White and Williams LLP

Focus on Intellectual Property *Spring/Summer 2010*

BUILDING THE ELECTRONIC SAFE: IS YOUR BUSINESS COMPLIANT?

by Ryan J. Udell, Esq. and Wasim S. Rahman, Esq.

In recent years, businesses and consumers have, for reasons of convenience and efficiency, embraced electronic transactions and the use of electronic data. As a result, extraordinary amounts of personal information, including credit card information, social security numbers, home addresses and the like are now stored electronically. Such information has increasingly become a target for theft and misuse. Numerous, recent, high-profile data security breaches have amplified concerns among consumers. For example, in 2007, TJ Maxx suffered the largest data breach in history when cyberthieves stole 45 million customer credit card numbers. It is estimated that the total damages incurred in this one breach are in excess of $4.5 billion.

From the TJ Maxx breach and others, federal and state governments have become acutely aware of the potentially disastrous consequences. They have enacted or are in the process of enacting legislation designed to minimize the occurrence of such breaches and mitigate the consequences of such breaches if and when they happen.

CALIFORNIA (AS USUAL) LEADS THE WAY

In 2002, the California legislature passed SB 1386, known as the data breach notification law. When the law came into effect on July 1, 2003, it was the first data breach notification law in the country. Since then, all but a handful of states have passed similar laws.

The California law requires all businesses, even if they are not based in California, to notify their California customers if they have experienced, or reasonably believe they have experienced, a breach in the security of personal information that they possess. Specifically, the data breach notification law requires Californians to be notified if their name is obtained along with one of the following pieces of data: social security number, driver's license number, account number (credit or debit card, along with pass code to access financial accounts), medical information or health information. Most significantly, the California law provides individuals whose personal data has been breached with a private right of action against the business that suffered the breach. Furthermore, prevailing plaintiffs may recover attorney's costs and fees in pursuing the action.

Last month, the California State Senate approved Senate Bill 1166, amending the California data breach notification law. The bill is now awaiting approval from the California State Assembly and signature from Governor Arnold Schwarzenegger. The amendment would require a company's data security breach notification be written in plain English, and contain detailed information about the breach, such

continued on page 3…

IN THIS ISSUE…

AROUND THE COURTS: RECENT VERDICTS

The United Stated States District Court for the Eastern District of Pennsylvania, in the matter of *Quad/Tech, Inc. v. Q.I. Press Controls B.V., et. al,* denied Plaintiff's motion for a preliminary injunction which was predicated on the Plaintiff's claim that the Defendants (the manufacturer and U.S. distributor of the allegedly infringing device) violated 35 U.S.C. § 271 of the Patent Act by allegedly selling and offering for sale a device that infringed a patent owned by the Plaintiff.

The allegedly infringing device is a registration control system used with newspaper and commercial printing presses. By way of background, four inks are used to print full-color images and those images are created by placing ink dots on a paper or other medium (web) to be printed. Color registration is the method used to check the location of the dots to ensure that the dots are properly aligned and the printed image remains in focus.Various methods have been developed to ensure that the dots are placed in the correct location and to ensure that any necessary corrections are made in the event the ink dots are not properly aligned. The most common method involves the placement of small registration marks that correspond to the particular colors on the web, which are referred to as "marked" systems or operating in a "marked" mode. Another method involves controlling registration using the printed image itself, rather than registrations marks, which are referred to as "markless" systems or operating in a "markless" mode.

The Plaintiff argued that the device sold by the Defendants in the United States infringed United States Patent No. 5,412,577 (the 577 Patent), because it allegedly has the capability to operate in both marked and markless modes, *i.e.,* with or without the use of registration marks. Defendants argued that the device sold in the United States was non-infringing, as it operates exclusively using registration marks—well known in the prior art—and has no "markless" capability. Defendants further argued that the 577 Patent not only failed to read on purely marked systems such as the one sold by the Defendants, but it expressly disavowed such systems by virtue of its criticism of prior art systems that used registration marks to control color registration.

After extensive discovery, a full evidentiary hearing and post-hearing submissions, the Court (Robreno, J.) issued a 31-page decision which accepted the Defendants' legal and factual position *in toto.* The Court found that the Plaintiff failed to prove a likelihood of success on the merits of its infringement claim, concluding, instead, that the 577 Patent disavowed the prior-art's use of registration marks. The Court found that the "disavowal stems from the prior-art's problematic use of registration marks distinct from the actual printed image or within the image, and the 577 Patent proposes to solve the problem." The Court further found that the "disavowal and criticism of prior-art in this case is unmistakable."

The Court found that the "disavowal stems from the prior-art's problematic use of registration marks distinct from the actual printed image or within the image, and the 577 Patent proposes to solve the problem."

The Court also concluded that the Plaintiff failed to prove the necessary element of irreparable harm, concluding that there was no proof establishing: (1) lost sales or lost market share; (2) a causal relationship between the alleged lost sales and the sale of the allegedly infringing product; (3) why money damages would not remedy its alleged injury; (4) that the Plaintiff practices the invention disclosed by the 577 Patent; or (5) why there was a 14-month delay from the Plaintiff's discovery of the alleged infringement to seeking injunctive relief. In short, the Court found that the Plaintiff's proof of irreparable harm was "conclusory, speculative and unsupported by any other evidence."

Onufrak

Kassak

Proper

Michael Onufrak, Chair of the Commercial Litigation Practice Group, Michael Kassak, Chair of the Intellectual Property Group and Justin Proper, partner in the Commercial Litigation Department represented the defendant, Print2Finish LLC. For more information about the attorneys and their practice, please visit www.whiteandwilliams.com.

BUILDING THE ELECTRONIC SAFE CONTINUED...

as the date and nature of breach, if possible. And, if more than 500 Californians are affected by a breach, the affected business would be required to submit a sample of the breach notification to the California Attorney General.

NEW LAWS AND RULES STRESS PREVENTION AS THE BEST MEDICINE

While the California data breach law focuses on notification after a security breach, the new Massachusetts Data Privacy Law (201 CMR 17), effective March 1, 2010, focuses on preventing breach of data security. The Massachusetts law requires all businesses that collect personal data of Massachusetts residents to adopt written security policies and utilize certain forms of encryption when handling personally sensitive data. Of course, firms cannot be compliant unless they understand how they handle sensitive personal information. For instance, a company that does not recognize how information flows within its own network, such as whether it transmits information over the internet or reaches third parties, could not comply with the Massachusetts law even if it had a policy in place.

Additionally, each company must revisit its security protocol to ensure that it is operational. A failure to comply with the law results in fines of $5,000 for each violation, $50,000 for each instance and $100 for every affected resident.

On August 1, 2009, the Federal Trade Commission (FTC) implemented the Red Flags Rule. Based on the Fair and Accurate Credit Transactions Act of 2003, the Red Flags Rule requires any company with invoices to establish written Identity Theft Prevention Programs.

The Rule allows each company's Identity Theft Prevention Program to vary considerably in complexity and scope. Programs are drafted based upon various "red flags," or instances where identity theft may occur. Accordingly, companies with a higher risk of identity theft in various transactions have more red flags, and consequently must draft more complicated policies to prevent identity theft. Companies with relatively straightforward transactions and lower exposure to risk of identity theft have fewer red flags, and accordingly simpler policies.

An Identity Theft Prevention Program must have a protocol in place for suspected instances of identity theft. These protocols may vary based on the nature of the risk. For instance, a business that detects unauthorized, irregular use of an account may monitor the account for evidence of identity theft, close the account completely, or even contact law enforcement immediately. Failure to comply with the Red Flags Rule may result in regulatory enforcement action and even hefty civil money penalties.

AND THERE'S MORE TO COME

Data security breaches undermine consumer confidence in businesses, and expose companies and consumers to potentially catastrophic risks. Just as the California notification law was adopted by state legislatures across the country, businesses should expect data security laws that focus on prevention, such as the Massachusetts law, to become the new status quo.

For more information regarding data privacy and security, please contact Ryan Udell (215.864.7152; udellr@whiteandwilliams.com) or Wasim Rahman (215.864.7186; rahmanw@whiteandwilliams.com).

DO I OWN WHAT I BOUGHT?

by Randy M. Friedberg, Esq.

Did you know that you can hire someone for a project, pay for the project, instruct that person how to do the project, and even enter into a signed agreement stating that the work is created for you, and still not end up owning the copyright to the work? Under the U.S. Copyright Law's work for hire section, it is true.

Every original work is protected by copyright law the moment it is reduced to a tangible form. And generally, that copyright is owned by the author of the work. An exception to this general rule is what is known as the work for hire provision of the Copyright Law.

Under work for hire, the copyright in a work is owned by the commissioning party either when it is (1) created by an employee acting within the scope of his or her employment; or (2) specially commissioned and the parties agree in a signed writing that the work will be made for hire, and even then only if the work fits within one of the categories expressly enumerated in the Copyright Law (contribution to a collective work, part of a motion picture, part of another audiovisual work, a translation, a supplementary work, a compilation, an instructional text, a test, answer material for a test, or an atlas).

So, whether a work may be said to be "for hire" requires a two-step analysis. The first step is to determine whether the work was created by an employee acting within the scope of his or her employment. If so, the work is owned by the employer and you need not proceed to the second step.

Care must be taken, however. In *Community for Creative Non-Violence vs. Reid,* 490 U.S. 730 (1989), the United States Supreme Court instructed that you look to the law of agency to determine who is an employee. The factors to consider are: the duration of the relationship between the parties, whether the hiring party has the right to assign additional projects to the hired party, the extent of the hired party's discretion,

continued on page 4...

White and Williams LLP
1650 Market Street
One Liberty Place, Suite 1800
Philadelphia, PA 19103-7395

DO I OWN WHAT I BOUGHT CONTINUED...

over his or her hours of work, the method of payment to the hired party, the hired party's role in hiring and paying assistants, whether the work is the regular business of the hiring party, whether the hiring party is in business, whether employee benefits are provided to the hired party and the tax treatment of the hired party. None of these is dispositive; all must be considered.

There are many reasons this analysis matters. In addition to determining ownership, it effects the term of the copyright (work for hire is 95 years from date of publication or 120 years from date of creation, whichever expires first, while a work not made for hire exists for the life of the author plus 70 years) and termination rights (which come into play 35 to 40 years after an assignment, but does not exist for a work for hire).

In sum, if you want to hire someone to create a work which you want to own, and the work does not fit within one of the categories set forth in the Copyright Law, you must contractually provide that the author assigns all of his or her interest in the work to you. You should also provide that the author will execute any documents required to give effect to this assignment. We strongly recommend that you require the author to also assign the author's rights in the work to you because determination of whether a work is a work for hire can be open to interpretation, even if you believe the work will be for hire.

For more information regarding the work for hire provision of the Copyright Law, please contact Randy Friedberg in our New York office at 212.714.3079 or friedbergr@whiteandwilliams.com.

EDITOR | MICHAEL O. KASSAK, ESQ.
856.317.3653
kassakm@whiteandwilliams.com

PRIMARY OFFICE: 1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103
REGIONAL OFFICES: Berwyn, PA | Boston, MA | Center Valley, PA | Cherry Hill, PA | Conshohocken, PA
New York, NY | Paramus, NJ | Pittsburgh, PA | Wilmington, DE