

Community Banks Benefit from Awareness of Payment Card Security

By Mike Petitti

Community Banks know the acronyms SOX, SAS-70 and GLBA. However, despite its regular appearance in trade periodicals and daily newspapers, PCI DSS—for Payment Card Industry Data Security Standard—may still elude some. Now is the time for community banks to understand their PCI DSS-related obligations and also promote awareness among their merchant accounts to protect themselves and their customers.

Consumers demand payment card security: PCI DSS compliance paves the way.

More than 30 states have enacted legislation requiring consumer notification when sensitive, personal information is exposed. As a result, news of credit and debit card information exposure (a payment card compromise or breach) at various merchant locations has become commonplace. This increased awareness of card fraud pushes concerns about the security of credit and debit cards to the forefront of consumers' and bankers' minds.

In a typical payment card compromise or breach, an unauthorized individual takes advantage of a flaw in a system that processes, transmits, or stores credit or debit card data. This individual will use free tools available online to scan the Internet for vulnerable systems and then penetrate the system to look for debit or credit card numbers, expiration dates, and other associated information. If they find cardholder information, they copy the information and then use it to create



fraudulent, embossed payment cards for sale on the black market.

With the advent of e-commerce, the major payment card brands (American Express, Discover, MasterCard and Visa) needed to address associated concerns regarding information security and credit and debit card fraud. Prior to 2004, each major payment card brand created and oversaw their own, separate data security standards for merchants and payment processors that accepted and processed their proprietary card brands. In 2004, the card brands came together to recognize the PCI DSS as the industry-wide, global standard for data security with which all entities that store, process, and transmit credit and debit card information must comply.

The PCI DSS lays out fundamental data security practices that protect the card associations, banks, merchants, service providers, and consumers from credit or

debit card fraud and the losses incurred in the aftermath of compromise. The standard includes 12 requirements and associated sub-requirements (clarifying specifically how to meet each requirement) in pursuit of six “control objectives”:

1. Building and maintaining a secure network
2. Protecting cardholder data
3. Maintaining a vulnerability management program
4. Implementing strong access control measures
5. Regularly monitoring and testing networks
6. Maintaining an information security policy

Each card brand enforces separate compliance validation requirements and deadlines depending on an organization's transaction volume. The card associations hold acquiring banks responsible for their merchants' PCI DSS compliance. An acquiring bank is the bank that contracts with merchants to allow them to accept credit or debit cards. Therefore, in the event of a credit or debit card compromise, the card associations levy various fines and fees against a compromised merchant's acquiring bank. The majority of acquiring banks then pass that fine along to the compromised merchant; however, it remains the acquiring bank's responsibility to collect and deliver payment on those fines to the card associations. Some card brands have levied fines against acquirers whose merchants did not validate compliance by their given due date. These fines for non-compliance may also recur periodically as long as the non-



compliant organization fails to validate. However, even more troubling are fines and fees levied should a non-compliant entity suffer a credit or debit card compromise.

If cardholder data in an entity's care is exposed and a forensic investigation shows that the entity was not PCI DSS-compliant at the time of the breach, the victim is liable for a number of charges and could be expelled from the card payment networks altogether. A non-compliant, compromised organization can expect association-issued fines (separate fines from each affected card brand) passed on from their acquiring bank in addition to costs related to the investigation of the incident and technology and services required to secure the compromised network environment.

Because of their regional focus, community banks experience the full repercussions of a payment card compromise. Payment card breaches can affect a community bank in a number of ways, aside from the repercussions should the bank itself fall victim. Because a community bank's customers (merchant and consumer) tend to be concentrated in one region, if a merchant customer of the bank is compromised, it's probable that some of the bank's consumer customers shopped at that merchant, thereby putting consumer accounts at risk.

If a community bank's merchant customer is compromised, and the bank facilitates that merchant's credit card acceptance, the bank will be held accountable by the card associations through fines and fees. In addition, if that bank's customer is also a regional merchant, in all likelihood, the card numbers exposed are those of at least some of the bank's consumer customer accounts. Since debit cards are now issued with new checking accounts and the majority of those cards are issued with the Visa or MasterCard logo, the community bank is also the issuing bank for those cards. The community bank will not only be responsible for resolving the card compromise, they also

must monitor at-risk consumer accounts on the issuing bank side.

Re-issuing a consumer card involves more than printing and mailing new plastic cards. If a data breach story breaks, phone lines jam with concerned consumers asking for the cancellation of an account they're worried may have been compromised and the issuance of new cards. From the consumer's viewpoint, the cost of this process is little more than minutes on the phone and days waiting for a new card to arrive by mail; the issuing bank knows otherwise.

That bank must

- Handle a deluge of calls from concerned customers;
- Evaluate suspect charges on at-risk cards;
- Wait for suspect charges to post;
- Reconcile fraudulent charges with monthly statements;
- Report any suspicious activity to the card associations;
- Close or block other potentially compromised accounts;
- Process the re-issuance of any new cards;
- Transfer customers' account information to reissued cards;
- Mail the new cards; and
- Attempt to recover losses

The card associations do offer tools to aid in the recovery of losses (see below for more information); however, complete recovery is impossible. Ultimately, preventing fraud in the first place is the only way to avoid its costs and give your customers peace of mind that their sensitive information is protected. Complying with the PCI DSS prevents fraud through sound information security policy, and community banks and their merchant and consumer customers all benefit from increased PCI DSS awareness. Merchants will appreciate a resource to turn to for PCI DSS guidance. Just as their bank wants to protect them, merchants want to protect their customers and benefit from a reputation as a data-secure business and partner. Consumers will appreciate their bank's commitment to information

security awareness and looking after their customers by putting pressure on merchants to comply.

Complying with the PCI DSS is a complex process, especially for acquiring or issuing banks. Below are a number of Web resources for additional information about the PCI DSS and compliance, but because a community bank's obligations vary depending on their environment, consulting an expert is recommended. **B**

Mike Petitti is senior vice president for AmbironTrustWave. In January 2007, AmbironTrustWave, a leading provider of data security and compliance management solutions, acquired managed security provider SecurePipe.

Resources

The Payment Card Industry Data Security Standard

Download the standard
www.pcisecuritystandards.org/tech

Validation levels, deadlines, and more

American Express
www.americanexpress.com/data security

Discover
www.discovernetwork.com/data security

MasterCard
www.mastercard.com/sdp

Visa
www.visa.com/cisp

Loss recovery for issuing banks

Visa's advanced authorization program
www.visadps.com/services/authorization_processing.html

Visa's Account Data Compromise Recovery (ACDR) program
usa.visa.com/merchants/operations/adcr.html