOLN INVESTMENT
(https://investor.lincolninvestment.com/)

PLATINUM SOLUTIONS
(https://www.netxinvestor.com/web/netxinvestor/login)

© Copyright 2015 Entrust Financial,
All Rights Reserved

SOCIALLY-CONSCIOUS INVESTMENT ADVISORY

EXHIBIT
L-14

INVESTMENT ADVISORY

INTRUST GLOBAL INVESTMENTS

WE ARE A SOCIALLY-CONSCIOUS INVESTMENT ADVISORY FIRM FOCUSED ON ENERGY AND INFRASTRUCTURE IN LATIN AMERICA. WE FORGE PARTNERSHIPS BETWEEN INVESTORS AND LATIN AMERICAN COMMUNITIES TO UNLEASH SHARED GROWTH.

FACTS ABOUT INTRUST GLOBAL INVESTMENTS

115
Projects in Pipeline

66
Communities Reached

140
Trained Universities

WHAT WE DO

WE ADVISE PUBLIC AND PRIVATE CLIENTS TO NAVIGATE INVESTMENT OPPORTUNITIES IN LATIN AMERICA'S RURAL AREAS. WE ALIGN INTERESTS OF INVESTORS AND INDIGENOUS COMMUNITIES WHERE WE WORK, UNLOCKING VALUE THROUGH ALLIANCES AND TRUST.

WHAT OUR ALLIES SAY

Nunc velit risus, dapibus non interdum quis, suscipit nec dolor. Vivamus tempor tempus mauris vitae fermentum. In vitae nulla lacus. Sed sagittis tortor vel arcu sollicitudin nec tincidunt metus suscipit.

— Tony Stark —

THE INDI FUND

INTRUST GLOBAL INVESTMENTS DEVELOPS THE INDI FUND, THE FIRST PRIVATE EQUITY FUND TO INVEST IN RENEWABLE ENERGY AND AGRIBUSINESS PROJECTS IN PARTNERSHIP WITH INDIGENOUS COMMUNITIES IN LATIN AMERICA. THE FUND'S OBJECTIVE IS TO ACHIEVE A TRIPLE BOTTOM LINE OF SUPERIOR FINANCIAL RETURNS, ALONGSIDE A POSITIVE ENVIRONMENTAL, AND SOCIAL IMPACT.

FOR MORE INFORMATION ON OUR SOCIAL IMPACT, VISIT THIS LINK.

Our Staff

MEET OUR TEAM

MANAGEMENT

ADVISORS

BOARD

WASHINGTON D.C.

1701 Pennsylvania Ave., NW, Suite 300, Washington D.C. 20006

Phone: 202-349-5559
Fax: 202 580 6559

NEW YORK

200 Park Avenue, Suite 1700, New York, NY 10166

Just Above Grand Central
Phone: 202-349-5559
Fax: 202 580 6559

MEXICO CITY

IZA BC Torre Vistral Piso 1, Av. Insurgentes Sur 730, Col. Del Valle, México D.F. 03104

Phone: +52-55-8000-8000

NEWS

HERE'S SOMETHING YOU CAN KNOW ABOUT WHAT WE ARE DOING AROUND LATELY.

A Smart Green Explorers Wheel: Empowering Innovative Local Communities

08 Apr

Co-authored by Julian Gresser, MA, JD and Francisco Acuna, MPA

InTrust's CEO remarks published in United Nations Book

15 Jan

January 2014 Francisco Acuña's remarks on sustainable energy projects where

Read More →

Mexican Tecnológicos and Clean Energy Agenda

14 Jan

Mexican Universities and InTrust Global Investments Cabo San Lucas, Mexico

Read More →

Read More →

CONTACT

WE'D REALLY LOVE TO HEAR FROM YOU SO WHY NOT DROP US AN EMAIL AND WE'LL GET BACK TO YOU AS SOON AS WE CAN.

Your Name

Your Email

Your Subject

Enter your message

FOLLOW US ON TWITTER

Happy NewYear to everyone! Feliz Año! This year will be a "transformational year" for our mission. Looking forward to working with you all!

Copyright InTrust Global Investments LLC 2015

OUR MISSION

FORGING PARTNERSHIPS BETWEEN INVESTORS AND RURAL MEXICAN AND LATIN AMERICAN COMMUNITIES TO UNLEASH SHARED GROWTH

Copyright InTrust Global Investments LLC 2015

EXHIBIT
L-15

THE SMART ALTERNATIVE

Today's investors are increasingly seeking new ways to expand their portfolios and diversify their investment holdings. Millennium Trust offers a wide range of products for individual investors including:

Self Directed IRAs
Solo 401(k)s

Millennium Trust custodies a broad range of asset choices, both alternative and traditional, to help you reach your investment objectives including building wealth for your retirement.

How can we help you?

Millennium Trust Company is an independent custodian serving the self directed retirement account market. We focus on providing custody services to individual accounts.

AUTOMATIC ROLLOVER IRA CLIENTS

If your company retirement plan recently rolled over your balance into a Millennium Rollover IRA, **click here** to learn more.

General Information

► **Important Notice** - New fee schedule effective January 1, 2015.

Year-End Reporting

Year-End/4th Quarter statements will be available by January 31, 2015
1099s (R, INT, DIV) will be mailed by February 2, 2015
1099-B will be mailed by February 17, 2015
5498 will be mailed by June 1, 2015 to those account holders who made a contribution for 2014

Client Service Hours
Monday - Friday
8:00 a.m. - 4:30 p.m. CT

Quick Links

Press Releases
Articles
Calendar of Events
Fact Sheets & White Papers
FAQs

Stay Connected

© 2011 Millennium Trust Company

EXHIBIT
L-16

Millennium Trust
About Us

LOCATION

Millennium Trust Company
2001 Spring Road, Suite 700
Oak Brook, IL 60523
630.368.5600

Millennium Trust is located 18 miles west of downtown Chicago at 2001 Spring Road, Oak Brook, IL. The reception to our offices is located on the 7th Floor. The facility includes 24-hour security features, including surveillance cameras.

VIEW MAP >

For directions, click on the view map button above.

General Information

Client Service Hours
Monday - Friday
8:00 a.m. - 4:30 p.m. CT

Quick Links

- Press Releases
- Articles
- Calendar of Events
- Fact Sheets & White Papers
- FAQs

Stay Connected

© 2011 Millennium Trust Company

EXHIBIT
L-17

Millennium Trust
About Us

CHOICE, EXPERTISE AND SERVICE

Millennium Trust Company is a leading financial services company offering niche alternative custody solutions to institutions, advisors and individuals. We serve as a complement to traditional services offered by other custodians. Our innovative solutions include rollover solutions, alternative asset custody, private fund custody and advisor support services. In every case, Millennium Trust offers a wide array of investment choices and the highest levels of expertise and service.

More Investment Choices: Alternatives to the Traditional

Millennium Trust is able to custody a broad range of alternative assets:

- Futures
- Hedge Funds
- Promissory Notes
- Real Estate
- Mortgages/Deed of Trust
- Precious Metals
- Private Equity
- Private Stock
- LPs/LLCs

We also custody traditional assets such as stocks, bonds, mutual funds, EFTs, and CDs.
We provide expanded FDIC insurance to $1 million on cash balances in IRAs through our Cash Sweep Program.

Expertise and Experience You Can Count On

- Experience in managing and servicing a variety of retirement and custody accounts
- Extensive expertise in the administration and custody of alternative assets
- Knowledgeable on regulatory and tax reporting requirements for IRAs and Employer Sponsored Retirement Accounts
- Well informed and abreast of IRS codes regarding alternative assets and how to process funds, expenses, reinvestments and distributions in accordance with these rules

General Information

Client Service Hours
Monday - Friday
8:00 a.m. - 4:30 p.m. CT

Quick Links

- Press Releases
- Articles
- Calendar of Events
- Fact Sheets & White Papers
- FAQs

Stay Connected

EXHIBIT
L-18

The Highest Level of Client Service

Tailored service solutions for individual clients and institutions through dedicated customer service teams available by phone, email, fax or in person
Best-in-class, state-of-the-art technology to document and record all account activity from inception to ongoing service and maintenance
Secure Web-based portal for easy account access
Educational resources for clients and advisors through seminars and Webinars

© 2011 Millennium Trust Company

About Nelnet

Why We Do What We Do: A Message from Mike Dunlap, Chairman of the Board

Personally I find that if I strive every day to fulfill a larger purpose—whether it is helping my kids, assisting associates and customers to reach their goals, or working toward serving a higher purpose—I find the most satisfaction. Our overall mission, to make educational dreams possible, falls into this category for me.

By helping people accomplish their educational goals instead of focusing on ourselves, we collectively have a huge impact on the quality of their lives, making the world a place where fulfilling dreams is possible. As we help families set up payment plans to better afford an education, support families' efforts to successfully plan for college, explain options to make it easier to pay back student loans, and simply answer questions, every interaction we have with customers impacts their educational experience, and I am proud to be a part of it.

I want to publicly thank all our associates for their hard work and dedication to our customers. It is making the world a much better place.

Who We Are and What We Do

With a #1 core value of focusing on the customer, we provide innovative educational services in loan servicing, payment processing, education planning, and asset management. These products and services help students and families plan, prepare, and pay for their education while making the administrative and financial processes more efficient for schools and financial organizations.

Headquartered in Lincoln, Nebraska, with other offices around the United States and Canada, we employ more than 2,250 associates who serve customers throughout the education life cycle.

Our Businesses

Specifically, we operate as four distinct business segments, with additional affiliated companies:

Who We Serve

Each of our business segments serves different customers, from students and parents to K-12 schools or colleges, to lenders and government.

We currently assist more than 5 million borrowers with their student loans, administer tuition payment plans for approximately 5,500 K-12 schools and colleges and universities, and process 6 million student inquiries about colleges annually.

But, no matter which kind of customer you are, you can know one thing is for sure—you are our #1 priority.

Mission and Core Values

Our Mission: Why We Exist
Making educational dreams possible by helping students, families, educational institutions, and organizations that serve them prepare for, deliver, and finance education and helping to manage the administrative burden of doing so.

Our Values: What We Believe In and How We Behave
Our core values have been and will continue to be:

- Customers are #1
- Create an environment in which associates can do what they do best
- Build a diversified education services company
- Maintain open, honest communication
- Give back to our communities

Vision: What We Want to Become
We want to be a leading diversified processing services company through our core service offerings including:

- Education loan financing and asset management
- Education loan servicing
- Payment, transaction, and operational processing
- Education planning and enrollment services

We strive to provide consistent, clear support for all of our customers. We focus strongly on our associates and community service, believing that, to be successful, it is essential to balance the needs of our four key stakeholders: customers, associates, shareholders, and the community.

EXHIBIT
L-19

Related Links

- Code of Conduct
- Our Culture
- Leadership and Board of Directors
- News
- Careers
- Investors

Nelnet Business Solutions
Reach across campus with our seamless commerce solution.

New to Nelnet?
Learn how to create an account, discover what to do next, and see how we'll work together.

Nelnet Diversified Solutions
Technologies developed for loan servicing, now available to the public.

Nelnet Enrollment Solutions
Helping students find the right schools and schools find the right students.

Nelnet Career Services
Getting job-seekers where they want to go.

Business Entities (BE)

Online Services
- **E-File Statements of Information for Corporations**
- **Business Search**
- **Processing Times**
- **Disclosure Search**

Main Page

Service Options

Name Availability

Forms, Samples & Fees

Statements of Information (annual/biennial reports)

Filing Tips

Information Requests (certificates, copies & status reports)

Service of Process

FAQs

Contact Information

Resources
- **Business Resources**
- **Tax Information**
- **Starting A Business**

Customer Alerts
- **Business Identity Theft**
- **Misleading Business Solicitations**

Business Entity Detail

Data is updated to the California Business Search on Wednesday and Saturday mornings. Results reflect work processed through Friday, April 10, 2015. Please refer to **Processing Times** for the received dates of filings currently being processed. The data provided is not a complete or certified record of an entity.

Entity Name:	MTRUST NETWORKS, INC.
Entity Number:	C3342134
Date Filed:	12/21/2010
Status:	SURRENDER
Jurisdiction:	DELAWARE
Entity Address:	228 HAMILTON AVE 3RD FL
Entity City, State, Zip:	PALO ALTO CA 94301
Agent for Service of Process:	LUBO POZGAY
Agent Address:	228 HAMILTON AVE 3RD FL
Agent City, State, Zip:	PALO ALTO CA 94301

* Indicates the information is not contained in the California Secretary of State's database.

- If the status of the corporation is "Surrender," the agent for service of process is automatically revoked. Please refer to California Corporations Code **section 2114** for information relating to service upon corporations that have surrendered.
- For information on checking or reserving a name, refer to **Name Availability**.
- For information on ordering certificates, copies of documents and/or status reports or to request a more extensive search, refer to **Information Requests**.
- For help with searching an entity name, refer to **Search Tips**.
- For descriptions of the various fields and status types, refer to **Field Descriptions and Status Definitions**.

Modify Search **New Search** **Printer Friendly** **Back to Search Results**

Privacy Statement | **Free Document Readers**
Copyright © 2015 California Secretary of State

EXHIBIT
L-20

Citizen Information Service

Commonwealth Museum

Corporations

- Filing Methods
- Filing by Subject
- **Search**
  - **Search the Corporate Database**
  - Search Corporation Card File
  - Search Corporate Rejected Filings
  - Search the UCC Database
  - Search the Liens Database
  - Search the Trademark Database
  - Search Name Reservations
  - Search E-Certificate Verification
- General Information
- Certificates and Certified Copies
- Services Offered

Elections and Voting

Lobbyist

Archives

Massachusetts Historical Commission

Public Records

Publications and Regulations / Bookstore

Registry of Deeds

Securities

State House Tours

Records Center

Regional Offices

Address Confidentiality

Corporations Division

Search for a business entity

Legal Information, Disclaimers, Policies **Search assistance. . .**

◉ **Search by entity name** (Company, LP, LLP, LLC, etc.)

Enter name: ntrust financial Search type: Begins with

○ **Search by an individual name** (Officer, Director, etc.) Search type: Begins with

First: Middle: Last:

○ **Search by Identification Number** Must be 9 digits

○ **Search by Filing Number**

Display number of items to view: 25 items per page

* No records found; try a new search using different criteria

Clear search fields **Search Corporations**

EXHIBIT
L-21

William Francis Galvin, Secretary of the Commonwealth of Massachusetts
Terms and Conditions

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

Intrust Financial Corporation,	)	
	)	
Opposer,	)	
	)	Opposition No. 91204456
v.	)	Application Serial No.: 85/250992
	)	Mark: NTRUST
nTrust Corp.,	)	
	)	
Applicant,	)	
	)	

Opposer's Third Rebuttal Notice of Reliance

Opposer Intrust Financial Corporation ("Intrust"), pursuant to 37 C.F.R. §§ 2.121 and 2.122 of the Trademark Rules of Practice, hereby gives notice that it introduces as evidence and intends to rely upon the documents and testimony identified herein, true and accurate copies of which are filed herewith and incorporated Exhibits M-1 through M-7. Nothing submitted herein concedes any point or waives any rights or arguments of Opposer concerning the admissibility of any documents or testimony submitted by Applicant. In accordance with Trademark Rules and *Safer, Inc. v. OMS Investments, Inc*., 94 U.S.P.Q.2d 1031, 1039 (Trademark Tr. & App. Bd. Feb. 23, 2010), all internet materials display the date accessed and printed and the source URL.

Deposition Exhibits

Exhibits M-1 through M-7 were used as exhibits during the deposition of Robert MacGregor, which took place on March 17, 2015. They are offered for impeachment of Mr. MacGregor and in rebuttal of Applicant's Exhibits. Exhibits M-1 through M-4 are printouts of the nTrust website. These exhibits are offered to the exhibits in Applicant's Category F in order to show that nTrust offers services that consumers would expect a bank to provide. They are also relevant to show the similarity in the appearance and the services offered by Intrust and

nTrust, and are offered to rebut exhibits in Applicant's Categories H and I, which Applicant contends are similarly-named entities but that, unlike nTrust, are distinguishable in appearance, services, trade channels, customer base, and/or markets. Exhibits M-5 through M-7 are articles containing quotes or interviews from Mr. MacGregor. In addition to the impeachment of Mr. MacGregor, they are offered to rebut the exhibits in Applicant's Category F, as they are relevant to show that money transmitter or money transfer services are part of the banking world, and that the financial services provided by nTrust include services provided by banks.

Respectfully submitted,

Dated: April 17, 2015

Michael J. Norton, KS #18732
William P. Matthews, KS #18237
FOULSTON SIEFKIN LLP
1551 N. Waterfront Parkway, Suite 100
Wichita, Kansas 67206-4466
Telephone: 316-291-9743
Facsimile: 866-346-2031
Attorneys for Opposer

Certificate of Service

I certify that a copy of **Opposer's Third Rebuttal Notice of Reliance** was sent via email to counsel of record as follows:

James D. Nguyen
JimmyNguyen@dwt.com
Davis Wright Tremaine LLP
Suite 2400
865 S Figueroa Street
Los Angeles CA 90017
Attorney for Applicant

on this 17th day of April, 2015.

Michael J. Norton, KS #18732

nTrust

nTrust Usage Fees

Aaland Islands

Δ π EXHIBIT 219
Deponent RM
Date 3/17/15 Rptr MW
WWW.DEPOBOOK.COM

Transfers | Cards | General Usage

Physical Card	PHP
Card & PIN Delivery	FREE
Online Purchase	FREE
POS Purchase	FREE
Activation	FREE
ATM Withdrawal (Domestic)	Security Bank - FREE Local PH ATM - 10.00
ATM Withdrawal (International)	300.00
POS Decline	None
ATM Decline	None
Balance Inquiry (Online)	FREE
Balance Inquiry (ATM)	Security Bank 0- FREE Local PH ATM - 1.00
Foreign Exchange charge	None
Replacement Card	150.00
Replacement PIN	50.00
Load Card from nTrust Account	1.9%
Dormant Card Fee (monthly, charged after 90 days)	FREE
Deactivate Card	None

Cloud Money™ Card	Classic	Lite
POS Transaction Fee	FREE	FREE
International POS Transaction fee	FREE	FREE
ATM Withdrawal Fee	$2.49	-
International ATM Withdrawal Fee	$3.99	-

EXHIBIT
M-1

ATM Decline Fee including International	$0.99	-
ATM Balance Inquiry Fee	$0.99	-
Foreign Currency Markup	2.99%	2.99%
Card Replacement	$10.00	$1.00
Replacement PIN Fee	$2.99	-
Load Card from nTrust Account	1.9%	1.9%
Cancellation Fee/Refund	$12.00	$12.00
Destroy Card	-	$1.00
Live Customer Support	FREE	FREE

Card Limits	Classic	Lite
Maximum Balance At Any Time	$5,000	$2,500
Maximum Value Per Cash Load	$2,500	$2,500
Minimum Value Per Load	$10	$10
Maximum Daily POS Purchase	$5,000	$2,500
Maximum POS Transaction	$5,000	$2,500
Maximum ATM Withdrawal	$1,000	-

© 2010 - 2015 nTrust Group | Read Disclaimer

nTrust

MasterCard

The nTrust Cloud Money™ Prepaid MasterCard® Classic

The Cloud Money™ Card Classic is a reloadable prepaid MasterCard® that gives you the freedom to spend at over 32 million MasterCard acceptance locations worldwide or withdraw cash from over one million ATMs in over 200 countries. The Cloud Money Card Classic is a safer, easier alternative to cash, whether you're at home or abroad.

Δ π EXHIBIT 220
Deponent RM
Date 3/17/15 Rptr. MW
WWW.DEPOBOOK.COM

Features

Easy to Use

Load or reload from your smartphone or computer and use to pay anywhere that displays the MasterCard® Acceptance Mark, in-person or online. Unload money back to your nTrust account at any time for free.

Secure

EXHIBIT
M-2

The Cloud Money™ Card Classic isn't connected to your bank account, so your identity and banking information remains separate and secu at all times. Just one more way to protect yourself and your money.

Spend Smarter

Pay with the speed and convenience of a credit card, without the interest rates and the debt. There's no risk of overspending, so sticking t budget is dead easy.

Fees

Request a card	$4.99 C
Load card from nTrust account	1.9
Unload card	FR
PIN Replacement	$2.99 C
ATM Withdrawal Fee	$2.49 C

nTrust is free to join

nTrust is a regulated Canadian company using the toughest global standards to protect your money

Sign Up

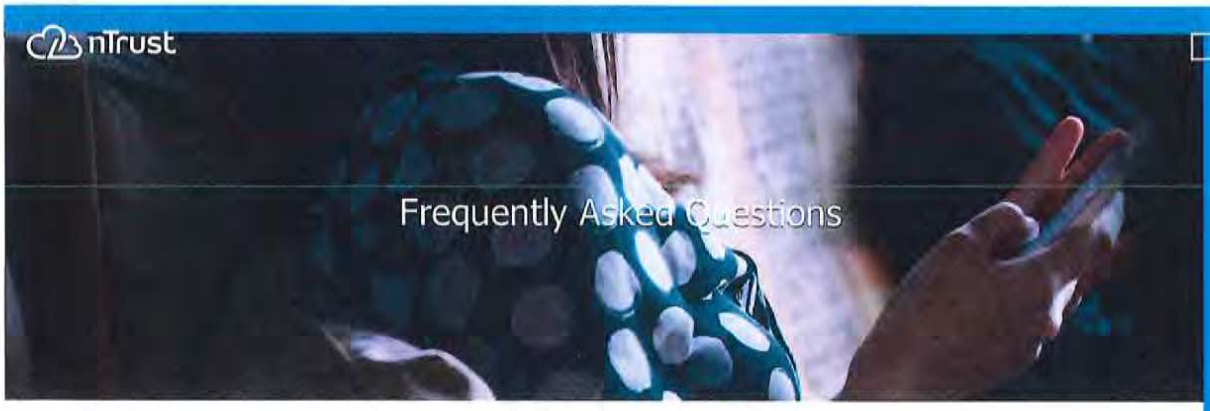
Features
Send Money
Cards
Pay Bills
Merchants

Company
Mission
FAQs
Charities
Help
Careers

Connect
Facebook
Twitter
Linkedin
Blog
Contact

Legal
Privacy Policy
Terms of Use

© 2010 - 2015 nTrust Group | Read Disclaimer



Q. Where is my money kept?

When you add money to your nTrust account, it's stored in a pooled account with a CDIC-insured financial institution, and kept separate from our operating funds.

Q. Is nTrust a bank?

No. nTrust works best for day-to-day transactions, like buying lunch, squaring up with a friend, or paying a bill. You don't need to move your life savings to nTrust, just enough to cover your daily expenses.

Q. Is nTrust available in my country?

Check here to see if nTrust is available in your region.

Q. Where is the nTrust Cloud Money™ Prepaid MasterCard® available?

Cloud Money™ Cards are currently only available in Canada and the Philippines. We're working on the rest!

Q. How do Cloud Money™ Cards work?

A Cloud Money™ Card is a prepaid MasterCard® you can load instantly with money from your nTrust account, and use to pay anywhere MasterCard® is accepted.
Learn more about cards.

Q. Is nTrust safe to use?

nTrust is as safe to use as any major online banking application.
Learn more about nTrust security.

Δ π EXHIBIT 221
Deponent RM
Date 3/17/15 Rptr. MW
WWW.DEPOBOOK.COM

Q. I need some help. How can I talk to a human?

If you would like to speak to a member services representative, please call:

Vancouver:
1-855-687-8788
Monday to Friday 9am to 5pm (PST)

Manila:
02-717-3700
Monday to Friday 8:30am to 5:30pm (PHT)

You can also send us an email and our member services team will get in touch with you. If you have a quick question, message us on Twitter or Facebook.

EXHIBIT
M-3

Features
Send Money
Cards
Pay Bills
Merchants

Company
Mission
FAQs
Charities
Help
Careers

Connect
Facebook
Twitter
Linkedin
Blog
Contact

Legal
Privacy Policy
Terms of Use

© 2010 - 2015 nTrust Group | Read Disclaimer

nTrust

Terms of Use

These Terms of Use ("Terms" or "Agreement") form a legally binding agreement between you and nTrust in relation to your use of the Services.

Latest Update: 18 June 2014

Δ π EXHIBIT 222
Deponent RM
Date 3/17/15 Rptr. MW
WWW.DEPOBOOK.COM

Latest Update: 18 June 2014

These Terms of Use ("Terms" or "Agreement") form a legally binding agreement between you and nTrust in relation to your use of the Services.

PLEASE READ THESE TERMS OF SERVICE CAREFULLY AS THEY CONTAIN IMPORTANT INFORMATION REGARDING YOUR LEGAL RIGHTS, REMEDIES AND OBLIGATIONS. You should you print off and/or save a copy of these Terms of Use for your records. Capitalized terms have the meanings attributed to them within the text or as provided in the "Definitions" section below.

1) APPLICATION AND ACCEPTANCE

1. Application. Unless otherwise agreed in writing with nTrust, these Terms apply to your use of the Services. You may not use the Services if you do not accept the Terms.
2. Acceptance. The Terms shall be deemed accepted by you upon the earlier of your: (i) creation of an Account; (ii) using the Services; or (ii) clicking to "accept" or "agree" or otherwise signifying your agreement when this option is made available to you in the course of accessing or registering for the Services.
3. Supplemental Terms. In the event that an additional Service is introduced or an existing Service is altered and supplementary terms and conditions of access or use are applicable, those additional terms ("Supplemental Terms") shall also apply. When Supplementary Terms apply to a specific Service, these may be accessible and/or presented to you within or prior to the use of such Service. These Terms shall continue to apply to such additional or altered Service and shall be deemed modified only to the degree they are in direct conflict with the Supplemental Terms, in which case the Supplemental Terms shall prevail.
4. Updates. nTrust may make changes to the Terms or Supplemental Terms from time to time, and nTrust will make a new version of the Terms available at in the "Legal Agreements" section of the Site. Any new Supplemental Terms may be made available to you from within, or through, the applicable Services. You understand and agree that you are responsible for periodically checking to determine whether the Terms or Supplemental Terms have been updated and, in any event, that if you use the Services after the date on which the Terms or Supplemental Terms have changed, you are deemed to have affirmatively accepted the updated Terms and/or Supplemental Terms. When nTrust posts changes to the Terms, the "Latest Update" date at the top of Terms will be updated.
5. Entire Agreement. The Terms (including the Privacy Policy and any Supplemental Terms) constitute the whole legal agreement between you and nTrust and govern your use of the Services (but excluding any services which nTrust may provide to you under a separate written agreement), and completely replace any prior agreements between you and nTrust in relation to the Services. These Terms and all representations, obligations, undertakings and warranties contained in it shall enure for the benefit of any successor and/or assignees of nTrust.

2) ELIGIBILITY

1. Minimum Age. You must be at least eighteen (18) years old to use the Services. Any registration, use of or access to the Services by anyone under 18 is unauthorized, unlicensed, and in violation of these Terms.
2. Legally Capable of Contracting and Receiving Services. Without limiting the foregoing, you may not use the Services and may not purport to accept the Terms if you are not of legal age to form a binding contract with nTrust, or are otherwise precluded from using or receiving such Services under the laws of the Jurisdiction or other countries, including the country in which you are resident or from which you intend to use or access the Services.
3. Your Representation and Warranty. You expressly represent and warrant that then you are at least eighteen (18) years of age and do not require the consent, approbation or approval of any other person or entity to conclude a contractual obligation of the type represented in these Terms.
4. Access to Services Conditional. We may terminate your Account and/or prohibit you from using or accessing the Service (or any portion, aspect or feature of the Service) for any reason, at any time in its sole discretion, with or without notice, including without limitation if we believes that you are under 18 or are otherwise ineligible to use the Services pursuant to these Terms.

EXHIBIT
M-4

3) ACCOUNTS

1. Single User Account. In order to use Services, you must register an nTrust account through the Site ("Account"). An individual User may only have one Account at a time.
2. Account Security. You agree and understand that you are responsible for maintaining the confidentiality of the password associated with your Account. KEEP YOUR PASSWORD STRICTLY CONFIDENTIAL. If a User shares their password with others or allows others to discover and use their password with the Account, the User is giving access to the funds and information in the Account and assumes all responsibility for transactions in their Account Accordingly, you agree that you will be solely responsible to nTrust for all activities that occur within or through your Account. If you become aware of any unauthorized use of your password or of your Account, you agree to notify nTrust immediately.
3. Dormant Accounts. Accounts with a positive balance, but which have not been accessed in twelve (12) months are considered "Dormant". We will attempt to contact you in advance of any account becoming Dormant using the contact details associated with your Account. Dormant accounts are subject to a Dormancy Fee per month (see "Fees & Availability" section on website). To regain access to your Account after it has reverted to Dormant status, please contact nTrust support.
4. Identity Verification / KYC. You authorize nTrust, directly or through third parties, to make necessary inquiries to verify your identity in accordance with nTrust's Privacy Policy. We may ask our Users at any time to verify their identity to mitigate potential fraud and/or to comply with banking or anti-money laundering and anti-terrorist financing regulations or best practices. You agree to furnish such documentation or information requested by nTrust in order to verify your identity for such purposes. If a User refuses to comply with such verification processes, the User's Account may be suspended regardless of any or all pending or unsettled transactions. Notwithstanding nTrust's identify verification practices, nTrust cannot and does not guarantee any User's identity.
5. Privacy. For information about nTrust's data protection practices, please read nTrust's Privacy Policy. This policy explains how nTrust treats your personal information and protects your privacy, when you use the Services. The terms of the Privacy Policy are incorporated herein by reference.
6. Account Access. nTrust reserves the right to limit Account access and/or functionality (including deposits, transfers or withdrawals) and the right to terminate the Account with no prior notice if we, in our sole discretion, have reason to believe that a User has violated these Terms or has engaged in a Prohibited Activity or for any other reason in our sole and absolute discretion. nTrust will use reasonable commercial efforts to investigate Accounts that are subject to Account access limitations expeditiously and to reach a final decision on said limitations. Should a User's Account be limited, all funds will be held for a period of time until the issue is resolved. However, it may be held for a lesser period which nTrust will determine.

4) FUNDING YOUR nTRUST CLOUD

1. Funding Your nTrust Cloud. You can load funds into your nTrust Cloud by various means, which, depending on your location and method of funding, may incur fees. Please note that some fees are not imposed by nTrust and are not within nTrust's control. Not all Cloud funding methods are available in all regions and nTrust makes no representation as to the availability or continued availability of a given method in a particular region.
2. Funding Limitations. Cloud loading options may vary from time to time depending on local availability and any limits that may apply to your Account. Also, in order to mitigate fraud and to comply with Anti-Money Laundering and Anti-Terrorist Financing legislation and best practices, certain limits will be imposed on loads into nTrust Clouds dependent on the status of an Account, Account transaction history, and load method.
3. Returned Load. Please ensure that you provide accurate data before initiating a bank transfer. If you load funds by bank transfer and the amount is unpaid due to non-sufficient funds (NSF), a closed account, a non-existent account or a stopped payment, you will be liable to pay a fee.
4. Charge-backs. In the event that a User initiates a Charge-back on a Cloud load, that User will be liable to pay a Charge-back Fee per incident (see "Fees" below).

5) TRANSFERRING FUNDS TO & FROM YOUR CLOUD

1. Please see the 'Fees and Availability' section on our website for a clear breakdown of our pricing and services.
2. Transfer Limitations. In order to mitigate fraud and to comply with Anti-Money Laundering and Anti-Terrorist Financing legislation, certain transactional limits will be imposed on transfers, which limits may vary from User to User dependent on the verification status of the Account and Account transaction history.

6) WITHDRAWING FUNDS FROM YOUR CLOUD

1. Withdrawing From Your nTrust Cloud. You can withdraw funds from your nTrust Cloud by various means, which may, depending on your location and method of funding, may incur fees. Not all withdrawal methods are available in all regions and nTrust makes no representation as to the availability or continued availability of a given method in a particular region.
2. Withdrawal Limitations. Cloud withdrawal options may vary from time to time depending on local availability and any limits that may apply to your Account. Also, in order to mitigate fraud and to comply with Anti-Money Laundering and Anti-Terrorist Financing legislation and best practices, certain limits will be imposed on withdrawals from a User's Cloud dependent on the status of the Account, Account transaction history, and withdrawal method.
3. Cloud Money Card. The nTrust-issued prepaid card is not a credit card or a pre-loaded debit card. The Cloud Money card is a reloadable card onto which you must transfer money. In order to use your card, you must transfer funds from your nTrust Cloud onto your card. The Cloud Money card can be used at any location worldwide that accepts MasterCard. You can use it to make purchases online or at in-store point-of-sale locations, and at any Maestro-sponsored ATM to withdraw cash. If your card is lost or stolen, you must notify

nTrust immediately. Upon receipt of notification, the card will be deactivated and any remaining funds on your lost or stolen card will be immediately transferred to your nTrust Cloud. You will then have to order a new card — a replacement card will not be automatically sent to you. Should you require a replacement card, you may be responsible for the cost of the replacement card. nTrust's issuing bank applies fees to the use of the card, which are described in Cloud Money Card Fee Schedule, which are deducted from your card balance; these fees are not imposed by nTrust and nTrust does not receive or collect any portion of these fees. Cloud Money Card are not available in all regions and nTrust makes no representation as to the availability or continued availability of a given method in a particular region.

4. Returned Withdrawal. Please ensure that you provide accurate data before initiating a bank transfer. If you withdraw funds by bank wire or bank transfer and the amount is returned due a closed account or unable to locate, you will be liable to pay a Rejection Fee per incident as well as any other associated fees passed on by correspondent banks.

7) ACCOUNT BALANCES and ADMINISTRATION

1. No Cloud Balance Required. You are not required to carry a balance in your nTrust Cloud.
2. Balances Not Co-Mingled With nTrust Funds. If you do hold a balance in Cloud, your funds will be kept separate from the corporate/operational funds of nTrust.
3. Administration. While your funds are in our custody or control, nTrust will combine your funds with the funds of other Users and place those pooled funds into pooled accounts with one or more insured banks. These pooled accounts will be held for the benefit of nTrust's collective Users. You acknowledge that you will not receive interest or other earnings on the funds that nTrust processes on your behalf through pooled bank or financial institution accounts. In consideration for your use of the Services, you irrevocably transfer and assign to nTrust any ownership right that you may have in any interest that may accrue on funds held in pooled bank or financial institution accounts. This assignment applies only to interest earned on your funds, and nothing in these Terms grants nTrust any ownership rights to the principal of the funds. In addition to or instead of earning interest on pooled bank or financial institution accounts, nTrust may receive a reduction in fees or expenses charged by banking services by the banks or institutions that hold your funds.

8) REVERSALS, LIABILITY and NEGATIVE BALANCES

1. Liability for Reversed Transfers.
    1. When you receive a transfer from another nTrust User to your nTrust Cloud, you are and the sender ("Sending User") are jointly and severally liable to nTrust for the full amount of the transfer sent to you (plus any Fees, if applicable) if the payment is later invalidated for any reason, including a reversal or invalidation of the funding of the Sending User's Cloud.
    2. nTrust will first attempt to recover the entire amount of the reversed or invalidated transfer from the Sending User directly. If there are insufficient cleared funds in the Sending User's nTrust Cloud to cover the entire amount of the transfer to you plus any applicable Fees, nTrust may place a temporary hold on the funds in your Account to cover the amount of the liability.
    3. If nTrust is unable to recover the full amount of the liability from the Sending User within fifteen (15) days, nTrust may recover any remaining amounts due to nTrust by debiting your Account. If there are insufficient funds in your Account to cover your liability, your remaining balance (if any) will be removed, your Account will have negative balance up to the amount of your liability, and you will be required to immediately add funds to your balance to eliminate the negative balance.
2. Negative Balances. In the event that you are liable for any amounts owed to nTrust, you agree to allow nTrust to recover any amounts due to nTrust by debiting your Account. If you do not have an Account balance that is sufficient to cover your liability, your remaining balance (if any) will be removed, your Account will have negative balance up to the amount of your liability, and you will be required to immediately add funds to your balance to eliminate the negative balance. If your Account has a negative balance, you agree to load funds into your Account to cover the negative balance immediately. In addition, if your Account has a negative balance, nTrust may set off the negative balance with any funds that you subsequently receive or deposit into your Account. If you have multiple currency balances in your Account and one of the currency balances becomes negative for any reason, nTrust may setoff the negative balance by using funds you maintain in a different currency balance.
3. Collections. If you do not promptly clear any negative Account balances, we reserve the right to recover the funds by any means necessary, including initiating collection efforts to recover such amounts from you by engaging a collections agency and/or law enforcement.
4. Security. To secure your performance of this agreement and compliance with the Terms, you grant to nTrust a lien on and security interest in and to the funds held in your Account in the possession of nTrust.

9) MULTIPLE CURRENCIES AND EXCHANGE

1. Maintaining Balances in Multiple Currencies. You are responsible for all risks associated with maintaining Account balances in multiple currencies. You agree that you will not attempt to use multiple Account currencies for speculative trading.
2. Currency Exchange Fees. A currency conversion fee applies whenever a currency conversion is required to complete your transaction. The exchange rate is determined by a financial institution and is adjusted regularly based on market conditions. 1.5% is added to this exchange rate. Adjustments may be applied immediately and without specific notice to you.

10) PROHIBITED ACTIVITIES

1. Abuse Reporting. To report Prohibited Activities or use of the Services contrary to these Terms, please email: .
2. Prohibited Activities. Users shall at all times act reasonably and in good faith when using the Services and you expressly represent and warrant that in connection with your use of the Site, your Account, the nTrust Services, or otherwise in the course of your interactions with nTrust, other Users, or third parties, you shall not engage in the following activities ("Prohibited Activities"):

1. breach these Terms or any other agreement or policy that you have agreed to with nTrust;
2. use our Services or any portion thereof in a manner that violates any law, statute, ordinance, or regulation or in furtherance of any illegal or fraudulent activity (if you are an international user, you agree to comply with all local laws and regulations regarding your conduct);
3. send or receive what we reasonably believe to be potentially fraudulent funds;
4. allow your Account to have a negative balance;
5. initiate a Chargeback or reversal of a valid Cloud funding transaction or abuse the reversal process by a upi through your bank, or report unusual credit card or bank account use to your issuing bank without cause;
6. initiate a incoming bank transfer that is rejected due to insufficient funds in the bank account or an incorrect bank routing/institution and/or account number;
7. open or attempt to open multiple Accounts;
8. provide false, inaccurate or misleading information;
9. impersonate any person or entity (including, without limitation, another User) or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity;
10. employ an anonymizing proxy or other technologies or techniques that does or attempts to spoof, mask, or mis-identify your location, IP address, identity or origin;
11. submit altered or falsified verification documents, or otherwise deceiving or attempting to deceive nTrust regarding their identity or other applicable information;
12. refuse to cooperate in an investigation or provide confirmation of your identity or any other information provided to or requested by us;
13. share or disclose your nTrust password to anyone;
14. permit or authorize any other person or entity to use our Services or access your Account without our prior written consent;
15. use automated scripts or any other automated method to collect information from or otherwise interact with the Service or the Site, including, without limitation, using bots, spiders or other automated information-gathering devices or programming routines to "mine" information displayed, register User accounts, perform transactions, interact with the Site or any other activities nTrust considers inappropriate;
16. test or reverse-engineer the Services to seek to uncover system limitations, vulnerabilities or to evade filtering capabilities;
17. bypass or attempt to bypass any measures nTrust may use to prevent or restrict access to the Services;
18. alter, disable, interfere with or circumvent any aspect of the Services.
19. post or transmit, or cause to be posted or transmitted, any communication or solicitation designed or intended to obtain the identity, of any nTrust User or the password, Account, or private information of any nTrust User;
20. use your Account or the Services in a manner that nTrust, Visa, MasterCard, American Express, Discover or any other electronic funds transfer network reasonably believes to be an abuse of the card system or a violation of card association or network rules or
21. take any action that may cause nTrust to lose any of the services from our Internet service providers, payment processors, or other suppliers.

11) REMEDIAL ACTIONS

1. Remedial Measures. If we have reason to believe or suspect that you have engaged or plan to engage in any Prohibited Activities, we may take various actions we deem appropriate to protect nTrust, our other Users or you from reversals, chargebacks, claims, fees, fines, penalties and any other risk, including, without limitation:
   1. we may close, suspend or limit your access to your Account or functionality within your Account;
   2. we may notify others who have transacted with you, contact your bank or credit card issuer and/or warn other Users, law enforcement or impacted third parties of your actions;
   3. we may update inaccurate information you provided us;
   4. we may refuse to provide the Services to you in the future;
   5. we may hold your funds for up to 180 days if reasonably needed to protect against the risk of liability;
   6. we may at any point ask for information regarding your business, the source of funds, or the reason for you sending or receiving the payment and you agree to furnish same; and/or
   7. we may take legal action against you.
2. Notice of Measures. If we close your Account or terminate or restrict your use of the nTrust Services for any reason, we will provide you with notice of our actions. You acknowledge that nTrust's decision to take certain actions, including limiting access to your Account by placing holds or other actions, may be based on confidential criteria that is essential to our management of risk and the security of Users' Accounts and the nTrust system. You agree that nTrust is under no obligation to disclose the details of its risk management or its security procedures to you.

12) DISPUTES

1. Inter-User Disputes. If you have a dispute with one or more Users, you release nTrust from any and all claims, demands and actual/consequential damages related to your transaction(s) with said User(s).
2. Contact Us First. If a dispute arises between you and nTrust, our goal is to learn about and address your concerns and, if we are unable to do so to your satisfaction, to provide you with a neutral and cost effective means of resolving the dispute quickly.
3. Good Faith Attempts to Resolve. The parties agree that they will make good faith efforts to settle any dispute, claim or controversy arising out of or relating to this Agreement by discussion and/or negotiation.
4. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Jurisdiction for purposes of any action commenced under this Agreement or with respect to any tort committed or alleged to be committed in the performance of this Agreement. No choice of law rules of any jurisdiction shall apply hereto. The parties hereto expressly waive any right they have to a jury trial and agree that any court preceding under this Agreement shall be tried by a judge without a jury.

1. Forum. You agree that: (i) the Service shall be deemed solely based in the Jurisdiction; and (ii) the Service shall be deemed a passive one that does not give rise to personal jurisdiction over nTrust, either specific or general, in jurisdictions other than the Jurisdiction; and (iii) the Terms, and your relationship with nTrust under the Terms shall be governed by the internal substantive laws of the Jurisdiction, without respect to its conflict of laws principles. Any claim or dispute between you and nTrust that arises in whole or in part from the Service shall be decided exclusively by a court of competent jurisdiction located in the Forum City. You agree to submit to the personal jurisdiction of the courts located in the Forum City, for the purpose of litigating all such claims or disputes. Notwithstanding this, you agree that nTrust shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.
2. No Waiver. You agree that if nTrust does not exercise or enforce any legal right or remedy which is contained in the Terms (or which nTrust has the benefit of under any applicable law), this will not be taken to be a formal waiver of nTrust's rights and that those rights or remedies will still be available to nTrust.
3. Severability. If any court of law, having the jurisdiction to decide on this matter, rules that any provision of these Terms is invalid, then that provision will be removed from the Terms without affecting the rest of the Terms. The remaining provisions of the Terms will continue to be valid and enforceable.

13) AGENCY.

nTrust provides third-party payment processing services and carries out related actions on your behalf. At all times, your funds are held separately from our corporate funds and are not incorporated into or used for nTrust's operating expenses or corporate purposes. You acknowledge that nTrust is not a bank and that the Services are a payment processing and transfer service rather than a banking service. By initiating and sending funds through the Service or adding funds to your Cloud, you appoint nTrust as your agent to obtain the funds on your behalf and transfer them to the designated receiver. When you initiate funding transaction into your Cloud or when you transfer funds to another nTrust User, nTrust processes the funds on your behalf through the banks or institutions that hold your funds. You will not be able to withdraw those funds or send the funds to any other User unless the initial transaction is canceled. When you receive funds through the Service from another nTrust User, nTrust processes the funds on your behalf through the banks or financial institutions that hold your funds. Funds received in your Cloud are held in pooled bank or financial institution accounts. You may, from time to time, authorize nTrust to transfer your funds through our Site, but any such transferee must be an nTrust User.

14) WARRANTIES and LIABILITY

1. Indemnity. You agree to defend, indemnify and hold nTrust, its parent, officers, directors and employees harmless from any claim or demand (including attorneys' fees) made or incurred by any third party due to or arising out of your breach of these Terms and/or your use of the nTrust Services.
2. nTrust makes reasonable efforts to ensure that requests for electronic debits and credits involving bank accounts, credit cards and check issuances are processed promptly, but we make no representations or warranties regarding the amount of time needed to complete transactions because our Service is largely dependent upon many factors entirely outside of our control. NOTHING IN THESE TERMS SHALL EXCLUDE OR LIMIT NTRUST'S WARRANTY OR LIABILITY FOR LOSSES WHICH MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR LOSS OR DAMAGE CAUSED BY NEGLIGENCE, BREACH OF CONTRACT OR BREACH OF IMPLIED TERMS, OR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, ONLY THE LIMITATIONS WHICH ARE LAWFUL IN YOUR JURISDICTION WILL APPLY TO YOU AND NTRUST'S LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW. YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICES IS AT YOUR SOLE RISK AND THAT THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." IN PARTICULAR, NTRUST, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT: (I) YOUR USE OF THE SERVICES WILL MEET YOUR REQUIREMENTS, (II) YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, TIMELY, OR FREE FROM ERROR, (III) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND (D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED. ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM NTRUST OR THROUGH OR FROM THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS. NTRUST FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

3. YOU EXPRESSLY UNDERSTAND AND AGREE THAT NTRUST, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR: (I) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY. THIS SHALL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS; (II) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF: (A) ANY CHANGES WHICH NTRUST MAY MAKE TO THE SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE SERVICES (OR ANY FEATURES WITHIN THE SERVICES); (B) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER COMMUNICATIONS DATA MAINTAINED OR TRANSMITTED BY OR THROUGH YOUR USE OF THE SERVICES; (C) YOUR FAILURE TO PROVIDE NTRUST WITH ACCURATE ACCOUNT INFORMATION; (D) YOUR FAILURE TO KEEP YOUR PASSWORD OR ACCOUNT DETAILS SECURE AND CONFIDENTIAL. THE LIMITATIONS ON NTRUST'S LIABILITY ABOVE SHALL APPLY WHETHER OR NOT NTRUST HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

15) DEFINITIONS

1. "Agreement" or "Terms" means this agreement including all subsequent amendments or revisions;
2. "Balance" means any money that you have in your Account. The terms "money" and "funds" are used interchangeably in this Agreement;
3. "Chargeback" means a request that a credit or debit card holder files directly with his or her debit or credit card company or debit or credit card issuing bank to invalidate a payment;
4. "eCheck" means a payment funded using a sender's bank account Payment Method that is held pending and not received by the recipient until it clears. When you send money using eCheck it will usually be held pending for up to eight business days;
5. "Forum City" means the city in which you are resident or from which you intend to use or access the Services
6. "Jurisdiction" means the country in which you are resident or from which you intend to use or access the Services;
7. "Services" means all our products and services and any other features, technologies and/or functionalities offered by us on our Site or through any other means. "Services" means any software, services and web site provided by or made available through nTrust or its affiliated or partner companies, including, without limitation the "nTrust" service, an online service to enable self-directed feedback and personal development management;
8. "Site" means any website www.nTrust.com operated by or on behalf of nTrust and through which Services are accessed by you;
9. "We", "our", "us" or "nTrust" means nCrypt Financial Corp. or any successor company or assignee; and
10. "User" means any person or entity using the nTrust Services, including you.

© 2010 - 2015 nTrust Group | Read Disclaimer

Breaking out great SAVINGS this March!

FINANCIAL POST

Customize your stocks now

Indices (Data delayed at least 15 min)	S&P/TSX	Dow Jones	NASDAQ	TSX Venture
	14,718.51 76.75 (0.52%)	17,633.19 -29.53 (-0.17%)	4,847.56 -12.20 (-0.25%)	669.00 -0.50 (-0.07%)

ENTREPRENEUR

This 'cloud money' startup knows what it takes to succeed

TONY WANLESS | December 28, 2014 | Last Updated: Dec 28 9:00 AM ET
More from Tony Wanless

Republish Reprint

NTrust's "Cloud Money" system began in 2011, one of a handful of Vancouver startups offering alternatives to traditional credit card and cash systems. Handout

Twitter Google+ LinkedIn Email Typo? More

As a lawyer, Rob MacGregor learned how to be thorough and careful when approaching any pursuit, especially one involving money. These qualities stood him in good stead when, five years ago, he began building nTrust, a Vancouver-based online payments and money transfer system.

Although primarily online, nTrust is not your typical tech story, where entrepreneurs take a product from garage to big office and hundreds of employees seemingly overnight. Unlike most rapidly expanding online companies, it's still small, albeit

Δ π EXHIBIT 223
Deponent RM
Date 3/17/15 Rptr. MW
WWW.DEPOBOOK.COM

Financial Post Newsletters
Get weekly tips on how to run your business in your inbox
Email address...
Privacy Policy

Tweets from @fpentrepreneur

Victoria Wells @vwells80 14m
If your startup has a funding announcement, I'd love to hear about it for a new weekly feature on @fpentrepreneur.
Retweeted by FP Entrepreneur
Reply Retweet Favorite

FP Entrepreneur @fpentrepreneur 1h
Amazon launches store selling exclusive products from 'Shark Tank,' Kickstarter campaigns natpo.st/1HDp6cr #entrepreneur
Reply Retweet Favorite

FP Entrepreneur @fpentrepreneur 5h
This craft beer startup uses some clever marketing tricks to win customers natpo.st/1C5auCw pic.twitter.com/UVyvJBYNyU

EXHIBIT M-5

steadily growing.

"I am a lawyer, trained to identify risk," MacGregor explains. "Usually this is anathema to entrepreneurs, but if you want to operate in the world of banking, you have to understand the rules. My training taught me what constraints there are around currency, but I recognized there was opportunity as well."

NTrust's "Cloud Money" system began in 2011, one of a handful of Vancouver startups offering alternatives to traditional credit card and cash systems. Aiming to be "Skype for money," Cloud Money is an online fund transfer system that facilitates uploading funds, making payments, and transferring money via mobile phones. It also expedites international payments and money transfers, which have tended in the past to be expensive.

An un-Big Bank in a sense, nTrust's ambitions are to be a large, low-cost player in money-transfer, whether locally, or in the cumbersome and intricate national and international financial system dominated by big financial institutions. As MacGregor puts it, nTrust's aim is to be used "anywhere there is a cheque."

Clearly, nTrust is directed at millennials, tech-savvy young adults with little brand loyalty and expectations to buy and pay, move money, make friends, find mates, and live a large part of their lives online. As its website asserts: "Free your money by uploading it to the 'nTrust Cloud,' then send it, spend it, or move it wherever you want as easily as sending a text."

Related

Put away your wallet: Why mobile payments' moment may have finally arrived

Banks intent on becoming pioneers of mobile payment systems

Comments for this thread are now closed.

AROUND THE WEB

Most recently, nTrust tested its mobile payment system with merchants at the University of British Columbia's student union building. It is also active with mobile food vendors such as food trucks, who generally deal in cash and welcome a payment system that frees up workers from cash registers to make a lot of food in a short period. Its first food truck client was Dougie Dog, a gourmet hot-dog vendor whose owner Dougie Love has appeared twice on Dragon's Den, and, while definitely a showman, knows his way around a payment system.

A not-quite-former lawyer — his private law practice remains "on hold" — MacGregor recognized early on that to realize its ambitions, nTrust had to jump through many regulatory hoops to gain credibility in the system. It didn't help that in the post 9-11 atmosphere, financial institutions were scared of new and seemingly wild adventures in money transfer.

Initially, nTrust focused on transferring money to the Philippines, where MacGregor had some connections, and where money was routinely remitted by Filipino workers in other countries. Also, nTrust spent most of its first year becoming PCI compliant, which meant passing rigorous testing that certified it to the standard of banks in terms of compliance and auditing — basically, it's now licensed like a bank.

That first year, the company was composed of the three founders, but under MacGregor's cautious and methodical steering, it has been growing quietly. For example, he knew it had to offer an nTrust credit card, and so proceeded to hit up 32 financial institutions to back it. Eventually, Scotiabank agreed.

Reply Retweet Favorite

Content from Twitter

Book Reviews

Book review: Dirty Little Secrets of Family Business

Book review: Startup Mixology

Book review: Business Insights

FP Entrepreneur Calendar

Networking and staying up to date with the latest trends is key to entrepreneurial success.

Send your events to entrepreneur@nationalpost.com

News Releases

Amica Mature Lifestyles to Announce Third Quarter Results and Host Conference Call April 10, 2015

Market Data Fees to Benefit Investors and Capital Raising Companies Aequitas NEO Exchange Announces Market Data Fees

Therapure Innovations Receives FDA Approval to Proceed with a Phase 1 Clinical Trial of Its Novel Anemia Therapeutic TBI 304H

Ergon BioFuels Enters into Comprehensive Service Arrangement with Gavilon

Cegedim Relationship Management Releases Digital Channel Engagement: A Measurable Opportunity, the Third in a Series of Multichannel White Papers

"Three years ago, we were in late Beta, and I knew the first thing I had to deal with was risk, both regulatory and entrepreneurial," MacGregor now says. "You have to deal with banks if you want to move money — they're the gatekeepers. So we had to be part of their ecosystem, we had to get them comfortable with us. It became a case of showing that here's the threshold required by law and here's where we are, way beyond it."

Today, nTrust has 35 employees in Vancouver and Manila and boasts 45,000 members who can transfer money with low fees. Small merchants and a growing number of mom-and-pop micro-businesses love its 1%-per-sale, low-cost credit card processing fees.

They have to be cautious too.

Find Entrepreneur on Facebook

Twitter Google+ LinkedIn Email Typo? More

Most Popular

Topics: Entrepreneur, FP Startups, Financial Services Sector

BizTVCanada

FP Marketplace: Business Services

Search listings Search

View all listings

6 Stocks to Hold Forever
wealthyretirement.c...
Looking to retire? These 6 stocks will generate regular income.

Canadian Dollar Investing
wallstreetdaily.com/T...
Power Shift In The Currency Market. 3 Currencies Set To Rise By 20-25%!

Request Comment Removal

POST POINTS | Earn rewards for being a loyal National Post Reader

canada.com | © 2015 National Post, a division of Postmedia Network Inc. All rights reserved. Unauthorized distribution, transmission or republication strictly prohibited.

Share 18

Follow

LinkedIn What is LinkedIn? Join Today S

Keep up with nTrust

Stay up to date with company news

Discover new job opportunities

Join LinkedIn to get the latest news, insights, and opportunities from over 3 million compan

nTrust

132 followers Follow

Home

nTrust is a regulated and trusted global money transfer platform designed to free its members' money by uploading it to the cloud. Cloud Money™ enables money transfers around the globe as fast and seamless as sending a text. nTrust is changing the way the world moves money by empowering users to manage, move and use their hard-earned funds.

Specialties
online money transfers, international money transfers, prepaid credit cards, international remittance, cloud money

Website
http://www.nTrust.com

Industry
Financial Services

Type
Privately Held

Headquarters
Downtown, City Center Vancouver, BC Canada

Company Size
11-50 employees

Founded
2011

Recent Updates

nTrust Our founder, Robert MacGregor, sat down with the National Post to chat about nTrust's origins, what it took to become PCI compliant, and how to strike a balance between risk and entrepreneurship. Check out the full article below!

This 'cloud money' startup knows what it takes to succeed

ntru.st · Minding your business: With a lawyer at its helm, nTrust understood from the start that if you want to operate in the world of banking, you have to know the rules

Like · Comment · Share · 2 months ago

nTrust We're hiring! Join our global headquarters in downtown Vancouver! We're currently hiring a Sales Manager, E Comm Specialist, and a Mid-Level QA Engineer.

Sales Manager |

ntru.st · nTrust is a regulated and trusted global peer-to-peer money transfer platform helping people free their money. Using Cloud Money, nTrust members can move money around the globe as fast and seamlessly as sending a text - for free.

Like (5) · Comment · Share · 11 days ago

Jessica Allen, Greg Holowaychuk +3

Add a comment...

nTrust We're hiring a Financial Analyst! If you're a data head, love creative problem-solving, and have some serious financial analysis chops, we'd love to hear from you. Join the nTrust team at our downtown

Ads You May Be Interested In

Monetize your Big Data!
Dr. Mo Automatic Statistician monetize your data by generating predictions.

Stop Ransomware
Why Security Awareness Training? Ransomware, that's why. Get a quote now.

Virtual Reality for AEC
VIMtrek provides a complete Visual Information Model with the data (BIM).

nTrust employees

Jessica Allen
Content Strategist

24 Employees on LinkedIn

See how you're connected

Ads You May Be Interested In

Security Awareness Course
Protect your Network with Kevin Mitnick Security Awareness Training

Cloud-Based Fax Solutions
Deploy your Business Instantly. Secure, Reliable and Affordable Fax.

Invitation from LinkedIn
Place ads on LinkedIn. Acquire new customers for your business. Try it now.

People Also Viewed

nTrust · Payfirma · newordstream · Allocadia · nTrust

Δ π EXHIBIT 224
Deponent RM
Date 3/17/15 Rptr. MW
WWW.DEPOBOOK.COM

EXHIBIT M-6

Vancouver global headquarters.

Financial Analyst, eCommerce |

ntru.st · nTrust is a regulated and trusted global peer-to-peer money transfer platform helping people free their money. Using Cloud Money, nTrust members can move money around the globe as fast and seamlessly as sending a text - for free.

Like (1) · Comment · Share · 20 days ago

nTrust

Add a comment...

nTrust NFC is gradually becoming more integrated with our daily lives. Check out this NFC SD card from Toshiba that lets you preview your photos with a tap.

Toshiba's NFC SD card lets you preview pictures with just a tap

ntru.st · Toshiba has just taken the wraps off of two new products to help make photographer's lives much easier. The company has just announced the world's first NFC-enabled SD card, as well as a new Wifi-enabled card.

Like (3) · Comment · Share · 2 months ago

Claudio Afonso, Julian Hakim and Jessica Allen

Add a comment...

nTrust Are mobile payments safe? What does encryption have to do with "sniffing"? And how secure is the Cloud? We sit down with Rino Ong, nTrust's CTO, for answers to these questions as well as an in-depth look at nTrust's security.

nTrust, Security, and You: An Interview with Rino Ong, CTO |

ntrust.com · nTrust is a regulated and trusted global peer-to-peer money transfer platform helping people free their money. Using Cloud Money, nTrust members can move money around the globe as fast and seamlessly as sending a text - for free.

Like (11) · Comment (1) · Share · 3 months ago

Ken Chen +9

LinkedIn Member Mr. Ong and Mr. Hsu. These two guys are two reasons why they have technology. Everyone else above them is useless. True story :-)
1 month ago

Add a comment...

nTrust Come work with us! We're hiring a Business Analyst: http://bit.ly/1uKRpO1

Business Analyst |

bit.ly · nTrust is a regulated and trusted global peer-to-peer money transfer platform helping people free their money. Using Cloud Money, nTrust members can move money around the globe as fast and seamlessly as sending a text - for free.

Like · Comment · Share · 4 months ago

nTrust Is your business ready for Cloud Money mobile payments? Hear what our first merchant partner, Dougie Luv of DougieDog Hot Dogs, has to say about Cloud Money in our newest video.

nTrust for Small Business

vimeo.com · Is your business ready for mobile payments? See how Cloud Money mobile payments have helped DougieDog Hot Dogs streamline transactions and connect with customers. Learn more at nTrust.com/merchants.

Like · Comment · Share · 4 months ago

nTrust We're hiring! If you're studying at UBC, love technology, and want to gain hands-on marketing experience, check out the UBC Cloud Money Rep position.

Are you the next UBC Cloud Money™ Rep?

ntrust.com · This fall, nTrust is going back to school! No, we're not getting our Critical Studies in Post-Structuralism on. We're not storming the Engineering building, either. We're bringing Cloud MoneyTM to UBC! If you were at the Point Grey campus earlier...

Like (4) · Comment · Share · 5 months ago

Julian Hakim, Erin Silo +2

Add a comment...

nTrust We're hiring! Take a look at our Careers page today to check out our current opportunities.

nTrust Careers

ntrust.com · nTrust is a rapidly-growing, dynamic start-up that enables secure and regulated online peer-to-peer international transactions through speed, simplicity and convenience of contemporary technologies (web & mobile). Sending money instantly is as...

Like (3) · Comment · Share · 6 months ago

Marie Lorabelle Reboya, Morgan Stewart and Jessica Allen

Add a comment...

Show More Updates

Sign up Help Center About Careers Advertising Talent Solutions Sales Solutions Small Business Mobile Language SlideShare
LinkedIn Updates LinkedIn Influencers LinkedIn Jobs Directories Members Jobs Pulse Companies Groups Universities Titles
LinkedIn ©2015 User Agreement Privacy Policy Community Guidelines Cookie Policy Copyright Policy Guest Controls

nTrust

New Website Helps nTrust Members Send Money Home in Three Easy Steps

January 24, 2014 / Features, News/Media

VANCOUVER, BRITISH COLUMBIA–(Marketwired – Jan. 24, 2014) - With an estimated $400 billion in global remittances each year, nTrust's newly launched website and mobile site is making it easier to send money around the world.

According to the World Bank global remittance grew by 6.6 per cent to $414 billion in 2013, and is expected to cross the half-trillion mark by 2016. Yet the high cost of sending money abroad through traditional channels continues to pose a challenge for both sender and recipient.

With an increasing number of migrant workers sending more money around the world and persistent obstacles such as significant transaction fees, nTrust's refreshed website and mobile site allow members to transfer money to friends and families living abroad in just three simple steps for as little as 1.9 per cent.

Once an nTrust Cloud is created, members simply log in nTrust, select a member in their nTrust Neighborhood to send the funds to, enter in the amount and money is transferred within seconds, for free. Additionally, the mobile site lets members conveniently transfer money while on the go.

"As global migration increases there is a growing need for a seamless service to help send money back home with little cost," says Rod Hsu, Chief Experience Officer for nTrust. "Our goal is to make it as easy and affordable as possible for our members to get their hard-earned funds to deserving loved ones in the click of a few buttons, avoiding long lines and wait times."

alternative payments bank transfer bank wire bills payment Cloud Money financial services remittance, money transfer service terrorist financing virtual currencies

Δ π EXHIBIT 225
Deponent RM
Date 3/12/15 Rptr. MW
WWW.DEPOBOOK.COM

Related Articles

EXHIBIT
M-7

How to send money overseas for free with...

Week #3 Winner Announcement: Win Your Purchase Contest

Week #2 Winner Announcement: Win Your Purchase Contest

Blog home

Features
Send Money
Cards
Pay Bills
Merchants

Company
Mission
FAQs
Charities
Help
Careers

Connect
Facebook
Twitter
Linkedin
Blog
Contact

Legal
Privacy Policy
Terms of Use

© 2010 - 2015 nTrust Group | Read Disclaimer