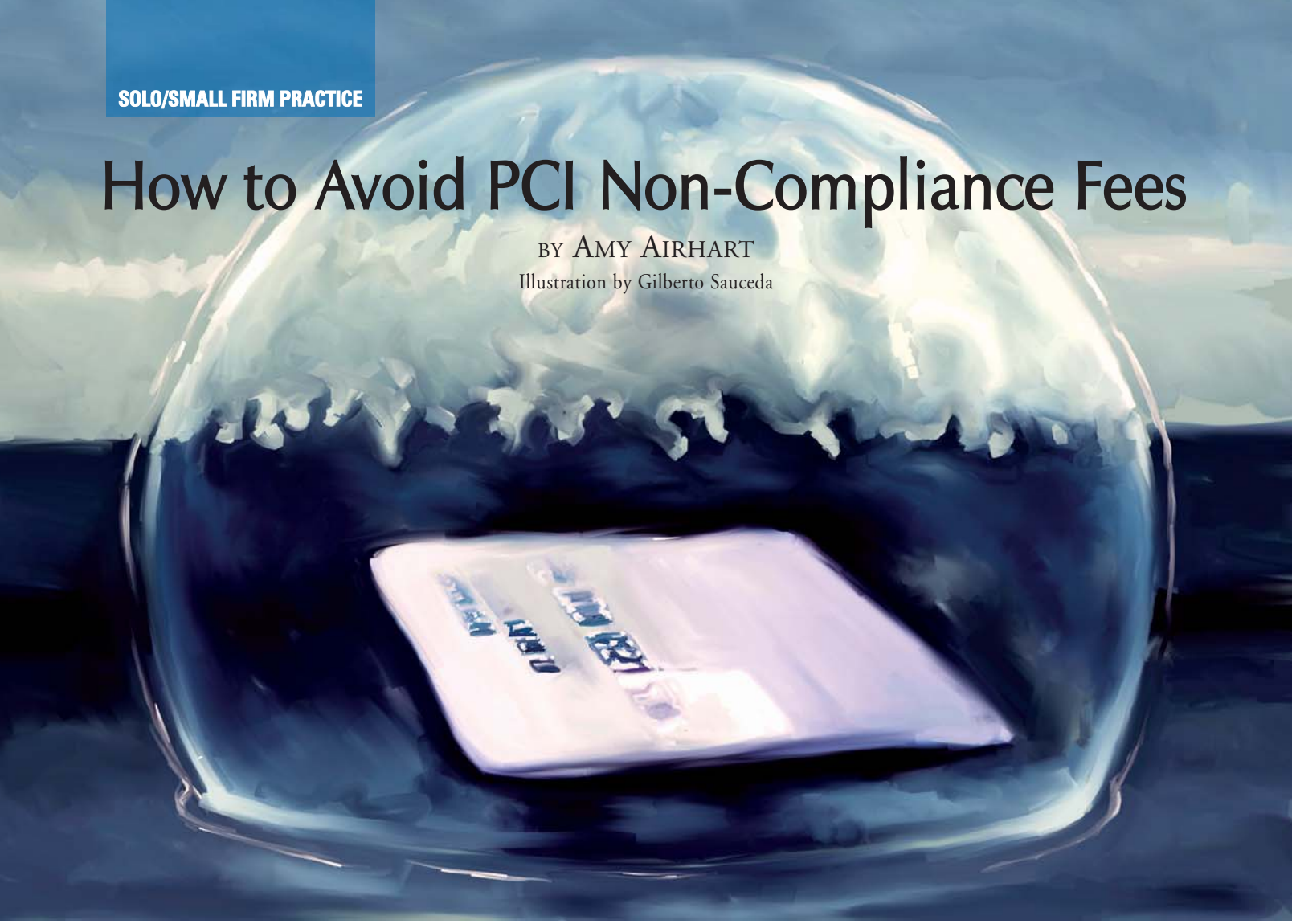
How to Avoid PCI Non-Compliance Fees

BY AMY AIRHART

Illustration by Gilberto Sauceda



If your law firm accepts credit card payments, you should have received information from your merchant provider regarding the recent updates to Payment Card Industry Data Security Standard (PCI-DSS) compliance requirements. When you accept credit card payments, you also accept the responsibility of protecting cardholder information. As of July 1, any firm accepting credit cards is required to comply with the PCI security standards. (Check with your merchant bank for deadlines and fees.)

In addition to the new requirements, most major processors have started implementing non-compliance fees. It may be helpful to review a recent merchant statement for those charges, which typically range from $15 to $25 per month. To avoid non-compliance fees, you will need to take steps to become PCI compliant. You may have received calls regarding non-compliance fees or enticements to switch to other processors; however, use caution as these calls may just be ambush marketing techniques. Please check with your acquiring bank for specific deadlines and fees.

What Is PCI?

In 2006, the major credit card brands (Visa, Mastercard, Discover, American Express, and JCB) formed a security council. The council's goal was to ensure the safe handling of cardholder data at all times and to reduce credit card fraud by developing a standardized set of regulations for the entire credit card processing industry. The resulting Payment Card Industry Data Security Standard, Payment Application Data Security Standard, and the PIN Transaction Security Standard work together to achieve that goal.

Payment Card Industry Data Security Standards are focused on protecting credit card information at the merchant level by implementing basic procedures to protect cardholder data. The new regulations will make protecting sensitive card information a priority, thus reducing identity theft and credit card fraud.

Regardless of how many transactions you accept or process, PCI is an important step in protecting the security of merchant account. To ensure credit card transactions are secure through every step of the payment process, all parties in the payment industry are now required to be PCI compliant.

Doing Your Part

PCI compliance is composed of two areas: How credit cards are processed through our systems and how you handle credit card information within the walls of your office. The security of your office is paramount for compliance. For example, do you store paper copies of credit card data in a secure way? Do you use a payment gateway or a terminal to process credit cards? These are practical security points addressed by the PCI-DSS and apply to any business that processes, stores, or transmits credit card data (**www.pcisecuritystandards.org**).

Until recently, most of the focus has been on major retailers that process in excess of 6 million Visa transactions per year. All merchants — regardless of credit card processing volume — must now comply with the regulations. Failure to meet requirements can result in security breaches, costly fines, and forensic audits.

Twelve Requirements Of PCI-DSS

Depending on how you process credit cards, some of these requirements may not apply to your business. Most small businesses that use a swipe machine (terminal) or payment gateway focus on Requirements 3, 9, and 12. These requirements will also be the basis for developing strong security policies and procedures for how your business handles credit card data.

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 security.

Becoming PCI Compliant

There are several steps every merchant must complete to become PCI compliant:

- **Complete a Self-Assessment Questionnaire (SAQ)** — The SAQ is a set of questions you need to answer about how your business processes credit cards;
- **Implement Changes** — Make the necessary changes to your standard operating procedures;
- **Develop Security Policies** — Update or create security policies and procedures for how your office handles credit card data;
- **Conduct Vulnerability Scan** (when applicable) — This step applies to all merchants transmitting credit card data over the Internet; and
- **Get Certified** — Complete "Attestation of Compliance" to confirm your business meets all PCI regulations.

Credit Card Compliance For Attorneys

Even though the PCI-DSS is not a federal law, several states have started mandating compliance to many provisions of the PCI standards. In 2007, Minnesota became one of the first states to adopt a set of enforceable standards that protect credit card data. Since then, Nevada, Washington, and Massachusetts have adopted similar laws.

Implementing small changes can have a big impact on your security. There are guidelines in the PCI-DSS that address Internet security and payment applications and also guidelines that address how businesses handle credit card data on a physical level. Assessing your vulnerabilities is a great way to fix potential issues and educate your staff. According to some reports, the majority of credit card fraud is caused by simple carelessness and theft (**www.datalossdb.org/statistics**). Office security policies that define procedures for changing passwords, storing information, and disposing of credit card data can make the difference between compliance and non-compliance.

AMY AIRHART
is PCI manager for Affiniscape Merchant Solutions and PCI Central (**http://www.pcicentral.com**).

SOLO/SMALL FIRM PRACTICE

To address the unique practice issues of solo and small firm lawyers, the *Texas Bar Journal* has developed this special series of articles that will appear regularly in the magazine. If you would like to see a particular topic covered, please send your story ideas to Associate Editor **Patricia L. Garcia** at **pgarcia@texasbar.com**.

TRADEMARK
Copyright & Patent Searches

"Experienced Washington office for attorneys worldwide"

FEDERAL SERVICES & RESEARCH:

Attorney directed projects at all Federal agencies in Washington, DC, including: USDA, TTB, EPA, Customs, FDA, INS, FCC, ICC, SEC, USPTO, and many others. Face-to-face meetings with Gov't officials, Freedom of Information Act requests, copyright deposits, document legalization @ State Dept. & Embassies, complete trademark, copyright, patent and TTAB files.

COMPREHENSIVE: U.S. Federal, State, Common Law and Design searches,
INTERNATIONAL SEARCHING EXPERTS: Our professionals average over 25 years experience each
FAST: Normal 2-day turnaround with 24-hour and 4-hour service available

GOVERNMENT LIAISON SERVICES, INC.
200 N. Glebe Rd., Suite 321
Arlington, VA 22203
Ph: 703-524-8200, Fax: 703-525-8451
Minutes from USPTO & Washington, DC
TOLL FREE:1-800-642-6564
www.GovernmentLiaison.com
info@GovernmentLiaison.com