

Privacy Litigation Update

August 31, 2007

New State Data Security Law Extends Liability for Security Breaches

In the wake of the largest credit card security breach involving TJX Companies, Inc.'s computer system, states have a renewed interest in pursuing legislation that protects consumers and punishes companies responsible for data breaches. Although more than two-thirds of states have passed various breach notification statutes, until May 2007 no state had enacted any of the Payment Card Industry ("PCI") standards, which consist of 12 data security controls developed by the major credit card associations. That fact changed, however, on May 21, 2007, when Minnesota became the first state to enact one of the PCI standards into law.

Minnesota's "Plastic Card Security Act" (the "Act"), which goes into effect after August 1, 2008, will impact companies that conduct credit or debit card transactions in Minnesota. The Act is broad in its scope, as the security breach does not have to take place in Minnesota, nor does the financial institution affected need to be located there. Any company or entity conducting business in Minnesota that accepts an "access device"—a magnetic stripe data or processor chips—must guarantee that it will not retain Track II data (the information drawn from magnetic stripes) or personal identification numbers ("PINs") once a credit or debit card transaction has been completed. Minnesota's prohibition against Track II data and PIN storage echoes the PCI standards' commitment to protecting cardholder data.

Minnesota's new data security law reflects a growing desire among states to shift the responsibility for data security breaches from banks, credit unions, and other financial institutions to retailers and merchants in possession of credit card information. Prior to the passing of the law, banks and credit unions were primarily

responsible for dealing with the expenses linked to data breaches. Now, once a company has violated the Act's anti-storage prohibition, it must reimburse the financial institution that issued the credit or debit card for the "reasonable costs" affiliated with responding to the breach. Costs may include those associated with notifying customers about breaches, closing accounts, or reissuing cards.

Minnesota is not alone in its commitment to increased scrutiny of merchant and retailer handling of consumer data. At least five other states—California, Connecticut, Illinois, Massachusetts, and Texas—are in the process of drafting legislation to curtail data security breaches. As other states follow Minnesota's example, merchants may be held strictly liable for data breaches that arise during the course of their business operations. Yet, even if only a few states enact statutes similar to the "Plastic Card Security Act," Minnesota may host a great deal of litigation due to the Act's broad territorial scope. As a result, companies that accept or store credit or debit card information should remain aware of the changing climate toward merchants and begin considering strategies for risk management in the event of data security breaches.

In This Issue

New State Data Security Law Extends Liability for Security Breaches	Page 1
Avoiding Liability for the Unauthorized Use of Discarded Information	Page 2
Federal Trade Commission Issues Guidelines for Securing Personal Information	Page 2
Sixth Circuit Decision Extends Privacy Expectation to E-mail	Page 3

Avoiding Liability for the Unauthorized Use of Discarded Information

In addition to potential bank or credit union reimbursement under current and prospective data security laws, companies should note the prospect of liability under the Fair and Accurate Credit Transactions Act (“FACTA”). Under § 1681c(g)(1), “no person that accepts credit cards or debit cards for the transaction of business shall print more than the last five digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.” Recently § 1681c(g)(1) has become the basis for many consumer class action lawsuits, specifically in California, Illinois, New Jersey, and Pennsylvania.

While many companies have challenged § 1681c(g)(1), claiming that it is vague and ambiguous, courts have held that the statute has only one reasonable meaning: that a receipt may not contain (1) the printing of more than the last five digits and (2) the expiration date. Any person who “willfully fails to comply” with Fair Credit Reporting Act (“FCRA”) requirements may be liable for “actual damages sustained by the customer as a result of the failure or damages of not less than \$100 and not more than \$1,000.” “Willful failure” has been interpreted to mean a knowing and reckless disregard of the FCRA. A company’s action will be considered a reckless disregard of the law when there is a violation of an FCRA provision and a plaintiff can demonstrate that the company ran a risk of violating the law “substantially greater than the risk associated with a reading that was merely careless.”

If a company has failed to abbreviate credit or debit card receipts, a consumer may bring a private cause of action for statutory damages, which may include punitive damages. Notably, courts have typically held that plaintiffs may be entitled to statutory and punitive damages even without proof of actual economic harm or loss.

Federal Trade Commission Issues Guidelines for Securing Personal Information

For companies attempting to implement security measures for the safekeeping of their customers’ and employees’ personal information, the Federal Trade Commission’s (“FTC”) newly released guidelines may be of assistance. The FTC’s guide entitled “Protecting Personal Information: A Guide for Business” designates

five critical principles that companies should follow when dealing with security issues relating to personal information.

Take Stock: Know What Personal Information You Have on Your Computers

The FTC guide recommends that every business assess what types of personal information it possesses and identify which individuals have access to that information. The FTC advises that companies make an inventory of all of the computer systems they use for storing secured data, such as computers, servers, laptops, disks, and backup tapes.

Scale Down: Keep Only What You Need to Conduct Business

Unless the retention of sensitive personal information has a legitimate business purpose, businesses should not retain such information beyond applicable retention requirements. If a business’s software settings automatically keep personal information, those settings should be changed to avoid permanent retention of information. For companies that have to retain information for business purposes or for compliance with the law, a written records retention policy should be established.

Lock It: Protect the Information That You Keep

The FTC highlights the four aspects of a highly effective data security plan: (1) physical security; (2) electronic security; (3) employee training; and (4) security practices of contractors and service providers. Regarding physical security, the FTC encourages businesses to limit access to hard-copy information as well as computer files, Zip drives, and backup tapes. Businesses also may improve electronic security and manage for risk by examining their employees’ usage of passwords, laptops, and wireless and remote access. The FTC also underscores the importance of providing proper training to employees regarding the use, retention, and disposal of sensitive personal information. Lastly, companies should establish an open dialogue with any contractors or service providers they use in order to effectively handle security issues as they arise.

Pitch It: Properly Dispose of What You No Longer Need

To minimize security breaches, companies should develop specific disposal practices to discard sensitive information that no longer needs to be retained. Unnecessary papers should be shredded, burned, or otherwise destroyed in accordance with the FACTA Disposal Rule. EN.16 C.F.R. § 682. Old computers and other storage devices should be disposed of through wipe utility programs.

Plan Ahead: Create a Plan for Responding to Security Incidents

Companies should establish response plans that include immediate investigation of breaches and prompt notification to the customers, financial institutions, and other entities affected by incidents. Planning and preparing for security incidents will facilitate a prompt business response in the event that a security breach actually happens.

While the FTC guide offers an overview of data security principles, it is not an exhaustive list of the security practices that businesses should be using in their day-to-day functions. Companies should use the guide as a starting point for planning their data security policies and consult with counsel to determine the reasonableness and defensibility of such policies. Ultimately, to safeguard personal information belonging to both customers and employees, companies will need to be mindful of how compliance with the FTC recommendations will impact the specific needs of their businesses.

Sixth Circuit Decision Extends Privacy Expectation to E-mail

A recent decision by the Court of Appeals for the Sixth Circuit involving warrantless searches and seizures and commercial Internet Service Providers (“ISPs”) has expanded the degree of privacy e-mail users should expect with regard to their e-mail messages. In *Warshak v. United States*, the federal government initiated a criminal investigation of Steven Warshak and obtained a court order under the Stored Communications Act (“SCA”) to compel two commercial ISPs to disclose the contents of his e-mail accounts. Another court order, issued under the SCA, permitted the government to delay notifying Warshak about the e-mail disclosures for 90 days. When Warshak learned of the disclosures a year later,

he filed suit, alleging that the compelled disclosure of his e-mails without a warrant violated both the SCA and the Fourth Amendment.

The Sixth Circuit emphasized that e-mail users have a “reasonable expectation of privacy in the content of their e-mails.” Modifying the injunctive order issued by the district court, the court held that the government did not have the right to access and view e-mails stored by a commercial ISP without either: (1) obtaining a search warrant under the Fourth Amendment based on probable cause; (2) providing the account holder with prior notice and an opportunity to be heard; or (3) making a fact-specific showing that the account holder had no expectation of privacy regarding the ISP.

In addition to upholding an injunction against the government, the Sixth Circuit concluded that the portion of the SCA allowing e-mail disclosure with delayed notice to the account holder violated the Fourth Amendment. For this reason, the court enjoined that particular unconstitutional section of the statute involving delayed notice. Ultimately, by asserting that account holders have an expectation of privacy in their e-mails, the Sixth Circuit has limited the government’s access to private e-mails stored by ISPs.

This likely means that companies’ e-mail management systems may become the target of further subpoenas and litigation inquiries. The most defensible and proven way to mitigate the risks associated with e-mail usage in the business environment is to implement an e-mail management policy that leverages an archiving system to capture, retain and, when permitted by law, dispose of business records constituting e-mails. Such policies will ease the burden on computer servers and reduce the volume of information reviewed in eDiscovery. Coupled with the privacy consideration and last year’s adoption of the eDiscovery amendments to the Federal Rules of Civil Procedure, the time to confront these issues is now.

For further information on Vedder Price’s privacy litigation team, please contact Timothy J. Carroll at 312-609-7709 or tc Carroll@vedderprice.com, or Bruce A. Radke at 312-609-7689 or bradke@vedderprice.com. The editors express their gratitude to Rachel Luberda, a student at The University of Notre Dame Law School, for her assistance in preparing these articles.

VEDDER, PRICE, KAUFMAN & KAMMHOLZ, P.C.

About Vedder Price

Vedder, Price, Kaufman & Kammholz, P.C. is a national, full-service law firm with approximately 240 attorneys in Chicago, New York, Washington, D.C. and New Jersey.

Commercial Litigation Group

The Vedder Price litigation practice group gives constant attention to providing cost-effective and efficient legal services, regardless of the size of the matter, and continuously updates clients with respect to estimated and actual expenses of litigation. Over the years, Vedder Price trial attorneys have been involved in a significant number of cases that have shaped the course of the law in various substantive areas at the local, state and national level. In addition to general business litigation experience, Vedder Price litigators have special knowledge in a number of areas, including the following:

- Antitrust, Unfair Competition and Intellectual Property Litigation
- Bankruptcy and Creditor Rights Litigation
- Commercial and Financial Institution Litigation
- Consumer Litigation
- Gaming Law
- Insurance Litigation
- Manufacturers Liability
- Real Estate and Land Use Disputes
- Records Management and eDiscovery
- Securities Litigation
- Tax Litigation
- Criminal Defense
- Alternate Dispute Resolution

Privacy Litigation Update is published periodically by the law firm of Vedder, Price, Kaufman & Kammholz, P.C. It is intended to keep our clients and interested parties generally informed about privacy-consumer issues. It is not a substitute for professional advice. For purposes of the New York State Bar Rules, this bulletin may be considered ATTORNEY ADVERTISING. Prior results do not guarantee a similar outcome.

© 2007 Vedder, Price, Kaufman & Kammholz, P.C. Reproduction of this bulletin is permitted only with credit to Vedder Price.

Contact the following for privacy-related counseling and risk-mitigation efforts:

Timothy J. Carroll
312-609-7709

John H. Eickemeyer
212-407-7760

Diane M. Kehl
312-609-7664

James S. Montana (Practice Area Leader)
312-609-7820

Michael R. Mulcahy
312-609-7513

Bruce A. Radke
312-609-7689

Michael J. Waters
312-609-7726

Chicago

222 North LaSalle Street
Chicago, Illinois 60601
312-609-7500
Fax: 312-609-5005

New York

1633 Broadway, 47th Floor
New York, New York 10019
212-407-7700
Fax: 212-407-7799

Washington, D.C.

875 15th Street NW, Suite 725
Washington, D.C. 20005
202-312-3320
Fax: 202-312-3322

New Jersey

Five Becker Farm Road
Roseland, New Jersey 07068
973-597-1100
Fax: 973-597-9607