

Practitioner's Perspective

by Holly K. Towle, J.D.



Holly K. Towle is a partner with Kirpatrick & Lockhart Preston Gates Ellis LLP (K&L Gates), an international law firm, and chair of the firm's E-merging Commerce group. Holly is located in the firm's Seattle office and is the coauthor of *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons). Holly.Towle@KLgates.com, 206-623-7580.

Practitioner's Perspective appears periodically in the monthly Report Letter of the CCH Guide to Computer Law. Various practitioners provide in-depth analyses of significant issues and trends.

Payment Card Liabilities: There's Trouble Ahead for Merchants That Don't Deal with PCI or a New Minnesota Law

One of my partner's friends called her to ask: "Do any of the lawyers in your firm know "CISP"? If they have to ask what that is, I don't need them." The same thing is true these days for "PCI": if you have to ask, it's time to make room in your brain for more. The exposure of merchants to liability for payment card data is ratcheting upwards, including under an unusual Minnesota law that codifies aspects of PCI.

What is PCI? "PCI" stands for "Payment Industry Card Data Security Standard." Some of the credit/debit card associations or companies have names for their own programs under that standard, hence, "CISP" (Visa's Cardholder Information Security Program).

How did it happen? PCI got started in 2005 when a consortium of major players in the payment card industry settled on it as a common standard. Basically (very), it requires covered merchants (*e.g.*, Internet retailers) to comply with a 12-step standard, including audits. In general, the 12 steps are:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security¹

The initial standard, PCI DSS January 2005, has been replaced with PCI DSS Version 1.1 which became effective December 31, 2006.

To Whom Does PCI Apply? Depending upon the contract, PCI can apply to merchants accepting the major credit cards such as American Express, Discover, MasterCard, Visa, Diner's Club and JCB. There are also significant new fines and penalties (*e.g.*, \$500,000), particularly if there is a data security breach by a noncompliant merchant. How could PCI apply to a retailer with an existing contract not mentioning PCI? Most "merchant contracts" include a clause under which the retailer promises to comply with association rules (or the like) as amended from time to time. In 2005, "sea change" amendments were made. Although there are contract law enforceability issues regarding some merchant agreement amendments and fines, the point here is that PCI exists and any compliance obligations should be examined.

Why Should a Retailer Care? There is plenty of reason to care about PCI on its own: if the standard applies to a merchant, a significant revamp of systems and procedures may be required, fines and penalties can be triggered, and even participation in the credit card system can be imperiled by noncompliance. To the extent PCI becomes an "industry standard," legal concepts applicable to such standards could apply. Also, states are beginning to leap into this arena with legislation.

Minnesota's New Statute. Minnesota's amended "security breach notice" statute is an example of such a leap. For the most part, security breach notification statutes are just that, *i.e.*, they force notice upon breach of the security of a system containing certain "personally identifying" information;² the notice alerts data subjects to watch for possible misuse of data. Minnesota amended its statute to include some PCI concepts and also to impose liability for security breaches that typically would not exist at all, or would not automatically be allocated to merchants.

a. Details. The amendment prohibits retention of certain data on a credit, debit, or stored value card, and then provides a long list of damages merchants must pay to

card-issuing financial institutions if there is a security breach regarding that data.³ The statute prohibits the following effective August 1, 2007:

Security or identification information; retention prohibited. No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the *card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe 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. A person or entity is in violation of this section if its service provider retains such 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.⁴

An "access device" is a card issued by a financial institution containing a magnetic stripe, microprocessor chip, or other means for storage of information, including a credit card, debit card, or stored value card;⁵ a "financial institution" is defined as "any office of a bank, bank and trust, trust company with banking powers, savings bank, industrial loan company, savings association, credit union, or regulated lender."⁶ This definition of financial institution is much narrower than the broad definitions in the federal Gramm Leach Bliley Act,⁷ the federal Bank Secrecy Act, and federal Regulation E (as applied),⁸ so merchants need to take note (*i.e.*, they can be liable under the MN statute because it will not treat them as a financial institution, even if they might be treated as a financial institution under those other statutes).

Data that may not be retained is the "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data." "Card security code" means the three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device that is used to validate access device information during the authorization process;⁹ "PIN verification code number" means the data used to verify cardholder identity when a PIN is used in a transaction¹⁰ ("PIN" means a personal identification code that identifies the cardholder¹¹); and "Magnetic stripe data" means the data contained in the magnetic stripe of an access device.¹²

b. Illustrative Ambiguities. A fundamental question for this kind of statute is whether it is unconstitutionally void for vagueness. For example, there is data in the

magnetic tracks on the back of the card and the “full contents” of that data is covered by the statute but not identified in it. This raises these kinds of questions: is a physical swipe of the card a condition to statutory coverage, *i.e.*, does the statute cover the “full” data *resulting from* the swipe (whatever it may be), or does the statute cover the data elements that would be in a swipe if a swipe were made (in which case, what are those data elements as a matter of law)? Answers are not apparent from the statute but are nevertheless important (*e.g.*, if a swipe is a condition precedent, there is no swipe in Internet and telephone transactions).

Another ambiguity concerns the phrase “full contents of any track of magnetic stripe data.” Assume there are 8 data elements in a magnetic track of a covered card. It is clear that the merchant may not retain *all* of 1 through 8 (“full contents”), but may it retain less than all (less than full)? Further, may it retain an element that is the same as an element on the track, but which element is obtained from a separate source instead of from the track? An example would be the name of the cardholder: many merchants will have that name on a customer list, for example. Does this statute prohibit the merchant from (a) having the name at all even if not obtained from the track, (b) obtaining the name from the track, and/or (c) obtaining the name from the track only if all of the other “track” data is also obtained (the full contents)? These issues are important because business realities or obligations will require the merchant to keep at least some of the magnetic track data, as both the PCI standard and the FTC acknowledge. For example, the PCI standard¹³ summarizes what may be stored as follows:

The Minnesota statute seems aimed at the “Sensitive Authentication Data,” which may not be stored. However, the PCI standard goes on to say that even though the “full contents” of any stripe may not be stored, “in the normal course of business” data elements such as the accountholder’s name, primary account number, expiration date, and service code from those stripes may need to be retained, *i.e.*, less than the full data may be needed. An example of this need would be evidentiary rules or proof of compliance with applicable laws or contracts and PCI allows that.

In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder’s name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements. Note: See “Glossary” for additional information.¹⁴

The PCI standard also refers to a glossary with more information which impacts the standard, yet is not referenced in the Minnesota statute.

c. **Confusion re PCI?** The point of this discussion is not to answer the above questions, but to note some of the problems created by the Minnesota statute, *e.g.*, it likely does not contain sufficient information for merchants to comply and may also create confusion or conflict with the PCI standard. If so, did the Minnesota legislature intend to supplant or supplement that standard or to force merchants to deviate from it even though their contracts may require them to comply with it? How will merchants doing business in Minnesota comply both with the statute and the standard, and meet other legal or business obligations requiring or making advisable retention of some of the prohibited information? The FTC, for example, encourages businesses not to store card information but acknowledges that they may have to do so.¹⁵

d. **Retailer Liability.** The liability provisions of the statute far exceed liabilities and awardable damage under existing law.¹⁶ Here is the liability provision; it applies as of August 1, 2008:

Liability. Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person’s or entity’s service provider, that person or entity shall reimburse

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company’s practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:

- (1) the cancellation or reissuance of any access device affected by the breach;
- (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;
- (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;
- (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and
- (5) the notification of cardholders affected by the breach.

The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.¹⁷

e. Policy Issues. The Minnesota legislature can fairly be accused of over-simplifying risks in an arena where multiple persons can all be wrongdoers and well as victims. The only certain wrongdoer is the thief who obtains data without authorization. To be sure, merchants are part of the security puzzle presented by the modern age, but so are financial institutions,¹⁸ payment card associations and networks, financial institution affiliated and nonaffiliated processors¹⁹ and other service providers, careless consumers,²⁰ and employees.²¹ Careful consumers are also part of the puzzle: if statutes allocate all liability to merchants for what is a much larger and complex problem, merchants will increase prices or go under and consumer choice will be decreased as prices rise. Further, this statute disturbs balances contemplated by association rules leaving risk with financial institutions or not allocating the risk only

to the merchant,²² including rules regarding storage of magnetic stripe information.²³

What's a retailer to do?

First, retailers may wish to review their "merchant contracts," *i.e.*, the contracts allowing them to submit credit and debit card charges for processing. Looking only at the original contract may not be helpful: consider all amendments since at least 2005. Complying with the contract is the next step, including with PCI. Some retailers are allowed to "self-certify" compliance—that is deceptively easy and can come back to "bite" the retailer hard (*i.e.*, read the certification carefully).

Second, retailers should watch for more laws like the Minnesota statute and either get into compliance (to the extent possible) and/or seek appropriate amendments.

Third, retailers may wish to review other aspects of the sea change that has occurred in payment system law. For example:

- ACH (Automated Clearing House) transactions have new and developing data security rules that started to appear about the same time as the PCI standard, but which are not the same;
- Class actions are becoming abundant regarding the now fully effective federal law requiring credit and debit card receipts to truncate the card number and omit the expiration date and state variations exist;²⁴ and
- Other surprises lurk. For example, merchants converting paper checks to ACH transactions are deemed to be "financial institutions" under federal Regulation E and must provide new disclosures to customers before taking the check.

Last, retailers should cross their fingers, hard: data security is not an area where perfection is possible no matter what precautions are taken.

Endnotes

- 1 PCI Standards "Payment Card Industry (PCI) Data Security Standard Version 1.1 Release: September, 2006.
- 2 For a list of these state statutes and a discussion of them, see Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* (2003-07, A.S. Pratt & Sons) at Chapter 16.08[3].
- 3 2007 Minn. Sess. Law Serv. Ch. 108 (H.F. 1758), creating MN ST § 325E.64.
- 4 MN ST § 325E.64, subdivision 2 (emphasis added).
- 5 *Id.* at § 1(b).
- 6 *Id.* at § 1(e).
- 7 See discussion in Chapter 12.10[2] of the *The Law of Electronic Commercial Transactions*.
- 8 See *e.g.*, discussion in Chapter 4.19[2] and [3] of the *The Law of Electronic Commercial Transactions*.

- 9 MN ST § 325E.64, subdivision 2 at § 1(d).
- 10 Id. at (i).
- 11 Id. at (h).
- 12 Id. at (g).
- 13 Payment Card Industry (PCI) Data Security Standard Version 1.1 (9/06) https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm.
- 14 Id. at § 3.2.1 (bolding added).
- 15 See *Protecting Personal Information: A Guide For Business* (3/9/07) at 7 <http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf> (“Don’t keep customer credit card information unless you have a business need for it. For example, don’t retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft”).
- 16 See e.g., the series of cases spawned by the FTC’s settlement with BJ’s Wholesale Club, Inc. regarding an FTC allegation that BJ’s failed to employ reasonable and appropriate security measures to protect personal information of consumers, in *In the Matter of BJ’s Wholesale Club*, FTC File No. 0423160 (copy available at www.ftc.gov/opa/2005/06/bjswholesale.htm). See also discussion of traditional damage approaches in *The Law of Electronic Commercial Transactions* at Chapters 16.06[2], 12.02[5], and 15.06[5].
- 17 MN ST § 325E.64 (3).
- 18 See e.g., claim made in *Huggins v. Citibank, N.A.*, 355 SC 329, 585 SE2d 275 (2003) and *The Law of Electronic Commercial Transactions* at Chapter 15.06[5][a].
- 19 According to Richard J. Sullivan, *Risk Management and Nonbank Participation in the U.S. Retail Payments System*, Economic Review, Second Quarter, 5 at 19 (2007), “Some of the largest payment-processing organizations in the U.S. are affiliated with banking organizations such as Fifth Third Bancorp, U.S. Bancorp and JPMorgan Chase. Many organizations that provide or process payments in the United States have no affiliation with a banking company. Among the larger organizations without affiliation are First Data Corporation, MasterCard and Paypal.”
- 20 Id. at 24 (2007) (“Payment card holders, for example, may not be sufficiently careful, because they often do not face any cost if they lose their card and it is used fraudulently.” These difficulties have lead the payments industry to embrace containment as an approach to risk management”).
- 21 For example, a 2005 study concluded that most computer sabotage is carried out by current or former employees or contractors intent on revenge. See *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, US Secret Service National Threat Assessment Center and CERT Coordination Center of Carnegie Mellon University (2005). See also *United States v. Willis*, 476 F.3d 1121(10th Cir, 2/16/2007) (collection agency employee in charge of controlling passwords to secure, third party financial information database “admitted that he had given a username and password to his drug dealer in exchange for methamphetamine;” drug dealer used the database for identity theft ring); *U.S. v. Millott*, 433 F3d 1057 (8th Cir. 2006) (employee with lead responsibility for disabling remote access accounts disabled manager’s account after not being offered a job with outsourcer for his department).
- 22 See e.g., *Pennsylvania State Employees Credit Union v. Fifth Third Bank*, Slip Copy, 2006 WL 1724574 (MD PA) (stating that Visa System does not provide mechanism for issuers to recover costs associated with card replacement but may recover compensation for fraudulent use of a compromised card; and that “Visa’s representative testified that he had a ‘general understanding’ that the omission of operational costs from recovery in the compliance process was a business decision made as part of its analysis of the proper allocation of responsibility, costs, and risks for participants in the Visa system”).
- 23 Id. at p.9 (court refused to find that credit union card issuers were third party beneficiaries of Visa prohibition on retention of full magnetic stripe data, finding instead that Visa intended that rule to benefit the system generally, including merchants).
- 24 See the Fair and Accurate Credit Transactions Act of 2003. Pub. L. No. 108-159, § 113 (2003) (amending 15 USC § 1681(c) (FCRA § 605) adding new subsection (g)). States may not impose requirements or prohibitions with respect to the conduct required by the specific provisions of FACT, but states are passing nonuniform legislation.