A Publication of Law Bulletin Publishing Company
Chicago Lawyer®

Is your business really PCI compliant?

December 2010

BY ALAN S. WERNICK, ESQ., FSB FISHERBROYLES, LLP T: 847.786.1005 – E: WERNICK@FSBLEGAL.COM

If your business accepts credit cards, then you are at risk for potential liability in the event of a data breach. You need to be aware of the importance of keeping your customers' personal information secure.

There are state and federal statutes, as well as a series of financial industry standards, that form a data security compliance bar surrounding Personally Identifiable Information (PII) - those pieces of information that can be used to uniquely identify a person.

While there is a cost to compliance, there is an even greater cost to noncompliance, particularly if a data breach occurs. Heartland Payment Systems Inc., a New Jersey based payment processor, experienced a tremendous data breach that cost the company $140 million, including legal fees, defending various claims and other investigation expenses.

PII comes in many different types. Depending on the state's law, PII can include a person's first name or first initial and last name in combination with any one or more of several data elements. These elements include:

- Social Security number
- Account number or credit or debit card number
- Financial information
- Medical information
- Passport number
- Employer identification number
- Taxpayer identification number
- Medicaid account number
- Insurance policy numbers
- Utility account number
- Employment history
- Biometric data such as fingerprints, facial scan identifiers, voiceprint
- Digitized or other electronic signature
- Any professional license, certificate, permit or membership number.

There are a number of federal and state laws that speak to the need for protection of PII, and the potential remedies and penalties in the event of noncompliance.

In addition, several companies in the financial services industry promulgated certain standards known as the payment card industry (PCI) standards for businesses that use credit cards as a form of payment for their goods and services.

The founding members of the financial services self-regulatory Payment Card Industry Security Standards Council are global payment brands, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The council does not validate or enforce the PCI security standards.

Enforcement is typically implemented through merchant services contracts with payment processors and financial institutions. However, the council does certify qualified security assessors and approved scanning vendors as those individuals and companies qualified to validate compliance to the PCI standards.

These standards include the Data Security Standard (DSS), Payment Application Data Security Standard (PADSS) and PIN Transaction Security (PTS) Requirements.

Depending on the agreement, a failure to comply with the PCI Data Security Standards may result in several remedies available to the merchant's credit card payment processor, including a requirement for the merchant to have a forensic audit of data security processes and procedures (which may cost the merchant thousands of dollars), or a holdback by the processor of credit card funds received and processed for the merchant.

A credit card data breach can have a devastating effect on a business - fines, forensic audit costs, investigation fees and legal fees, lost management time and a potential loss of trust by those customers who entrusted the business with their credit card information.

PCI-DSS essentially posits best practices in the handling of credit card information. Ongoing diligent attention to the PCI-DSS may, in addition to mitigating the risk of a credit card data breach, provide a business with a competitive advantage by protecting the trust of its customers when protecting their valuable credit card information.

There are 12 requirements in the PCI Data Security Standard that, according to the council, fall into six general categories:

1. Build and maintain a secure network;
2. Protect cardholder data;
3. Maintain a vulnerability management program;
4. Implement strong access control measures;
5. Regularly monitor and test networks;
6. Maintain an information security policy.

As a credit card holder, you might review the PCI-DSS and think that these are common-sense steps that you would expect any merchant to whom you trust your credit card information would follow.

However, common sense isn't always that common.

Many businesses accepting credit cards are unaware of the PCI standards and may only learn about them when a data breach occurs. While there may be many causes for a data breach beyond the control of the merchant, being aware of the PCI standards and appropriately implementing them in your business is part of the cost of doing business today.

