Mailed:
August 14, 2008
jtw

UNITED STATES PATENT AND TRADEMARK OFFICE

_____

Trademark Trial and Appeal Board

_____

In re AXALTO S.A.

_____

Serial No. 78724979

_____

Edward W. Weisz of Cohen, Pontani, Lieberman & Pavane for AXALTO, S.A.

Ahsen Khan, Trademark Examining Attorney, Law Office 113 (Odette Bonnet, Managing Attorney).[1]

_____

Before Bucher, Zervas and Walsh, Administrative Trademark Judges.

Opinion by Walsh, Administrative Trademark Judge:

AXALTO, S.A. (applicant) has filed an application to register the mark PROTIVA in standard characters for goods identified as "multi-factor authentication apparatus for logical access consisting primarily of encoded smart cards, digitally encoded tokens, and authentication software" in

[1] Two Examining Attorneys other than the one currently assigned handled this application prior to appeal.

International Class 9.[2]

The Examining Attorney has refused registration under Trademark Act Section 2(d), 15 U.S.C. § 1052(d), based on a likelihood of confusion with Registration No. 2296799 for the mark PROTEVA in standard characters for goods identified as "electrical and scientific apparatus, specifically computers" in International Class 9. The registration issued on November 30, 1999, and it is active.

Applicant and the Examining Attorney have filed briefs. We affirm.

Section 2(d) of the Trademark Act precludes registration of an applicant's mark "which so resembles a mark registered in the Patent and Trademark Office… as to be likely, when used on or in connection with the goods of the applicant, to cause confusion…" The opinion in *In re E. I. du Pont de Nemours & Co.*, 476 F.2d 1357, 177 USPQ 563, 567 (CCPA 1977) sets forth the factors to consider in determining likelihood of confusion. Here, as is often the case, the crucial factors are the similarity of the marks and the similarity of the goods of applicant and

[2] Application Serial No. 78724979, filed October 3, 2005, based on a statement of applicant's bona fide intention to use the mark in commerce under Trademark Act Section 1(b), 15 U.S.C. § 1051(b), and based on a foreign registration under Trademark Act Section 44(e), 15 U.S.C. § 1126(e), and also claiming priority under Trademark Act Section 44(d), 15 U.S.C. § 1126(d), based on a foreign application filed on September 19, 2005.

registrant. *Federated Foods, Inc. v. Fort Howard Paper Co.*, 544 F.2d 1098, 192 USPQ 24, 29 (CCPA 1976)("The fundamental inquiry mandated by Section 2(d) goes to the cumulative effect of differences in the essential characteristics of the goods and differences in the marks."). We will consider each of the factors as to which applicant or the Examining Attorney presented arguments or evidence.

As to the marks, in comparing the marks we must consider the appearance, sound, connotation and commercial impression of the marks at issue. *Palm Bay Imports Inc. v. Veuve Clicquot Ponsardin Maison Fondee En 1772*, 396 F.3d 1369, 73 USPQ2d 1689, 1692 (Fed. Cir. 2005).

Applicant says very little about the marks other than arguing that, "the Examiner only analyzed the supposed similarity in sound in concluding that the marks are similar." Applicant's Brief at 2.

The Examining Attorney argues that the marks are "nearly identical in sound and appearance with the only difference being that applicant's mark is spelled with an 'i' and registrant's mark is spelled with an 'e.'" Examining Attorney's Brief at 5. The Examining Attorney also argues that the marks create a similar commercial impression.

We conclude that the marks are highly similar. As the Examining Attorney argues, they differ by only one letter, and that difference is not significant. The differing letters in question, "i" and "e," are both vowels with similar sounds. The differing letters also appear in the middle of the marks, which are otherwise identical. Thus, the marks are highly similar in both appearance and sound. Also, both marks appear to be coined terms with no meaning. There is no obvious connotation or commercial impression. However, due to the high degree of similarity in appearance and sound, to the extent that the marks may project a connotation or commercial impression, we conclude that it too would be highly similar. Overall, the difference between the marks is subtle, if not imperceptible. Furthermore, as the Examining Attorney points out, the proper test for similarity is not a side-by-side comparison. Rather, purchasers rely on their imperfect recollection of marks. *In re 1st USA Realty Professionals Inc.*, 84 USPQ2d 1581, 1587 (TTAB 2007).

Accordingly, we conclude that PROTIVA and PROTEVA are highly similar.

As to the goods, the goods of applicant and the registrant need not be identical to find likelihood of confusion under Section 2(d). They need only be related in

such a way that the circumstances surrounding their marketing would result in relevant purchasers mistakenly believing that the goods originate from the same source. *On-Line Careline Inc. v. America Online Inc.*, 229 F.3d 1080, 56 USPQ2d 1471 (Fed. Cir. 2000); *In re International Telephone & Telegraph Corp.*, 197 USPQ 910, 911 (TTAB 1978).

Furthermore, in comparing the goods and the channels of trade we must consider the goods as identified in the application and registration. *See Octocom Systems, Inc. v. Houston Computers Services Inc.*, 918 F.2d 937, 16 USPQ2d 1783, 1787 (Fed. Cir. 1990) ("The authority is legion that the question of registrability of an applicant's mark must be decided on the basis of the identification of goods set forth in the application regardless of what the record may reveal as to the particular nature of an applicant's goods, the particular channels of trade or the class of purchasers to which the sales of goods are directed.") *See also Paula Payne Products v. Johnson Publishing Co.*, 473 F.2d 901, 177 USPQ 76, 77 (CCPA 1973) ("Trademark cases involving the issue of likelihood of confusion must be decided on the basis of the respective descriptions of goods.").

Applicant identifies its goods as "multi-factor authentication apparatus for logical access consisting primarily of encoded smart cards, digitally encoded tokens,

and authentication software" in International Class 9. The goods in the cited registration are identified as "electrical and scientific apparatus, specifically computers" in International Class 9.

Here also, applicant offers limited argument. Applicant appears to argue that the Examining Attorney found the goods related merely because the goods are in the same class or because the goods are "in the same broad field." Applicant's Brief at 5. Applicant also argues, "Applicant's goods (i.e., smart cards) are marketed toward and purchased by highly sophisticated customers. In contrast registrant's goods (i.e., computers) are marketed towards the general public." *Id.* (We will address applicant's sophisticated-purchaser argument, also referenced here, separately below.)

The Examining Attorney argues that the respective goods are highly related because the identification of goods in the cited registration is broad enough to include applicant's goods and because the respective goods would be used together. The Examining Attorney has provided substantial evidence in support of the position that the respective goods are overlapping, and closely related.

First, applicant assumes that the goods identified in the cited registration are narrow in scope, that is, that

"computers" would only be sold to the general public. The *Merriam-Webster's Collegiate Dictionary* (11th ed. 2003) defines "computer," in relevant part, as "a programmable usu. electronic device that can store, retrieve and process data."[3] There is nothing in this definition, nor in the identification of goods, which would limit the sales of "computers" to the general public. In fact, "computer," as defined here, and as generally understood, is an extremely broad term encompassing a wide range of devices which could be sold to a wide range of potential purchasers.

The Examining Attorney has provided voluminous evidence regarding "smart cards," the item of goods applicant emphasizes in its brief. That evidence shows (1) that "smart cards" falls within the definition of a "computer," (2) that "smart cards" and the other authentication apparatus applicant identifies may be incorporated into a "computer" and (3) that "smart cards" and the other authentication apparatus applicant identifies are also used with and complementary to "computers."

Excerpts from applicant's own website show that applicant itself markets the identified goods, along with

[3] The Board may take judicial notice of dictionary definitions. *University of Notre Dame du Lac v. J. C. Gourmet Food Imports Co., Inc.*, 213 USPQ 594 (TTAB 1982), *aff'd*, 703 F.2d 1372, 217 USPQ 505 (Fed. Cir. 1983).

"computers," such as, card readers, for use in connection with computer systems for businesses, such as, financial institutions. Attachment to June 8, 2007 Office Action.

An excerpt from google.com explains what a "smart card" is:

> We'll focus on two types of smart cards: memory smart cards, which can be viewed as miniscule removable read/write discs with optional security; and processor cards, which can be viewed as miniature computers with an input and output port.

Id.

An excerpt from google.com states:

> A Smart Card is a plastic card the size of a credit card with an integrated circuit built into it. The integrated circuit may consist of EEPROM in the case of a memory card or it may also contain ROM, RAM and even a CPU… Smart cards include a microchip as the central processing unit, random access memory (RAM) and data storage of around 10MB… A smart card is a mini-computer without the display screen and keyboard. Smart cards contain a microchip with an integrated circuit capable of processing and storing thousands of bytes of electronic data. Due to the portability and size of smart cards, they are seen as the next generation of data exchange.

Id.

Another excerpt from mips.com includes an article entitled, "Smart Card: The Computer in Your Wallet." *Id.*

An excerpt from nist.gov, a site connected with the Federal National Institute of Standards and Technology includes the following:

> Q. What is a smart card?
>
> A. A smart card is typically a "credit card" sized form factor with a small-embedded computer chip. The card-computer can be programmed to perform tasks and store information. There are different types of smart cards, memory cards, processor cards, electronic purse cards, security cards, and JavaCards. A smart card that has a processor is inserted into a smart card reader (commonly called a card terminal) and is available for use. The software wishing to communicate with the reader needs to send some commands to manage the reader, things like power up and transfer command to card. The commands sent to cards can be custom, but we prefer to use the standard ISO7816 Specifications, which define command formats in great detail. Many different types of readers exist and soon we hope to see them shipped as standard equipment on PCs.
>
> …
>
> Q. Why are smart cards always associated with security?
>
> A. One of the fundamental problems in securing computer systems is the need for tamper-resistant storage of keys. Smart cards provide this functionality as well as the ability to upgrade and/or replace a security solution when it becomes compromised. For example, there are millions of digital satellite systems that are smart-card enabled, and when some enterprising hackers crack the security, the millions of DSS units need not be replaced, we can just mail out new cards. With JavaCard it gets even better in that we just send new cardlets [JavaCard application] to everyone.

Id.

An excerpt from howstuffworks.com states, "Smart cards can be used with a smart-card reader attachment to a

personal computer to authenticate a user." Attachment to June 8, 2007 Office Action.

The Examining Attorney has also provided third-party registrations to show that the respective goods are related.

For example:

> Registration No. 2145060 for the mark SECURITY FOR A CONNECTED WORLD for goods identified as:
>
> computer hardware and software, namely, smartcards to store information in electronic format; card readers; and computer software in the field of network I&A (identification and authentication) for outside access to the network, data encryption and decryption, identification of persons by stored images recorded on smartcards, password protection for access to networks, computer programs and computer files, and security for communications between network users and public networks such as the global communications network; and computer systems comprising such cards, such card readers, and computers loaded with such computer software; computer systems comprising smartcards to store information in electronic format; card readers; and computers loaded with computer software in the field of network I&A (identification and authentication) for outside access to the network, data encryption and decryption, identification of persons by stored images recorded on smartcards, password protection for access to networks, computer programs and computer files, and security for communications between network users and public networks such as the global computer network; computer hardware and software for use as a global computer network firewall that is used to protect user access from an untrusted network to a trusted network, using integrated authentication tokens for a challenge/response logon as well as encryption for files on desktop and laptop computers;

smartcards to store information in electronic format; card readers; and computer software in the field of network I&A (identification and authentication) for outside access to the network, data encryption and decryption, identification of persons by stored images recorded on smartcards, password protection for access to networks, computer programs and computer files, and security for communications between network users and public networks such as the global communications network; a computer system that incorporates a smartcard, a smartcard reader and the software to insure the security of businesses, employees and computer networks, and to provide network security and access control, a data repository for emergency medical information and personnel data, systems integrity, and identification with digital photo images and fingerprints encoded in the smartcard;

Registration No. 2484541 for the mark SAFENET for goods identified as:

Products that provide secure communication on global computer communication networks and local are networks, namely computer hardware for use with encryption, user verification and authentication, local area networks, firewall applications; electronic encryption units; encoded smart cards containing programming used to generate and verify user passwords; data encryption computer software; local area computer network monitoring software, and computer peripherals, namely modems and routers; computer software in the field of security firewall for computers and computer users;

and

Registration No. 2717912 for the mark SMART@IO for goods identified as:

desktop personal computers; notebook personal computers, portable personal computers; cellular telephones; personal digital assistants; handheld personal computers; input/output controllers, namely, electronic controllers, computer cursor

> controller devices, namely, computer mouse; media readers, namely bar code readers, magnetic encoded card readers; smart card readers; smart card controllers for controlling smart card interface with computers; personal computer peripherals, namely, reader support smart cards containing programming used for interfacing with computers; secure digital computer memory; multi-media cards, namely blank smart cards or magnetically encoded smart cards; compact flash readers for reading smart cards; universal serial bus including ports, modems, and adapters; serial ports; parallel port interfaces.

These registrations are representative of many more which the Examining Attorney has made of record. These registrations, and the others submitted by the Examining Attorney, suggest that the respective goods are of a type which may emanate from the same source. *In re TSI Brands Inc.*, 67 USPQ2d 1657, 1659 (TTAB 2002); *In re Albert Trostel & Sons Co.*, 29 USPQ2d 1783, 1785-86 (TTAB 1993). In fact, in this case, as we stated above, the totality of the evidence, including the third-party registration, show (1) that "smart cards" falls within the definition of a "computer," (2) that "smart cards" and the other authentication apparatus applicant identifies may be incorporated into a "computer" and (3) that "smart cards" and the other authentication apparatus applicant identifies are also used with and complementary to "computers."

Accordingly, we conclude that the respective goods are closely related, if not identical, and that the channels of trade for the respective goods are overlapping.

Applicant argues most strenuously that there would not be a likelihood of confusion here because the purchasers of its goods are sophisticated. Applicant argues that the Examining Attorney has not given proper weight to this factor. Applicant states:

> The personnel making the decision to purchase smart cards are educated, sophisticated purchasers with a high level of technical expertise in smart cards and in the computer equipment in which the smart cards will be implemented. Such purchasers need to know the technical requirements for the security systems they are designing. This requires knowledge of the computer system and the smart cards. Thus, such purchasers would be expected to exercise a great deal of care in selecting smart cards and would be able to differentiate between applicant's mark and registrant's mark.

Applicant's Brief at 4 (citation omitted). The Examining Attorney disagrees and argues that purchaser sophistication is not a controlling factor here.

First, we note that in the presentation of its arguments as to this factor applicant explicitly acknowledges that there is an integral relationship between smart cards, on the one hand, and computers and computer systems on the other. That is, they are used together. While we do not have direct evidence that the purchasers of

the smart cards and the other authentication equipment identified in the application are sophisticated in all instances, we will assume as applicant argues, that these individuals would have significant relevant technical expertise. However, we cannot consider this factor in isolation; in this case the marks are highly similar and the goods are closely related, if not identical. Furthermore, even sophisticated individuals are not immune from trademark confusion. *In re Decombe*, 9 USPQ2d 1812 (TTAB 1988); *In re Pellerin Milnor Corp.*, 221 USPQ 558 (TTAB 1983). Therefore, after considering the totality of the circumstances in this case, we conclude that the sophistication of potential purchasers would not diminish the likelihood of confusion.

Finally, after considering all evidence and arguments bearing on the *du Pont* factors, we conclude that there is a likelihood of confusion between applicant's PROTIVA mark if used in connection with "multi-factor authentication apparatus for logical access consisting primarily of encoded smart cards, digitally encoded tokens, and authentication software" in International Class 9 and the registered PROTEVA mark used in connection with "electrical and scientific apparatus, specifically computers" in International Class 9.

Decision: We affirm the refusal under Trademark Act Section 2(d).