Merchant Liability and Breaches In Payment Card Security Standards

According to a recent report, there has been almost a 50 percent increase in reported data security breaches at businesses, government agencies and educational institutions since 2007. The financial losses to affected companies also have increased.

Surveyed companies reported that average data breach response and business costs rose in 2008, with the per-victim cost to the affected company of some $202 per affected consumer, an increase of nearly 40 percent since 2005. To counter this trend, many states have enacted or strengthened privacy laws that have regulated, among other things, the display of Social Security numbers, encryption of sensitive consumer information, secure disposal of consumer data, and the scourge of malware.

Beyond legislation, merchants and certain financial institutions that handle credit card transactions must also comply with the Payment Card Industry Data Security Standards (or PCI standards), industry standards promulgated by the major credit card brands that are a baseline of important security controls to safeguard sensitive cardholder data.

This article discusses the PCI standards and credit card transactions generally, recent litigation, and state legislative developments in the area of merchant liability for data security breaches.

PCI Standards in General

The PCI standards are a comprehensive set of 12 data security requirements imposed on all entities that process, store or transmit certain sensitive “cardholder data,” comprising merchants, banks and credit card transaction processors. The 12 core principles center around certain data security requirements, including, among other things, installing firewalls and anti-virus software, protecting stored cardholder data, restricting access to sensitive information, and monitoring data access.

Since security breaches allegedly occurred to some Payment Card Industry-compliant companies, commentators have questioned the effectiveness of the PCI standards and have cautioned that while they are excellent security baselines, they do not necessarily mean a network is 100 percent secure.

The PCI standards detail specific policies, procedures, network architecture requirements and other measures that entities must adopt to protect sensitive cardholder data that is processed during a transaction. The standards are not law. Rather, they are industry standards promulgated under contract by a council of the major credit card payment brands to regulate their member acquiring banks, who in turn are responsible for ensuring that merchants and businesses, for whom they process transactions, conform to the standards.

Simply put, an “acquiring bank” is a bank that processes credit card transactions on behalf of merchants, as opposed to an “issuing bank,” which issues credit cards to consumers.

Verification of PCI compliance can be performed by a qualified security assessor and quarterly network scans by an approved scan vendor, and in certain circumstances, smaller merchants may complete a self-assessment questionnaire.

Failure to comply can result in fines, additional audit requirements or the suspension of the ability to process credit card transactions.

Every two years, the PCI Standards Council updates the PCI standards, and also periodically releases new guidelines on emerging security areas. For example, in August 2008, the council announced new draft requirements to improve the security of personal identification number-based transactions for unattended payment terminals (e.g., self-service ticket machines, automated fuel pumps).

Until now, security requirements centered on traditional point-of-sale devices in the traditional retail staff environment. In October, the council also released an updated version of the PCI standards. According to a council statement, PCI standards Version 1.2 did not “introduce any new major requirements,” but clarified definitions regarding the best practices for particular data security safeguards.

Credit Card Transactions

Generally speaking, every time a cardholder uses a credit card to pay a merchant for goods or services, the issuing bank, acquiring bank and merchant must interact to process and complete the transaction.

After the merchant’s computer scanners “read” the cardholder information contained in the magnetic strip, the merchant then sends the pertinent account information...
through the network to the issuing bank. The issuing bank reviews the cardholder information and, assuming the card is valid with sufficient available credit, it authorizes the transaction.

Upon receiving notification, the merchant completes the transaction with the cardholder, and then forwards the receipt to the acquiring bank who pays the merchant. The acquiring bank then notifies the issuing bank that payment has been received, and the issuing bank pays the acquiring bank and charges the cardholder. See generally Sovereign Bank v. BJ’s Wholesale Club Inc., 533 F.3d 162 (3d Cir. 2008).

However, as the cardholder information is transmitted to and from the merchant, there are security risks. Cyber-thieves could potentially intercept the transmission and steal sensitive personal information, which is why the PCI standards require encryption for card information transmitted over public networks.

In addition, criminals could also infiltrate the merchant’s own computer systems and steal consumer information; hence, the PCI standards mandate numerous security precautions to protect against network intrusions, including firewalls, log monitoring, access controls, and periodic vulnerability scans to ensure the merchant’s system has not been compromised.

Recent Litigation

In the past year, there have been a number of lawsuits that directly and indirectly involve the PCI standards.

In July 2008, the U.S. Court of Appeals for the Third Circuit held that credit card issuing banks may seek reimbursement for losses in connection with a data network security breach at a retailer on the theory that they were intended beneficiaries of the information security agreement between the retailer’s payment processor/acquiring bank and the credit card system. See Sovereign Bank, supra.

The credit card issuing banks had brought suit against the retailer and the acquiring bank, claiming a large-scale breach at the retailer caused the issuing bank to incur expenses related to unauthorized charges.

Notably, the appeals court distinguished a prior decision, In Re TJX Companies Retail Security Breach Litigation, 524 F.Supp.2d 83 (D. Mass. 2007), which involved nearly identical facts. In TJX, the district court dismissed actions by a class of issuing banks that sought to recover their costs arising out of a merchant’s security breach and ruled that a later version of the Visa Operating Regulations (which, among other things, mandates compliance with the PCI standards) adopted after the events of Sovereign Bank expressly precluded an intended beneficiary theory.

Following breaches of sensitive information, consumer litigants asserting negligence claims against retailers and other holders of consumer data are increasingly claiming that the applicable duty of care for credit card data security should be PCI compliance.

In response, companies that were certified PCI compliant at the time of a breach are contending that they met the standard of care and should not be held liable.

For example, in the TJX security breach litigation, a computer forensic audit revealed that the retailer failed to comply with nine out of 12 PCI standards requirements, a fact that the class action plaintiffs in the case asserted against the retailer; a final settlement to the

To stem cyber intrusions, Heartland’s CEO appealed for more industry sharing of known system vulnerabilities and updated procedures to stem future cyber-attacks, including industry wide, end-to-end encryption to safeguard cardholder data and updated security to detect network anomalies in real time.

Most recently, in January, Heartland Payment System, a credit and debit card processor, announced the discovery of malicious software that compromised its network and produced suspicious activity surrounding processed card transactions. In response, at least four putative class action lawsuits have been filed against Heartland, alleging federal statutory claims as well as breach of contract, negligence and state privacy law claims.

In one complaint, the plaintiffs claim Heartland breached a duty to exercise reasonable care in safeguarding and protecting such information from being compromised and/or stolen. According to the complaint, this duty arose, in part, from contractual duties expressly imposed upon Heartland from “agreements between Defendant and third parties, and industry standards (such as PCI).” See ¶59 of plaintiffs’ Complaint, Cooper v. Heartland Payment Sys. Inc., 09-00392 (D.N.J. Complaint filed Jan. 27, 2009).

In addition, at least two issuing banks have filed putative class actions seeking to recover the costs of canceling and reissuing credit cards compromised in the Heartland breach. See e.g., Tricentury Bank v. Heartland Payment Sys. Inc., 09-00697 (D.N.J. Complaint filed Feb. 13, 2009).

Specifically, the banks claim Heartland breached its obligations under the PCI standards in failing to prevent or contain the intrusion to its networks and that the plaintiffs are intended third-party beneficiaries of these agreements. The banks also assert negligence claims, alleging that Heartland failed to properly manage the encryption of sensitive credit card data and failed to comply with the PCI standards.

Merchant Liability Legislation

Following the newsworthy breaches of the last few years, state legislators have introduced numerous bills to strengthen consumer privacy concerning data disposal practices, data sharing, account information displayed on payment card receipts, the use and display of social security numbers on public records, encryption requirements for certain sensitive information, and amendments to breach notification laws.

More pointedly, the states have also sought to codify, in part, the PCI standards and impose liability upon merchants for the reimbursement of replacement card and other breach-related costs borne by financial institutions.

Generally speaking, the PCI standards are
integrated in two different contracts, namely, the agreements between merchants and acquiring banks, and the agreements between acquiring banks and credit card brands.

As a result, following a data security breach that compromises consumer credit card information, a successful lawsuit might be brought by the acquiring bank against the merchant, or the credit card brand against the acquiring bank. The issuing banks, however, are not parties to those agreements and the Third Circuit’s Sovereign Bank ruling notwithstanding, they have faced obstacles in recovering their costs in reissuing credit cards following a breach caused by a merchant or acquirer.

Thus, some state legislators have taken up so-called merchant liability bills that seek to codify certain portions of the PCI standards and allow financial institutions to recover certain costs stemming from a merchant’s data breach.

In 2007, Minnesota enacted the Plastic Card Security Act, and it currently remains the first and only state to pass such merchant liability legislation. Minn. Stat. § 325E.64 (Supp. 2007). The statute essentially codifies fundamental PCI security standards (namely, Requirement 3 concerning the controls on credit card authentication data) into law for merchants conducting business in Minnesota that handle sensitive consumer data. It grants financial institutions (not consumers or cardholders) the right to recover security breach-related costs from merchants who retain certain credit and debit card transaction data beyond the time frames set forth in the statute.

Under the statute, such transaction data includes the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data following the authorization of a transaction.

Bills Under Debate

Over the past several years, similar state merchant liability bills have died in various state legislatures, but at least three bills remain under debate.

For example, a Texas bill (H.B. 345) would require businesses that collect sensitive personal information consumer data through a credit card access device to comply with PCI standards or face potential liability to financial institutions for certain costs of data breaches. A business could avoid liability if it provides proof of compliance with the PCI standards as issued by an authorized auditor, or contracts its data security to a third-party, who has agreed to comply with the PCI standards.

A Washington state bill (H.B. 1149) would provide financial institutions a cause of action against businesses that violate magnetic stripe data retention requirements similar to the Minnesota statute, and suffer a data security breach affecting more than 5,000 or more unencrypted individual names or account numbers.

The current version of a New Jersey merchant liability bill (A2270) appears broader than the others because it would apply to not only merchants, but those entities covered under the state’s data breach notification law, and would impose liability for breaches of any protected personal information (not just payment card transaction data).

Conclusion

The recent Hannaford and Heartland data security breaches have raised issues about the potential limitations of the PCI standards. It has been reported that both companies had been certified PCI compliant, though only a forensic investigation will determine whether the companies were PCI compliant at the time the breaches occurred and whether certain required network and file-integrity checking tasks were performed.7

Since the breaches allegedly occurred to PCI-compliant companies, commentators have questioned the effectiveness of the PCI standards and have cautioned that while the PCI standards are excellent security baselines, they do not necessarily mean a network is 100 percent secure.8 Indeed, to stem cyber intrusions, Heartland’s CEO appealed for more industry sharing of known system vulnerabilities and updated procedures to stem future cyber-attacks, including industry wide, end-to-end encryption to safeguard cardholder data and updated security to detect network anomalies in real time.9

It remains to be seen whether the credit card brands will institute stricter security controls on merchants and payment processors in response to recent developments.


6. More notably, in 2007, California Governor Arnold Schwarzenegger vetoed a merchant liability bill. Again, in 2008, he received an amended merchant liability bill (A.B. 1656) that was re-introduced in the legislature, which would have prohibited businesses and agencies that process credit cards from storing or sending sensitive data without complying with certain security standards similar to the PCI standards.

