PROSKAUER ROSE LLP®

Client Alert

A report
for clients
and friends
of the firm

March 2005

ChoicePoint Data Theft a Wake-Up Call for Companies to Evaluate Their Legal Exposure for Computer and Data Security Breaches

The recent well-publicized security breaches involving consumer data — such as ChoicePoint's disclosure to identity thieves of personal information concerning 145,000 Americans — are leading businesses to evaluate their exposure to legal claims, and to re-evaluate their business practices concerning the protection of consumer data.

There Is No Across-the-Board Standard for Data or Computer Security

Financial institutions and healthcare providers that possess personal information have privacy and security rules imposed upon them by federal law, the Gramm Leach Bliley Act (GLBA) and HIPAA. (For example, the FTC recently proceeded against Nationwide Mortgage Group for violation of the GLBA safeguards and privacy rules, alleging that the company failed to protect against computer network vulnerabilities that would expose customer information to attack, and failed to assess its security risks). Under the 2003 Fair and Accurate Credit Transactions Act (FACTA), effective June 1, 2005, businesses must take reasonable measures to destroy information obtained from consumer credit reports before discarding them. And under Section 5 of the FTC Act and its state analogues prohibiting unfair and deceptive trade practices, companies that expressly or impliedly promise data security must live up to those promises or face liability. (The FTC so far has filed only a handful of actions in the area of information security, but is promising more enforcement. State Attorneys General have been slightly more aggressive in their enforcement efforts. In a recent example, Ziff Davis settled with multiple attorneys general after hackers broke into its customer database and stole names and credit card numbers, at a time when the online Ziff Davis privacy policy promised safeguarding personal data). Still, despite these piecemeal regulations and episodic enforcement, there is no national standard for data security. Should an unregulated company therefore feel safe from liability for data security breaches?

Victims of Crime Normally Not Responsible for Criminal Acts

Normally, a company that is a victim of a crime is not responsible for losses to others. Identity theft, whether from computer hacking or otherwise, is a crime. But many believe that principle of immunity should be narrowed when the crime is foreseeable and preventable — their theory is a little like an apartment building owner being liable for attacks on his property when he knows criminals are lurking and how they get in to attack the tenants. Computer-using companies counter that it almost always is impossible to predict how hackers or scammers will attack, and therefore the companies should not have liability. But pleading ignorance of high-tech criminal techniques will only go so far as a defense.

Plaintiffs' Lawyers Are Employing Various Theories of Liability

Private civil actions may create new law in the area of data security. ChoicePoint itself has been sued, following the revelations of its massive personal data disclosures, for "willful noncompliance" with the Fair Credit Reporting Act (governing disclosures of

consumer reports), for invasion of privacy and misappropriation, and for violations of California consumer protection statutes. All of the claims stem from ChoicePoint's alleged negligence in failing to have proper safeguards against disclosure. ChoicePoint also has been sued for securities fraud, for failing to reveal or misstating its data vulnerabilities.

Bank of America currently is being sued by a company that alleges inadequate security allowed thieves to steal funds from the company's online account with the bank.

As data disclosures become more notorious, creative plaintiffs' counsel will find new and untested ways to challenge the custodians of the data — companies with customer information in their computers and files. Virtually every company is a custodian of data, and a potential target for liability.

California Law Imposes a Duty to Notify Persons of Computer Security Breaches

In the meantime, as the theories of liability percolate, there is an important current California law *applicable nationwide to companies holding data of California residents*. Under California Civil Code § 1798.82, *et seq.*, companies must notify California residents if personal information maintained in computerized data files has been compromised by unauthorized access. Californians must be notified when their name is obtained illegitimately from a server or database with other personal information such as their social security number, driver's license number, account number, credit or debit card number, or security code or password for accessing an account. There are specific rules on how notice must be provided.

Congress Is Considering New Laws to Deal With Data Disclosures

The United States Congress currently is considering a federal notification standard modeled on the California law just mentioned. There also are proposals for regulation of credit bureaus such as ChoicePoint. And bills are pending that would ban the sale of social security numbers, which facilitates much identity theft.

What Should a Company Do While the Law Sorts Itself Out?

In light of the patchwork of actual or potential regulations, what should companies be doing to limit their exposure to liability if personal data in their possession leaks out through others' wrongdoing? At a minimum, we recommend the following:

- Review all publicly disseminated policies, online and off, to make sure you are not promising or suggesting more than you can deliver when it comes to privacy or data security.
- If you view yourself as unregulated under Gramm Leach Bliley or HIPAA, it may be worthwhile to confirm your status with counsel, as many entities have obligations under the statutes of which they are unaware.
- Make sure that all known or suspected computer vulnerabilities are addressed promptly and professionally. A computer security audit from an outside firm can help document your reasonableness.
- Review your business partners' obligations to safeguard data and spread the risk where you can.
- Explore liability insurance for data security breaches.

NEW YORK • LOS ANGELES • WASHINGTON
BOSTON • BOCA RATON • NEWARK
NEW ORLEANS • PARIS

For further information, contact Chris Wolf, Chair of the Proskauer Privacy and Security Practice Group, 202-416-6818, cwolf@proskauer.com. Chris advises and represents clients on international, federal and state privacy and data protection laws. He is a member of the New York and Washington Electronic Crimes Task Forces established by the United States Secret Service, and is an adjunct professor of Internet and Privacy Law at the Washington & Lee University School of Law.

Proskauer Rose is an international law firm that handles a full spectrum of legal issues worldwide.

You can also visit our Website at **www.proskauer.com**