



Defeating Credit Card Fraud

What Retailers Need to Know

- **Credit Card Fraud is a Global Issue**
- **Visa and MasterCard Take Steps to Address Device Tampering**
- **How Vulnerable are You to Fraud?**
- **Is Now the Time to Upgrade Your Equipment?**



Credit Card Fraud is a Global Issue

Fraud and theft are a constant concern of retailers and trying to catch criminals isn't getting any easier. Recently customers in two Rhode Island Stop & Shop stores had their credit card information stolen by thieves who removed terminals from store checkout lanes, cleverly placed electronic bugs inside the terminal and returned them to the store checkout without store personnel being aware of the thieves' actions. This information theft occurred only weeks after TJX Cos. of Framingham, parent company of Marshall's, TJ Maxx and other stores announced that thieves had broke into a computer database, potentially as early as 2003, and stole credit card numbers by the millions to make illegal purchases from Florida to Hong Kong.

Credit card fraud is a global concern. In July 2006, Canadian police arrested 10 people they say used rigged card terminals to intercept PINs as cardholders entered them at the point of sale as part of a scheme in which they stole \$4 million (Canadian) from 18,000 customer bank accounts. Suspects swapped their own card readers for those installed in some 42 convenience stores and gas stations in the Montreal area, then used Wi-Fi connections to send PINs and card numbers to a remote receiver. With that information, they were able to forge cards and loot the associated accounts through ATM withdrawals. Apparently stores clerks were bribed to install the bugged card readers.

According to the British organization Card Watch, in the United Kingdom most plastic card fraud on UK-issued cards is committed via face-to-face transactions in retail stores. Common credit card fraud involves store ATMs. Criminals commit fraud at cash machines in a number of ways:



- Skimming (Machine Tampering) – a skimming device is attached to the card entry slot to record the electronic details from the magnetic stripe of your card as it is inserted into the cash machine. A separate, miniature pinhole camera is hidden overlooking the PIN pad to film you inputting your PIN. This enables the criminal to produce a counterfeit card with your card details on it and to withdraw money at a cash machine, using your PIN.
- Shoulder surfing – where criminals look over your shoulder and watch you enter your PIN, then steal your card using distraction techniques or pick-pocketing.
- Card-trapping – a device, inserted into a cash machine card slot, retains your card inside the cash machine. The criminal then tricks you into re-entering your PIN while they watch. After you stop trying and leave the machine the criminal removes the device.

Visa and MasterCard Take Steps to Address Device Tampering

You may have read recently about new standards being implemented by Visa and MasterCard jointly to implement security standards designed to reduce credit card fraud both at a retail store level and at retail data centers. One of the areas addressed at store level is the tampering with credit card PIN-entry devices and credit card terminals. This is the type of fraud experienced by Stop & Shop.

Addressing card entry device fraud is not new to Visa and MasterCard. They have developed standards for fraud reduction in the past and will continue to do so in the future. From a historical perspective, one of the earliest standards developed by Visa was known as Visa PED (PIN Entry



Device) and was implemented in 1997. Today both Visa and MasterCard define PED security requirements, these security requirements are known as PCI-PED. PCI is an acronym for Payment Card Industry. Since its inception, the PED requirements have been update to address the latest forms of device tampering.

Visa PED

Version 1 - 1997: Announced in 1997 and put into effect in 1998, version 1 of the Visa PED program was a self-administered program in which the manufacturer of PIN-entry devices and credit card terminals must comply with a defined set of security requirements.

Version 2 – 2002: The program was modified with additional security requirements and introduced the use of accredited evaluation laboratories to validate the vendor response to the questionnaire. This version also stated all PEDs must support Triple DES.

Version 3 – 2003: This version modified PED to incorporate minor changes made to better support terminals that provide internal PIN functions and allow for the ability to shift liability for application authentication from the manufacturer to the acquirer or an agent of the acquirer.

PCI-PED

Version 1 – In 2004: MasterCard and Visa agreed to form one common set of security requirements for PIN entry devices. In the agreement MasterCard agreed to accept those approved devices that had been evaluated by an accredited security laboratory. The



PCI requirements defined a much more stringent set of requirements for PIN entry devices. Instead of relying on switches and epoxy for tamper detection and physical security, PCI-PED required a minimum cost threshold for finding vulnerabilities and exploiting those vulnerabilities. PCI has also established that starting January 1, 2008 all newly purchased PEDs must meet PCI-PED requirements. Visa PED approved devices are now referred to as pre-PCI-PED approved devices. For all those PEDs that pre-date Visa PED and are not listed as approved PIN entry devices a sunset date was set. All devices that are not on the approval list must be removed from service by July 1, 2010.

Version 2 – 2008: PCI-PED requirements are constantly evolving. PCI-PED version 2 is set to go into effect April 1, 2007 with a mandate that all PEDs submitted for evaluation after April 1, 2008 must meet version 2 requirements. PCI-PED version 2 provides even stricter security requirements. There are a number of changes to the requirements but the most significant is allowing case replacement as a valid attack. Under version 1, the time and cost required to repair damage to a PED that has been compromised is calculated in the overall attack cost. Now the PED must become inoperable no matter what damage is made to defeat the security mechanisms. Version 2 also includes the magnetic stripe reader (MSR), if the PED has one, to the security zone. This rule was adopted by Visa and MasterCard because PED magnetic stripe readers were having bugs attached to the reader to capture card information.

One thing is clear, as technology evolves so will the methods used by criminals to steal credit card information. PCI-PED requirements will continue to change to thwart new methods of attacks.



How Vulnerable Are You to Fraud?

It is no surprise to most retailers that the greatest chance for fraud in your store is employee theft. In fact a study conducted by the University of Florida and sponsored by ADT found that employee made up 42.7 percent of the total losses, shoplifting 34.4 percent, administrative error 17.6 percent and vendor fraud 6.3 percent.

Most retailers have found that the best way to reduce fraud exposure is to be on the offensive through exercising good business judgment in the management of store operations. According to *Retail Speak Magazine* typical common sense actions taken by retailers involve creating a loss prevention culture which includes implementing loss prevention teams at store level, centralizing the corporate loss prevention function, developing key store metrics and monitoring key store EPOS data.

These principles also apply to the protecting your store from credit card equipment tampering. Two key ways of reducing potential for the embarrassment associated with credit card fraud are employee education and monitoring and the upgrading of older credit card equipment. Don't ignore deterrence. Let cashiers and managers know how fraud and error leaves tracks that can be detected. Use simple precautions such as insuring that all equipment is in each lane at the end of the business day and that scheduling of employees is done in such a way as to reduce the chance of equipment being taken from the store in the evening and returned first thing in the morning.

Upgrade older credit card equipment. Security standards for store payment equipment are being upgraded continually as we've discussed. Remember



that fraud flows to the most vulnerable operations and this applies to credit card equipment.

Is Now the Time to Upgrade Your Equipment?

Most retailers take a broad view of fraud prevention as it applies to their retail stores. Each fraud element is prioritized and procedures are put in place to minimize the potential loss associated with each level of risk. Spending dollars where the greatest potential savings in fraud reduction exists is just good common sense.

These same rules apply to your store PIN-entry devices and credit card terminals. If your equipment was purchased prior to January 2004, this may be a good time to evaluate upgrading your equipment. When Visa and MasterCard announced their plans to create a common standard in 2004 most equipment manufacturers anticipated the change to PCI-PED and incorporated many of the security features recommended by Visa and MasterCard before they were required by code.

The decision to upgrade your payment equipment now will most likely be based upon any number of factors. Common factors influencing the purchasing decision include general wear-and-tear of existing equipment, cost of warranty/ repair of existing equipment, new features available on the latest manufacturer's model as well as price point.

With equipment replacement cycles continually shortening many retailers are developing ROI models to help in their upgrade decision. When evaluating equipment security risk, it may be wise to talk with your equipment supplier to weigh the potential liability associated with equipment



tampering. You may find that your equipment meets most but not all of PCI-PED requirements. In some cases it may even make sense to purchase equipment now at competitive prices and then skip a generation of security standards before making your next purchase.

You are never fully safe from fraud. Therefore developing a culture of risk management as it applies to all potential forms of store fraud is imperative. The on-going planning for payment equipment purchases needs to be an integral part of your fraud prevention program.



Hypercom Corporation
2851 West Kathleen Road
Phoenix, Arizona 85053 USA
TEL: +1.602.504.5000
FAX: +1.602.504.4655
www.hypercom.com

© 2007 Hypercom Corporation. All rights reserved.

This publication is propriety to Hypercom and intended solely for use by Hypercom customers. It may not be reproduced or distributed for any purpose without the written permission of Hypercom.

The information Hypercom furnished in this publication is believed to be accurate and reliable. However, Hypercom assumes no responsibility for its use. Hypercom also reserves the right to make changes to the publication at any time without notice.

Trademarks

Hypercom is a registered trademark of Hypercom Corporation. The Hypercom logo is a trademark of Hypercom Corporation.

Hypercom has attempted throughout this publication to distinguish proprietary trademarks from descriptive terms by following the capitalization style the manufacturer uses. Every effort was made to supply complete and correct information. Any error in identifying or reflecting any proprietary marks or notices is inadvertent and unintentional.