

The Payment Card Industry Data Security Standard: The Sleeping Giant is Wide Awake

Charles H. Kennedy
Of Counsel, Morrison & Foerster, LLP

INTRODUCTION

Plagued by a series of high-profile losses of cardholder data, the major payment card associations are more determined than ever to enforce their security standards. Merchants who fail to comply with the Payment Card Industry Data Security Standard face heavy financial penalties and loss of their ability to accept debit and credit cards. This White Paper explains how the Standard works, how it is enforced, and how litigation and new legislation are reinforcing the Standard's requirements.

One of the headline business events in 2007 was the spectacular loss of payment card data at TJX Companies, Inc., followed by investigations and lawsuits in which both banks and customers demanded that TJX pay damages. Less spectacularly, but no less importantly, the payment card industry tightened up its enforcement of the PCI Standard, and state legislatures considered (and Minnesota enacted) legislation intended to add an additional layer of liability for merchants who permit customers' card data to be compromised. Putting all of this together, 2007 saw a focus on payment card data security that will carry forward into 2008 and beyond.

The purpose of this White Paper is to provide further perspectives about the new PCI Standard environment. Specifically, it will review:

1. Why the PCI Standard is necessary;
2. What actions, including sound records management and disposal, the Standard requires;
3. How the Standard is enforced;
4. How private lawsuits and new legislation compound the risks that companies handling payment card data will face.

Charles Kennedy is of counsel in the Washington, DC offices of Morrison & Foerster LLP. He is also an adjunct professor of law at the Columbus School of Law, Catholic University of America, and the author or co-author of four books on the law of electronic communications. Mr. Kennedy can be reached at ckennedy@mofo.com.

WHY DOES THE CARD INDUSTRY NEED THE STANDARD?

The PCI Standard is needed because of two important facts:

1. Payment card transactions move huge amounts of valuable data among multiple players, creating many opportunities for data theft, fraud and monetary loss;
2. In the absence of a system like the Standard, merchants and other entities that use and manage card data lack incentives to handle that information securely. The Standard therefore requires all parties to transactions to handle card data with care, and penalizes those merchants and other entities that fail to do so.

To understand the first point – that is, how card data is handled and how it can be compromised – we need to know how card transactions work. To simplify our story, we will describe a transaction in which a customer presents a credit card to a cashier at a retail store.¹

A Typical Credit Card Transaction

The customer is known for our purposes as the *cardholder* – that is, a consumer who has been granted credit by a financial institution that serves as a *card issuer*. Each charge made on the card is a loan from the issuer to the cardholder. The issuer bills the cardholder for amounts charged to the card and earns interest on outstanding balances.

When the cardholder presents the card at the checkout counter, a third player enters the scene. This is the *merchant*, which in our example is the retail store. If the merchant has arranged to accept cards of the type presented by the cardholder, the cashier will initiate the transaction process. This process also involves a number of additional players.

The first of these additional entities is known as the *merchant acquirer*, *acquiring bank* or simply the *acquirer*. The acquirer is a financial institution that enters into relationships with merchants rather than card holders. (In the cases of American Express, Discover and Diners Club, the same institution acts in both capacities – that is, as the card's issuer and the acquirer of merchants who accept the card.)

The acquirer becomes involved when the cashier keys in the purchase information or the cardholder swipes the card on a card reader. These actions initiate an authorization request, which is transmitted to the acquirer. If the acquirer has delegated its transaction processing chores to a contractor, that contractor is called a *transaction processor*, or simply a *processor*. For purposes of our example, we'll assume that the acquirer is processing the transaction on its own behalf.

When it receives the authorization request, including the merchant identification, transaction amount, card number, credit limit, and expiration date, the acquirer forwards the information electronically to the card issuer, which confirms the authenticity of the card and the availability of credit for the amount of the purchase. This process results in a return transmission to the acquirer, either authorizing or denying the charge. The acquirer forwards the response to the merchant.

The process we have described so far is commonly called the *authorization process*. At this point, no money has changed hands. The financial transactions associated with the card purchase come next, in what is commonly called the settlements process.

Our merchant starts the settlements process at the end of the business day, when it bundles its credit card transactions and sends them to its acquirer or acquirers. Each acquirer sends the transaction information to a *merchant accounting system* ("MAS"), which may be part of the acquirer's operations or may be a separate entity. The merchant accounting system forwards that information to the networks of the *card associations*,

¹ In other words, we do not discuss debit card transactions and "card-not-present" sales, such as online purchases, which work somewhat differently.

such as MasterCard, Visa, Discover, American Express and Diners.² If we assume that the day's transactions involve only MasterCard and Visa (the other networks operate somewhat differently), the merchant accounting system next takes out a fee for the merchant acquirer's part in the transactions and authorizes an *automated clearinghouse network* to credit the balance to the merchant's bank account.

The MAS next transmits transaction information concerning these purchases to a part of the Visa or MasterCard network called *Interchange*. Interchange sends the transaction information to the appropriate issuing banks, which bills the cardholder. The bank also must remit certain fees to Interchange.

Transaction Security Issues

Now is a good time to step back and consider the security issues that these processes present. The consumer started the transaction by presenting a card that is a storehouse of valuable information. The cardholder's name and account number appear in plain view on the face of the card. The magnetic stripe, running across the back of the card, includes the account number, the issuing bank, the credit limit and other valuable information.

When the card is swiped, the information on the magnetic stripe starts on a journey that will take it to the merchant's computer, to the acquirer, to the card issuer. If security is weak at any point along the journey, a thief might acquire that information: from the store computer, by acquiring the contents of wireline or wireless transmissions within the store, by intercepting the transmissions from merchant to acquirer or processor, or by intercepting the transmissions from the acquirer or processor to the issuing bank. The thief also might acquire the information from the computers of the acquirers, processors or issuing banks.

Electronically stored data is not the only security concern. Retail payment card transactions also leave a paper trail. Paper receipts contain valuable information, as does the paperwork that is completed when merchandise is returned or exchanged.

Recent Security Incidents

We all have seen how this process can go wrong. For example, in an incident involving CardSystems Solutions Inc., the processor used by a number of acquirers suffered a massive data loss when hackers accessed cardholders' names, account numbers and other data. In cases involving BJ's Wholesale Club, Inc. and TJX, the merchants allegedly kept customer card data longer than necessary and failed to secure that data against unauthorized access, with the result that hackers gained access to those retailers' networks and obtained payment card and other personal consumer information.

Who suffers when these incidents occur? There are at least three scenarios, each one of which leaves its own trail of financial costs.

In one scenario, the loss of data becomes known, but there is no hard evidence that the information was used to make false charges against the card accounts or to open and use other accounts. Nevertheless, cardholders may claim that their cards are no longer secure. In these cases, cards must be cancelled and new cards must be issued. This imposes a cost on the issuing banks, which most likely were not the source of the security breach.

In another scenario, the lost data is used to make fraudulent charges to existing customer accounts. The cardholders then find the items on their bills and complain to their issuing banks. If the issuer receives a complaint, it will investigate and determine whether the merchant followed proper procedures. The investigation and its outcome will be governed by the rules of the card association. Depending upon the results, the merchant might be assessed a charge-back, which is reflected as a debit from the merchant's account with its acquirer. Merchants with excessive charge-backs will lose the ability to accept the cards in

² The card associations do not grant credit or sell products or services to cardholders. They design and operate the systems by which transactions are processed and, most importantly for our purposes, set the rules for those transactions. Those rules include the obligation to comply with the PCI Data Security Standard.

question. The customer may also demand that a new card be issued. Potentially, this second scenario imposes costs on the issuing bank, the acquirer and the merchant.

In still another scenario, the stolen card information is used to create new accounts – the classic case of identity theft. This results in charges being made to cards or other accounts that the original cardholder has not authorized. Again, there may be charge-backs against acquirers and merchants. Cancellations of the fraudulently-opened accounts will result in costs to the card issuers or other creditors with which those accounts were opened. The authorized accounts that were compromised also must be closed and replaced with new accounts, imposing costs on those issuers.

As these examples show, breaches of payment card data security almost always are costly for someone, and the costs are not necessarily borne by those persons and companies that failed to secure the compromised data. Not surprisingly, the card industry decided that the best way to prevent these problems is to secure the data to start with. The PCI Data Security Standard is intended to do just that.

WHAT ACTIONS DOES THE STANDARD REQUIRE?

The PCI Standard applies to all “members, merchants, and service providers who store, process or transmit cardholder data.”³ All such entities must implement the following protections for cardholder data that they process, maintain or transmit:

- Install and maintain a firewall configuration to protect data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored data by keeping cardholder information storage to a minimum, developing a data retention and disposal schedule, and limiting storage amount and retention time to that which is required for business, legal and/or regulatory purposes.
- Encrypt transmission of cardholder and sensitive information across public networks.
- Use and regularly update anti-virus software or programs.
- Develop and maintain secure systems and applications, by implementing vendor-supplied security patches and identifying and correcting system vulnerabilities.
- Restrict access to data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security for employees and contractors.

Each of these 12 requirements is explained in more detail in the Standard. Among the many security obligations that the Standard imposes, two are especially worth noting because they are sometimes overlooked:

1. The importance of proper handling of paper, as well as electronic, records;
2. The importance of having and following a records management program that includes records retention and destruction policies.

³ MasterCard International Payment Card Industry Data Security Standard, p.1 (available online at <https://sdp.mastercardintl.com>).

As to the first point, the Standard requires members, merchants and service providers to “physically secure all paper and electronic media (for example, computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.”⁴ Entities subject to the Standard also must maintain “strict control over the internal or external distribution of any kind of media that contains cardholder information,” including proper labeling of the media as confidential and sending the media “via secured courier or a delivery mechanism that can be accurately tracked.”⁵

The Standard also requires secure storage of media – including paper records – that contain cardholder information, and secure destruction of media containing cardholder information when it is no longer needed for business or legal reasons by shredding, incineration or pulping.⁶

These requirements for secure storage and disposal of paper records are especially important in light of the heightened interest by both regulators and law enforcement agencies in insecure disposal of paper records. Notably, in 2007, the attorneys general of Texas and other states increased their enforcement of state “must-shred” laws, and the Federal Trade Commission brought its first enforcement action under its Disposal Rule, which implements the secure disposal obligations of the Fair and Accurate Transactions Act. This increased scrutiny of records disposal practices makes it increasingly likely that poor disposal practices involving credit card data will be exposed and dealt with, not only under the PCI Standard, but under state and federal law as well.

As to the second point, the Standard’s requirement that media be securely disposed of when no longer needed is underscored by the BJ’s and TJX cases. In both incidents, it was alleged by regulators that the merchants kept cardholder data longer than necessary for any legal or business reason, ensuring that the data would be available when hackers struck. A sound records management policy, including a schedule for disposal of credit card data and other personal records, will go a long way toward avoiding liability under the PCI Standard and otherwise.

HOW IS THE STANDARD ENFORCED?

The card associations are serious about their Standard, which is enforced by a combination of compulsory validation procedures and penalties for noncompliance. The validation procedures vary according to whether an organization is a merchant or a service provider, and according to the volume of card transactions the merchant or service provider handles.

For example, Visa distinguishes four levels of merchants for PCI compliance purposes:

- Level 1 merchants are those that process more than 6,000,000 Visa transactions per year.
- Level 2 merchants process between 1,000,000 and 6,000,000 Visa transactions per year.
- Level 3 merchants process between 20,000 and 1,000,000 Visa e-commerce transactions per year.
- Level 4 merchants include those who process fewer than 20,000 Visa e-commerce transactions per year or up to 1,000,000 Visa transactions, using any acceptance channel, per year.⁷

⁴ See MasterCard International, Payment Card Industry Data Security Standard, sec. 9.6.

⁵ *Id.* sec. 9.7.

⁶ *Id.* secs. 9.9-9.10.

⁷ As these categories suggest, the card associations regard e-commerce sales, in which the cardholder is not present at the point of sale, as riskier than other types of card transactions.

The card associations impose different validation obligations on each merchant level.

Level 1 merchants must complete an annual on-site assessment and a quarterly network scan. The assessment must be performed by a qualified security assessor, or, if signed by an Officer of the company, it may be conducted internally. The annual assessment results in a Report on Compliance, submitted to the merchant's acquirer. The scan must be performed by an approved scanning vendor.

Level 2 and 3 merchants are not required to obtain or conduct an annual on-site assessment, but are required to complete an annual PCI Self-Assessment Questionnaire and obtain a quarterly scan from an approved scanning vendor. Level 4 merchants may also be subject to similar obligations at the discretion of their acquirers. Network security scans are not required of merchants who do not have externally-facing IP addresses.

Service providers, defined by Visa as "organizations that process, store, or transmit Visa cardholder data on behalf of Visa members, merchants, or other service providers," also are subject to PCI Data Security Standard obligations. Level 1 service providers are all VisaNet processors and all payment gateways. Level 2 service providers are not in level 1 and store, process or transmit more than 1,000,000 Visa accounts and/or transactions annually. Level 3 service providers store, process or transmit fewer than 1,000,000 Visa accounts and/or transactions annually.

Validation requirements for service providers are similar to those for merchants. Level 1 and 2 service providers must engage a qualified security assessor to conduct an annual on-site data security assessment and must have a quarterly network scan performed by an approved scanning vendor. Level 3 service providers must complete an annual PCI Self-Assessment Questionnaire and must have a quarterly network scan performed by an approved scanning vendor.

Service Providers and the PCI Standard

The Standard also requires the use of service providers who are compliant with the Standard. For this purpose, the card associations publish lists of compliant providers of various services, including merchant payment services, account billing services, off-site data protection, records management and secure shredding. All listed service providers have completed a PCI Standard assessment, based upon the report of an independent security assessor.

The validation requirements are supported by a substantial system of penalties for noncompliance. Notably, Visa set a compliance deadline of September 30, 2007 for its level 1 merchants. On October 1, 2007, Visa began fining U.S. merchant acquirers \$25,000 per month for each level 1 merchant that had missed the deadline for certification of compliance. Similarly, Visa set a deadline of December 31, 2007, for certification of compliance by level 2 merchants, and acquirers will face penalties for their level 2 merchants who fail to meet the deadline.

Failure to certify compliance in timely fashion is not the only source of PCI Standard penalties. For example, members of the Visa system who fail to give Visa immediate notice of suspected compromise of card transaction information are subject to a penalty of \$100,000 per incident. Also, fines of up to \$500,000 per incident may be imposed on merchants or service providers who suffer a compromise of the security of cardholder or transaction data and are out of compliance with the Standard at the time of the incident.

For a merchant, the monetary penalties under the PCI Standard might be the least of the consequences for failure to protect card data. The loss of the ability to accept credit and debit cards as payment for goods and services can be devastating, especially for online businesses that cannot accept cash and checks. Even where merchants do not lose card privileges altogether, a poor data security record can make them ineligible for card system fee discounts and raise their costs relative to those of competitors.

MORE LIABILITY: LAWSUITS AND LEGISLATION

Major payment card data losses, such as the ongoing TJX incident, have made card issuers and consumers more determined than ever to be compensated for the results of poor data security. Those incidents also have had repercussions in the state legislatures, a number of which are considering laws that would create additional penalties for failure to comply with PCI Standard obligations. One state – Minnesota – now has enacted such a law, and other states are likely to follow.

On the litigation front, the TJX events demonstrate the complex and costly lawsuits that a major loss of credit card data can cause.

Estimates vary, but *The Wall Street Journal* reports that data concerning as many as 40 million payment cards were exposed when outsiders gained access to the TJX computer network through wireless connections at two of the company's local stores.⁸ Investigations discovered a number of practices that arguably violated the PCI Standard. These included the failure to complete the transition of TJX's wireless local area networks to a more advanced encryption standard and storage of individuals' card data longer than needed for business purposes.

Among other consequences, the TJX breach launched a scramble among consumer class action lawyers, the card-issuing banks, TJX and TJX's acquirer, Fifth Third Bancorp, to shift the financial fallout from the loss. Although a precise count is difficult to come by, it is reliably reported that at least 18 separate lawsuits by banks and consumers were brought against TJX, along with investigations by the Federal Trade Commission, state attorneys general, Canadian privacy authorities and others. Also, Visa exercised its rights under the PCI Standard to assess a penalty of at least \$880,000 against Fifth Third Bancorp for failure to ensure TJX's compliance with the Standard.

TJX set aside \$107 million against the cost of pending litigation and has been working diligently to dispose of the various claims.

The consumer class action lawsuits included complaints filed in Alabama, Puerto Rico, California, Massachusetts, Illinois, Michigan, Missouri, Ohio, and Texas. Consumer complaints also were filed in Canada. In September, 2007, TJX announced a tentative settlement of the consumer complaints that will furnish affected customers with up to three years of credit monitoring and identity theft insurance, reimbursement for the cost of obtaining new drivers' licenses, and other relief.

In December of 2007, TJX announced a settlement agreement with most of the banks and banking associations that had sued for reimbursement of their card replacement costs and losses incurred in covering fraudulent transactions. TJX also reached an agreement with Visa, announced on November 29, 2007, under which the retailer would pay \$40.9 million to be allocated by Visa among affected banks. The settlement is said to include an offer by Visa to forego the fine against Fifth Third Bancorp.

The settlements, assuming they become final, will not relieve TJX of all of the pending litigation and investigations. Notably, investigations continue by the Federal Trade Commission, the attorneys general of at least 37 states, the Canadian Privacy Commissioner and the United Kingdom Information Commissioner's Office.

Also, a number of pending complaints allege that TJX violated the Fair and Accurate Credit Transactions Act ("FACTA") by failing to truncate credit card information on its printed receipts for card sales. These class actions demonstrate the continued importance of proper handling of paper records.

⁸ Depositions of Visa and MasterCard executives suggest that the number of exposed accounts may be closer to 90 million.

The Liability of Merchants

The ongoing litigation against TJX also pointed up what the banking industry regards as a gap in the PCI Standard protections. Specifically, the PCI Standards are incorporated in two sets of contracts: the contracts between acquirers and merchants and the contracts between card associations and acquirers. Accordingly, a violation of the Standard by a merchant might support a lawsuit by the merchant's acquirer, and a violation of the Standard by an acquirer might support a lawsuit against it by the card association. However, because the issuing banks are not parties to those contracts, they have had difficulty recovering damages when they are forced to cancel and reissue cards because of merchants' or acquirers' violations of the Standard.

For this reason, as well as a general sense that government should do more to enforce payment card security, state legislators have introduced bills that would make merchants responsible to issuing banks for losses that result from poor card data security practices. Minnesota has enacted such a law, which makes a merchant liable if it, or its service provider, "retains [payment card] data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction."⁹ Merchants or service providers who retain card data longer than permitted must reimburse issuers for "the costs of reasonable actions undertaken by the financial institution as a result of [a] breach [of the retained data] in order to protect the information of its cardholders or to continue to provide services to cardholders..."¹⁰ including cancellation or reissuance of cards, refunds or credits made to cardholders, notification of affected cardholders, and any damages paid to cardholders.¹⁰ The Minnesota law also authorizes private lawsuits by affected cardholders against the merchant or service provider.¹¹

The Minnesota statute, like the PCI Standard itself, underscores the importance of records management and disposal. Under the Minnesota law, liability is based, not on failure to implement any particular security measure, but on a merchant or service provider's failure to dispose of records in a timely fashion. If a merchant or service provider chooses to hold cardholder data beyond the time authorized, it is at risk for the costs of any subsequent breach of that data, regardless of the cause. This is a strict standard that can only be addressed by a well-designed records management and disposal policy, rigorously implemented by merchants, service providers and qualified vendors that are approved for PCI compliance.

* * *

Insecure payment card data is one of the identity thief's most potent weapons. If 2007 is any guide, the New Year will see increasing enforcement of the PCI Standard and new initiatives, in legislatures and courtrooms, to force merchants and service providers who mishandle payment card information to bear the full cost of resulting data breach incidents.

⁹ Minnesota Statutes chapter 325E, sec. 325E.64.

¹⁰ *Id.*

¹¹ *Id.*

©2008 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

 **IRON MOUNTAIN®**
745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout North America, Europe, Latin America, and Asia Pacific.

For more information, visit our Web site at www.ironmountain.com.