Pillsbury Winthrop Shaw Pittman LLP

Global Sourcing
Consumer & Retail
July 30, 2007

Client Alert

New Minnesota Data Retention Law Creates Potential Liability for Merchants

by John L. Nicholson and Meighan E. O'Reardon

Beginning August 1, 2007, merchants with customers in Minnesota may not retain credit or debit card security data after a transaction is completed. Merchants violating the law face strict liability to financial institutions for the costs associated with a card security breach.

The new law also imposes liability on merchants for the data retention practices of their service providers. Any merchant that accepts credit or debit card payments from Minnesota residents may be exposed to liability under this first-of-a-kind law, which codifies into law one of the Payment Card Industry Data Security Standard (PCI DSS) requirements.[1]

Minnesota is not alone in its efforts; a number of other states have similar legislation pending. Merchants should consider taking proactive steps to avoid future liability. In particular, merchants with customers in Minnesota should audit and bolster their security plans and procedures related to credit and debit card security data, as well as review their existing contracts with service providers to update data retention practices.

Background: Minnesota Data Retention Law (H.F. No. 1758)

In response to the recent TJX Companies, Inc., credit card data breach, which compromised over 45 million cardholders' information, the Minnesota Legislature has enacted the Plastic Card Security Act.[2] This new law imposes strict liability on merchants that retain credit or debit card security data. Any merchant conducting business in Minnesota after August 1, 2007, may not keep "card security code data,[3] the PIN verification code number, or the full contents of any track of magnetic stripe data" after a transaction is authorized.[4] Security data may, however, be maintained for PIN debit transactions for up to 48 hours after a transaction but not longer.[5]

In the event of a security breach, the Plastic Card Security Act imposes significant liability on merchants that have violated the law's data retention provisions. Specifically, Minnesota imposes strict liability, meaning merchants will be liable regardless of whether the security breach was the result of negligence or some other factor such as poor security. The law also holds merchants responsible for violation of the data retention requirements by their service providers.

Where security data has been retained in violation of the law and a data breach occurs, merchants will be liable to any financial institution for the costs incurred to remediate and recover from the breach. The Act specifically lists the following costs for which merchants will be responsible following a breach: (1) the cancellation or reissuance of any access device affected by the breach;[6] (2) the closure of 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 accounts affected by the breach; (4) any refund or credit that must be made to a cardholder to cover the cost of unauthorized transactions related to the breach; and (5) notification to the cardholders affected by the breach.[7] Merchants will also be liable for damages that financial institutions pay to injured cardholders as a result of the security breach. The costs imposed by this new Minnesota law are in addition to any other remedies that are already available to financial institutions. Security analysts hired by financial institutions and industry reporters estimate that the cost of the TJX breach may exceed one billion dollars.[8]

The Minnesota law is scheduled to be phased in over a one-year period. The provisions forbidding retention of credit or debit card security data take effect August 1, 2007, while the provisions imposing liability will take effect August 1, 2008.

Implications for Businesses Located Outside of Minnesota

Even merchants not physically located in Minnesota potentially face liability under this law. Notably, the statute applies to any merchant conducting business in Minnesota. Determining whether a particular merchant is **conducting** business in Minnesota for purposes of this statute is a fact-specific inquiry. Rather than list activities that **are** considered conducting business in Minnesota, the Minnesota Foreign Corporation Act identifies a number of activities that are **not** considered to be conducting business in the state.[9] In particular, the statute notes that a foreign corporation will not be transacting business in the state if it is "conducting an isolated transaction completed within a period of 30 days and not in the course of a number of repeated transactions of like nature."[10] Although the Minnesota "long arm" statute for jurisdiction holds that the state cannot exert jurisdiction over a foreign corporation for privacy causes of action when all the foreign corporation has done is commit an act outside Minnesota that causes injury or property damage in Minnesota,[11] the "long arm" statute does provide jurisdiction when the foreign corporation or nonresident is transacting any business within the state.[12] Ultimately, any merchant that conducts business with Minnesota residents using credit or debit cards will need to assess whether their specific contacts with those residents constitute conducting business in Minnesota. Given the current public sensitivity to the consequences of data breaches and the potential cost of violations of the Plastic Card Security Act, merchants may wish to err on the side of caution and assume that multiple transactions with Minnesota residents will constitute conducting business in Minnesota.

Codifying PCI Data Security Standards

The Minnesota law is one of the first of its kind to codify elements of the PCI DSS. Version 1.1 of the PCI DSS outlines twelve security requirements that have been developed by the major payment card networks to regulate the storage, processing, and transmission of credit and debit card numbers. Requirement 3 of the

PCI DSS prohibits storage of "sensitive authentication data," which includes magnetic stripe data, card validation codes, PINs, and encrypted PIN blocks.[13] By requiring the destruction of all such data immediately following a transaction, the Minnesota law has given this requirement legal effect.

Relationship to Minnesota's Data Breach Notification Law

Minnesota also has a data breach notification law.[14] This law requires any person or entity conducting business in the state to notify residents when there has been a breach of the residents' unencrypted personal data. Such notification must be made in a timely manner. As a result of Minnesota's notification laws, any merchant informing a Minnesota resident of a breach that involves card security data will now also be acknowledging possible liability for the costs of the incident. While financial institutions are not directly contacted under the Minnesota notification law, these organizations will presumably become aware of such unauthorized access through customers and the media. As a result, financial institutions may be able to rely on the merchant's acknowledgement that data was compromised to recoup costs under the Plastic Card Security Act.

Momentum for Similar Legislation

Minnesota is not alone in its efforts to bolster protection of card security data; a number of other states are also actively pursing similar legislation. In particular, California is currently considering a measure that would make responsible entities liable for the costs of credit and debit card replacement as well as consumer notification. The pending California legislation is more stringent than the Minnesota statute and would require merchants to comply with seven of the PCI standards related to protecting cardholder data.[15] Connecticut, Illinois, Massachusetts, and Texas are also each working to adopt comparable statutes. In addition to individual state efforts, there is also support at the federal level for similar legislation.

Compliance with Minnesota's New Law

Merchants doing business in Minnesota should take action to limit their exposure by taking the following steps:

- Merchants that do regular business with residents of Minnesota should confirm that they are not storing card security data in violation of the Minnesota law, including auditing their existing data retention policies and practices and updating them where appropriate.

- Existing contracts with service providers should be reviewed and updated to reflect the new data retention provisions. As appropriate, merchants should work with their third party providers to ensure compliance with the Minnesota law. Additionally, contracts should include provisions to indemnify the merchant in cases where the service provider has breached the Plastic Security Card Act.

- Finally, any entity handling credit card data should regularly monitor PCI DSS updates and modify its security practices accordingly. For the latest PCI DSS requirements, see https://www.pcisecuritystandards.org/tech/pci_dss.htm.

Live Link

Payment Card Industry Data Security Standard, Version 1.1; PCI Security Standards Council; September 2006 (Note: Select a language to view the PDF document.)

For assistance in reviewing or developing data retention policies and procedures, assistance with contracts with third party service providers, or for further information, please contact:

John L. Nicholson (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

Catherine D. Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Deborah S. Thoren-Peden (bio)
Los Angeles
+1.213.488.7320
deborah.thorenpeden@pillsburylaw.com

[1] *See* Payment Card Industry Data Security Standard, Version 1.1 (September 2006) available at https://www.pcisecuritystandards.org/tech/pci_dss.htm.

[2] *See* H.F. No. 1758 - 85th Legislative Session (2007-2008); *See also* Joseph Pereira, "Breaking The Code: How Credit-Card Data Went Out Wireless Door - In Biggest Known Theft, Retailer's Weak Security Lost Millions of Numbers," WALL ST. J. (May 4, 2007).

[3] According to the Plastic Security Card Act, card security code data means "the three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic strip of an access device which is used to validate access device information during the authorization process."

[4] MINN. STAT. § 325E.64(2) (2007).

[5] A PIN debit transaction immediately removes funds from a cardholder's account since authorization and settlement of the transaction is accomplished in one step. PIN debit transactions are processed over Electronic Funds Transfer (EFT) networks similar to Automated Teller Machine (ATM) transactions.

[6] According to the Minnesota Statute, an access device means "a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card."

[7] MINN. STAT. § 325E.64(3) (2007).

[8] *See* Ross Kerber, "Analysts: TJX Case May Cost over $1B," BOSTON GLOBE (April 12, 2007); *See also* Sharon Gaudin, "Estimates Put T.J. Maxx Security Fiasco at $4.5 Billion," InformationWeek (May 2, 2007).

[9] MINN. STAT. § 301.03 (2006).

[10] MINN. STAT. § 301.03(h) (2006).

[11] MINN. STAT. § 543.19(1)(d)(3) (2006).

[12] MINN. STAT. § 543.19 (2006).

[13] *See* Payment Card Industry Data Security Standard, Version 1.1, Requirement 3 (September 2006) available at https://www.pcisecuritystandards.org/tech/pci_dss.htm.

[14] MINN. STAT. § 325E.61 (2006).

[15] Bill Analysis, A.B. 779, "Security of Personal Information: State Agencies and Businesses," California Senate Judiciary Committee, Senator Ellen M. Corbett.