

BEST PRACTICES: HELPING TO PROTECT YOUR PIN ENTRY DEVICES AND BUSINESS FROM FRAUD

Fraud prevention is an increasingly hot topic across all industries that accept payment cards for goods and services. As a result, Canadian merchants continue to look for ways to include additional security measures into their point-of-sale environment. Central to these efforts is the security of merchant's PIN entry devices (PEDs).

At Chase Paymentech, we take fraud seriously. That is why we have developed this short Best Practices piece to enhance your current fraud prevention measures. The Best Practices are broken out into three sections to illustrate the various aspects of fraud prevention: Procedural, Physical and Technical:

PROCEDURAL BEST PRACTICES:

1. Educate all staff, including management and front-line, on proper card acceptance.
2. Properly process all credit and debit cards; Chip and PIN cards included.
3. Educate your staff on and always follow all card verification procedures (see Payment Brand websites for full details)
4. Remind customers to use their hand and/or body as a shield while keying in their PIN.
5. Record and audit the make, model and serial number of all payment equipment nightly, using a central tracking and signoff sheet to ensure all codes match.
6. Restrict access to your point-of-sale equipment to staff and authorized service personnel only. Ensure to always validate the identity of any technicians.
7. Administer thorough background checks on both seasonal and non-seasonal employees (where allowed by law). Always make informed decisions when hiring staff.¹
8. Immediately report all stolen, decoy or suspected tampered devices to Chase Paymentech and if applicable, your terminal provider. All stolen and/or decoy devices should also be reported to the local police department.

PHYSICAL BEST PRACTICES:

1. Your terminal and/or PIN Pad should be located where it is not visible or accessible from outside traffic and hidden when not being used.
2. Treat your PIN Pads like they were cash and lock them up at closing.²
 - o If you have a question with regards to how to properly remove your PIN Pad from the POS you are using, please contact Chase Paymentech Merchant Support at: 1.800.265.5158
3. Consider physically securing terminals and PIN Pads to counters using locking stands to help prevent removal. Although they come at an additional cost, they do provide another layer of physical security for your PEDs. Stands with alarms are also available.
4. Make sure to secure any loose cable connections and record how many connections (leads, aerials, etc) are normally associated with each terminal.³
5. Provide a screen or panel for customers using PIN entry devices for added privacy. Some PIN Pads already have a privacy panel included by the manufacturer.

6. Regularly monitor the area surrounding your terminal equipment for any evidence of skimming equipment. Build terminal inspections into shift changes and also make it a habit and a daily procedure to document these inspections of your payment terminal area.⁴ This is especially important for unattended devices such as self-checkout lanes, pay-at-the-pump, etc. as they are most vulnerable to skimming.
7. Regularly check your POS terminal and/or PIN Pad for noticeable tampering. This includes checking security seals for any signs of disruption or even removal. Again, check that the serial numbers match those on file.
8. Periodically weighing the equipment and comparing it to vendors' specification weight to identify if bugging devices may have been inserted.⁵
9. Check for pin-hole cameras that could be hidden in the ceiling and surrounding areas.⁶
10. Consider adding surveillance cameras directly around the point of sale area.

TECHNICAL BEST PRACTICES:

Point-of-sale and PIN Entry Device (PED) equipment protection needs to meet certain technical criteria to help protect your business from various forms of fraud. Prior to 2003, PED security standards were controlled by each payment brand vendor and varied greatly based on security requirements for both PINs and PEDs. Security standards, development and testing for PIN Entry Devices are now managed by the Payment Card Industry Security Standards Council (PCI SSC). The requirements for PED are streamlined through the council ensuring that consistent and up-to-date security measures are in place.⁷

1. Always use equipment that meets PCI SSC requirements. You can find these at: https://www.pcisecuritystandards.org/security_standards/ped/index.shtml.
2. Ensure that you have the most up-to-date version of your payment application software. Older versions may lack adequate functionality to facilitate Payment Card Industry Data Security Standard (PCI DSS) compliance.

Risk management practices for fraud are not a perfect solution. However, when used properly, they do add an additional layer of security. Adjusting your point-of-sale setup and closer monitoring of your payment devices is something that managers and frontline staff can carry out to help protect customer information and the business from fraud attacks.

A critical piece to implementing or reinforcing any fraud prevention practices is to communicate to your front-line early and frequently. Ultimately, it is your front-line staff that will drive your company's approach to preventing and detecting fraud. Reinforcement of fraud training for employees (including seasonal, part-time, volunteer, etc) is central to helping to protect your business from potential fraud – especially during holidays and peak seasons where fraudulent activity is at its highest.

There is no one solution to prevent fraud. Rather, there are layers of protection offered by Chase Paymentech and steps you can take at the store level that may help to mitigate fraud. As such, it is important that your policies and procedures for fraud prevention are current and reflective of trends in your industry. As always, feel free to contact your Relationship Manager for any questions you may have.

Sources:

1. PCI SSC. "Skimming Prevention Form." <www.pcisecuritystandards.org/pdfs/skimming_prevention_form.pdf>, August 2009.
2. Interac Canada. "Prevent Fraud." www.interac.ca.
3. PCI SSC "Skimming Prevention: Best Practices for Merchants." August 2009.
4. ibid
5. ibid
6. Interac Canada. "Security." www.interac.ca.
7. PCI SSC. "PCI PED Frequently Asked Questions." April 2008

Chase Paymentech provides the compilations, summaries and other information contained within "NewsFlash" to serve as general guidelines and is provided "as is". While we strive to make sure this information is accurate, Chase Paymentech does not warrant the completeness, timeliness, or suitability of this information for your specific needs. In addition, the compilations, summaries and information contained within this document do not substitute for the Payment Brand Rules, which are part of your contract with Chase Paymentech.

We appreciate the opportunity to serve as your payment processor. We value our partnership and remain committed to providing you the product and service solutions you need to increase your operational efficiency. TM Registered Trademark of Chase Paymentech Solutions, LLC, Chase Paymentech Solutions authorized user. All other trademarks, registered trademarks, product names and logos identified or mentioned herein are the property of Chase Paymentech Solutions, LLC, or their respective owners. © 2010, Chase Paymentech Solutions. All rights reserved.
