

by Michael E. Smith



Have You Given Thieves the Key to Your Register?

There's an old story of two campers who are sitting around a fire when a bear wanders into their camp. The first camper responds by putting on his running shoes. "You can't outrun a bear," the second camper says. The first camper replies, "I don't have to outrun the bear; I just have to outrun you."

The first camper in the story drives home a crucial message for securing hotel and restaurant cash registers—and your customers' payment card data: although criminals will always be among us, there are steps we can take to become a less attractive target. By eliminating these vulnerabilities and reducing the possibility of exposure or theft, you can avoid becoming the next target of opportunity.

Hotel and restaurant operators are first-hand witnesses to the recent consumer trend away from cash and checks in favor of payment cards. Debit cards account for a large and growing share of purchases in both venues. Consumers can use debit cards in two ways: they can sign the receipt or they can enter their PIN. Increasingly, consumers are entering their PIN, and as volume increases the need for strong security protections becomes all the more important.

A new breed of criminals has their sights set on this trend, and these devi-

ants are using increasingly sophisticated technology in their attempts to steal PIN numbers and other valuable payment card information. Such criminals are constantly probing for vulnerabilities that will yield the biggest profits while presenting the least degree of risk.

The payments industry has always placed a large emphasis on PIN security, creating worldwide payment system requirements for PINs and cryptographic key management. Today, initiatives and controls continue

to evolve to safeguard PIN transactions.

The Payment Card Industry PIN Security Requirements, mandatory for all participants in the transaction processing chain that accept cardholder PINs, represent another safeguard. Of the 32 PCI PIN security requirements, there are five critical areas where merchant non-compliance could potentially subject payment data to an extremely high level of risk. Merchants are urged to carefully review their processing environments to ensure they comply with these critical requirements.

Merchants should review the requirements below to validate their level of compliance and refer to the PCI PIN security requirements manual, as needed.

>>Use Compliant Equipment – Purchase only terminals that have been lab-evaluated and approved for use by payment card companies, and work with your merchant bank or encryption and support organization (ESO) to create a plan that ensures all deployed POS PIN pads are payment card company-approved and use triple DES encryption (TDDES).

>>Do Not Log PIN Blocks – Although PINs are protected in an encrypted or enciphered form within a transaction message, they must not be retained in transaction

Visa's PIN Security Best Practices Guide

To help merchants avoid such risk, Visa offers a PIN Security Best Practices guide, which details several proactive measures to effectively reduce the threat and risk of PIN data exposure that include the following:

1 Do not store magnetic-stripe data after transaction authorization. The full contents of track data, which is read from the magnetic stripe, must not be retained on any system once a transaction has been authorized. Do a thorough review of all payment applications to ensure non-storage of magnetic-stripe data, then confirm the review findings with your service providers.

2 Educate your line management. Talk to your employees about the potential for PIN compromise when POS PIN pads are missing or when there are any noticeable signs of device tampering. Inspect POS PIN pad inventories regularly.

3 Restrict terminal/PIN pad access. Make sure you use only authorized personnel to service deployed terminals and PIN pads. Properly manage PIN pad inventories and physically secure PIN pads at all locations so they cannot be easily removed, modified or replaced.

4 Report suspicious activity. Immediately contact your merchant bank and law enforcement if you suspect tampering of any POS PIN pads.

5 Evaluate your current/pending payment applications. Confirm the security of your payment applications using the Payment Application Best Practices (PABP), which can be downloaded from the CISP Web site at www.visa.com/cisp. This site also lists all software vendors whose payment applications have been validated by a Visa-approved security assessor.

journals or logs subsequent to PIN transaction processing.

>>Always Maintain Secure Key Loading Procedures

– When POS PIN pads and host security modules are first initialized, they must be securely loaded with encryption keys. Regardless of the type of tamper-resistant security modules being initialized, the principals of split-knowledge and dual-control must be in place at all times to maintain the secrecy of the key being entered.

>>Only Use Keys for a Single Purpose – To limit the magnitude of exposure should any key be compromised, encryption keys must be used only for their intended purpose. This applies to all keys used in POS PIN pads and network processor links. Production keys must never be shared or substituted within an entity’s test system. All master keys or hierarchy keys used in any production or test environment must be unique and separate for each environment.

>> Ensure All Devices Have Unique Keys – Cryptographic keys resident within a PIN pad must be unique to that device. This



includes key exchange keys, and PIN encryption keys. By ensuring that these keys are unique to each device, a merchant can make sure their PIN pads are unattractive targets for an attack. This is because a unique key that has been compromised exposes only those PINs that were actually entered at the particular device attacked.

With the speed of today’s technology, the threats to the payments system will not lessen. Working together, financial institutions, merchants and third-party vendors must strive to anticipate future threats, and harden our collective environment against them. By looking closely at their own enterprises and taking action to avoid critical vulnerabilities, hospitality merchants can help ensure that criminals intent on committing PIN fraud look elsewhere.

Michael E. Smith is senior vice president, enterprise risk and compliance at Visa U.S.A.

Connect. Manage.

Demand Management
for the global travel industry

- Automate multiple distribution channels
- Exceed your revenue goals
- Eliminate booking errors
- Streamline processes

www.hotelbookingsolutions.com • 678-391-3100 • info@hbsconnect.com

