DORSEY

INTELLECTUAL PROPERTY UPDATE

A PUBLICATION OF THE INTELLECTUAL PROPERTY GROUP OF DORSEY & WHITNEY LLP

E-Burglary – Protecting Your Computer Data While Avoiding Lawsuits

In the not-too-distant past industrial espionage consisted of photocopying and carting out files. Identity theft, a rare crime until recent years, happened when someone's wallet was stolen by a pickpocket. The computer and the Internet have dramatically changed the playing field. Now, customer lists, marketing plans and financial information can be passed to the competition with a simple click of the mouse, and a high school hacker can break into computers that store a wealth of personal information.

Two laws, one that took effect just last year and the other just being discovered as a deterrent to computer theft, when taken together, not only require organizations to be responsible custodians of personal data stored in their computers, but also make the theft of data from a computer a federal crime that can be vindicated through a civil lawsuit. In response to these two laws, companies need to take a number of prudent measures.

The California Identity Theft Statute

The new California identity theft statute[1], effective since July 1, 2003, requires businesses operating in California to notify individuals when they have reason to believe an individual's personal information — social security number, driver's license number, etc — maintained as computer data has been stolen. The purpose behind this statute is to provide sufficient notice to individuals whose personal information has been stolen by an unauthorized person so they can take the appropriate steps to protect themselves from identity theft. This statute only applies to "unencrypted personal information."

The statute also expressly provides that individuals who are damaged by the failure to provide the notice required by the law have the right to bring lawsuits to recover any monetary losses caused by the failure to provide the required notifications. While the jurisdiction covered by this statute is limited to California, it applies to any business "that conducts business in California."

The Federal Computer Fraud and Abuse Act

In contrast, the Computer Fraud and Abuse Act (CFAA), does not impose obligations on custodians of computer data, but rather is a federal criminal statute designed to protect computer data from theft. The CFAA covers all computers used in interstate commerce. The CFAA is effective as a broad device to protect computer data because it permits a civil action — monetary damages and injunctive relief to retrieve the stolen data and prevent its use by a competitor.

Despite the fact that the CFAA has provided for civil relief since 1994, it was not until recently that federal courts around the country have relied upon the CFAA to uphold the right of businesses to protect their valuable information from competitors. Like the California identity theft statute, the CFAA is predicated on "unauthorized" access to computers and data.

Federal Court Interpretation of Authorization

Because the CFAA has been on the books far longer than the California identity theft statute, the federal courts have interpreted the CFAA in a number of significant cases to give breadth and meaning to what is and is not illegal "unauthorized" access to computer data. This article will examine those interpretations, and what pro-active steps a company can take to comply with the California statute and simultaneously position itself to take advantage of the powerful remedies offered by the CFAA to protect its valuable computer data.

In interpreting the CFAA, the federal courts have recognized two categories of unauthorized conduct — those inherent in common law principal/agency relationships and those explicitly established by the owner of the computer data. In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,[2] for example, the court held that employees who sent their employer's data via e-mail from a Shurgard computer to their new employer, a competitor, lost their authorization to use their employer's computer "when they committed this "serious breach of loyalty" to their employer.

While this legal precedent is good news for companies who will be able to use the CFAA to retrieve their stolen computer data from disloyal employees who join competitors and enjoin them from using the stolen data to compete against them, it has the opposite effect with respect to the California identity theft statute in which the company is responsible for notifications if the personal information is taken by an unauthorized person who is one of their own employees. Indeed, the California statute by its terms explicitly recognizes that a company employee is not "unauthorized" when the employee is not acting in "good faith."

The federal courts have also found access to be "unauthorized" when rules established and promulgated by the employer or owner of the computer data have been violated. In *US Greenfiber v. Brooks*,[3] the defendant, plaintiff's former Quality Control Manager, "removed from the computer assigned to her all documents, e-mail files, and Microsoft Office, including the Outlook e-mail program." The Court found that the defendant's taking of the computer data was unauthorized under the CFAA by virtue of the company's work rules and procedures established to protect the confidentiality of its computer data.

In addition to determining what is unauthorized in the corporate workplace, the federal courts have also opined on what is unauthorized activity with respect to taking data from public websites. An express rule, a term of use on the website prohibiting the use of an automatic robot to download data from the website, was relied upon by the court in *Register.Com, Inc. v. Verio, Inc.*[4] to find that the downloading by the defendant was unauthorized under the CFAA. Another case, *EF Cultural Travel BV v. Explorica, Inc.*,[5] relied upon a confidentiality agreement between the employer and former employees to find that the former employees lacked authorization under the CFAA to construct an automatic robot based on confidential information to download their former employer's pricing data through its website.

A number of practical lessons can be drawn from these cases to assist companies in complying both with the new California identity theft statute and in taking advantage of the remedies offered by the CFAA. These cases suggest a proactive program.

Protections Built Into the Computer Network

First, because there is no foolproof way to prevent the theft of data, there are technological solutions that can minimize such thefts. For example, Liquid Machines, a company, headquartered in Massachusetts, that provides information security management software has recently released a product that not only encrypts data, but it regulates from a central point in the company who in the company can access particular data and records Those rights can be revoked at any time, preventing former employees access to sensitive information once they leave the company. Vidius, a California-based company with another technology solution, has a product known as "Port Authority" which can make it impossible for certain sensitive information such as social security numbers or specific documents to leave the network.

Company Policies and Procedures

Companies have enormous options to establish the rules by which employees under various circumstances are entitled to access the company's computer data — work rules, employee handbooks, compliance policies and confidentiality agreements. As with the restrictions built into the network, the key overriding principle is to limit data to those with a legitimate need to use the information to perform their job functions. It is also important to post rules on a public website to establish authorized access to data.

In addition to restricting physical access, rules should be established recognizing that computer data can be easily removed from the workplace by sending it via e-mail or copying data to easily hidden devices. A business that allows telecommuting or has a sales force must decide what rules will govern the removal of computer data from the workplace.

Employee training is a critical part of this process. It is important not only in conveying the rules to the

workforce concerning who is entitled to access which computer data and under what circumstances, but in impressing the importance of being vigilant for thefts of personal data so that notices, as the California Act requires, can be provided on a timely basis and appropriate action can be taken to retrieve the stolen data — either through the CFAA or by reporting the theft to law enforcement.

Proving Illegal Access to the Data

Finally, an integral component of any sound data protection program is the ability to prove that an unauthorized access occurred. This is important under the California law, since having reason to believe that the personal data has been acquired by an unauthorized person triggers the notification requirement. It is equally important if a company should decide to take advantage of the civil remedies offered by the CFAA. The technology solution mentioned above from Liquid Machines, for example, also tracks the flow of a document though the network, providing an evidentiary trail showing who accessed, printed or e-mailed a particular document.

EU Compliance

Many companies now operate on an international basis and the Internet has enabled even small businesses to operate in the global market. However, the lure of attracting and doing business in other parts of the world at the touch of a button and without having to incur the operational costs of physically setting up an overseas office, must be contemplated carefully. The Internet has undoubtedly removed certain physical barriers to entry, however, there are invisible barriers that can catch the unsuspecting company. In the EU, access to data (authorized and unauthorized), data protection and privacy is stringently protected; the mere transfer of personal data to, for example, the US is fraught with regulation. Companies with subsidiaries or other form of presence in the EU need to ensure even stricter compliance with regard to accessing and protecting such data.

In short, most companies right now probably could not comply with the new California statute, nor could they successfully mount a legal challenge to confidential data taken from their computers. The prudent CEO or CFO working with its IT department, the general counsel, the company's compliance officer and the company's human resources professional, should address these needs sooner rather than later if they want to protect their company's confidential and proprietary information.

---

1 § 1798.82, et. seq. of the California Civil Code

2 119 F. Supp. 2d 1121 (W.D. Washington, 2000)

3 No. Civ. A. 02-2215, 2002 WL 31834009, at *3 (W.D. La. Oct. 25, 2002)

4 126 F. Supp. 2d 238 (S.D.N.Y. 2000)

5 274 F.3d 577(1st Cir. 2001)

THE AUTHOR

Nick Akerman
New York
202.415.9217
akerman.nick@dorsey.com

A partner in the Trial Group, Nick's practice focuses on corporate governance and compliance, intellectual property litigation, technology, Internet and e-commerce, trial, white collar crime and civil fraud.

For further information regarding our intellectual property law practice, please contact any group leader.

Trademark, Copyright & Brand Management Group

Elizabeth Buckingham, Minneapolis
612.343.2178
buckingham.elizabeth@dorsey.com

Patent Group

Lee Osman, Denver
303.629.3434
osman.lee@dorsey.com

Franchise & Distribution Group

Nancy Smith, San Francisco
415.544.7017
smith.nancy@dorsey.com

James Hermsen, Seattle
206.903.8852
hermsen.james@dorsey.com

IP Litigation Group

Ralph Taylor, Washington, D.C.
202.442.3562
taylor.ralph@dorsey.com

Dorsey & Whitney offices that offer intellectual property services

Denver
Des Moines
London
Minneapolis
Missoula
New York
Palo Alto
San Francisco
Seattle
Washington, D.C.

For change of address or subscription:

Toni Byard, Minneapolis
byard.toni@dorsey.com
612.340.7824

DORSEY

INTELLECTUAL PROPERTY UPDATE

USA CANADA EUROPE ASIA

Dorsey & Whitney is a full-service international law firm with core practices in the areas of intellectual property, corporate securities and finance, M&A, international law and complex litigation.

Vol. 4 — No. 2

Dorsey & Whitney LLP
Suite 1500
50 South Sixth Street
Minneapolis, MN 55402-1498