PAYMENT SECURITY

Best Practices

VeriFone®
THE WAY TO PAY™

At VeriFone, the protection of cardholder information is a **top priority.**

To ensure merchants have secure payment solutions for their customers, and to help protect merchants from penalties levied by Payment Card Industry Data Security Standards in the event of a breach, we have developed a series of best practices that apply to traditional PIN pad devices, as well as today's leading-edge payment solutions that incorporate touch screens and advanced wireless capabilities. These best practices will help retailers determine whether an existing payment device has been tampered with, while also outlining measures that can prevent security breaches from happening in the first place.

Why should merchants be concerned about security?

The PCI Council adopted PIN Transaction Security (PTS) requirements because of concerns that sophisticated criminals may have the resources to tamper with payment devices and collect personal card data. Prior to the advent of PCI, the burden of security lay almost completely on the retailer; but now, security requirements have been standardized across the industry to make tampering progressively more difficult. While this does mean that today's PIN pad and POS devices are inherently more secure than those developed pre-PCI, the simplest and often most effective preventative measures are still those that retailers and merchants can incorporate into routine operations.

How do PIN pad-based security breaches happen?

Criminals are targeting less secure devices, which often pre-date PCI compliance requirements – typically either tampering with an in-store device or obtaining the same device that a retailer uses and modifying it for criminal purposes before substituting the tampered device for the retailer's device. The criminal then either returns to retrieve the device to obtain the stolen information, or in some cases, the device transmits personal card data wirelessly to another off-site computer.

Today's newer devices incorporate a number of physical security precautions designed to make it extremely difficult to modify a device. These precautions are constantly tested and certified by independent labs.

How to Protect **Your Business** and **Your Customers**

Even with the physical security built into today's devices, there are things that merchants can do to significantly reduce the likelihood of a device being subjected to tampering.

Physical Hardware

1. **Perform routine visual inspections of every device**, looking for potential signs of tampering. Also keep track of any operational difficulties that begin happening on a regular basis. Some examples of things to look for include:
   - Damaged or altered tamper seals
   - Missing manufacturer labels
   - Missing screws or screws with damaged heads
   - Incorrect keyboard overlays
   - External wires
   - Holes in the device housing
   - An electronic serial number that does not match the number printed on the label on the bottom of the device
   - A high number of mag-stripe read failures or debit card declines
   - Difficulty inserting a chip and PIN card into the EMV slot

   If you notice these or anything else out of the ordinary, stop using the device immediately and disconnect it from the POS device or network, but do not power it down. Immediately contact your bank or services provider, corporate security team, or local authorities, and explain your concern. Continue to perform visual inspections weekly in high-traffic areas and more frequently in locations with low foot-traffic or PIN pad use.

2. **Store spare devices under lock and key** to prevent unauthorized removal. Incorporate a shift change procedure to validate the inventory of devices at every shift to ensure none have disappeared. Physically inspect devices before deploying them for use.

3. **Institute a procedure that requires all visiting repair technicians to sign in with their name and company information** and to track the serial numbers of any devices that are installed, removed and/or replaced.

4. **Securely mount devices** so that cables cannot be unplugged simply by turning the device over. You may also want to consider installing locking stands to prevent unauthorized removal.

Software

5. **If your POS equipment is connected to a network via Ethernet,** ensure you have a working and updated network firewall where the connection enters your location.

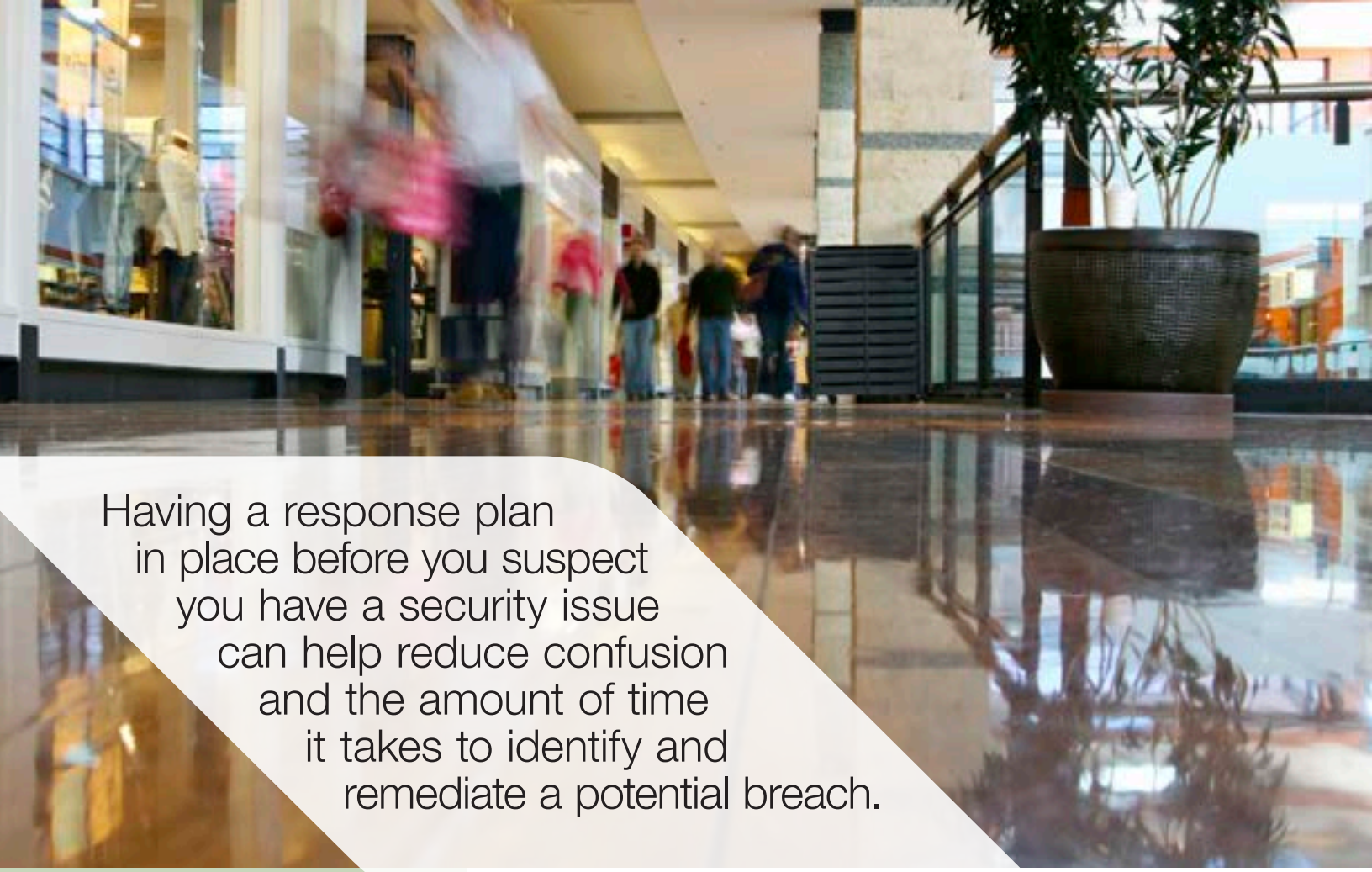
6. **Make sure your POS equipment is protected by an encryption and tokenization solution** that encrypts credit card information at the point of capture (swipe, tap, etc.). As added protection, you may want to install an estate management solution that lets you monitor the status of all of your devices. In addition to monitoring normal system functions (power, faulty hardware, etc.), it can also provide alerts related to encryption and tokenization.

7. **Change the device's default admin password.** These default passwords become widely known. Contact your account executive if you need help changing this password.

Purchase & Repair

8. **Only obtain payment devices from a manufacturer or a manufacturer's authorized partner.** Unauthorized resellers, which often may be found online at sites such as eBay, may potentially sell devices that are already compromised, whether intentionally or unwittingly.

9. **For similar reasons, have your devices repaired by the manufacturer or at an authorized manufacturer's repair center** that has completed a key injection audit.



Having a response plan in place before you suspect you have a security issue can help reduce confusion and the amount of time it takes to identify and remediate a potential breach.

At a minimum, this plan should include:

1. Steps to take to isolate all suspect payment systems to prevent further loss of information and to preserve the attack method used for future investigation.
2. A contact list: Local law enforcement, acquiring bank, your processor, a qualified security assessor and any payment system vendors with which you work.

At VeriFone, we take a strong stance on security. With more than 30 years of experience, we are leveraging our close relationships with retailers, banks and industry bodies to develop and deliver the most dependable and secure payment solutions across all retail environments. In fact, all VeriFone payment solutions, including our payment processing software, conform to the most stringent security requirements outlined by the PCI Council. Our ultimate goal is to make it impossible for fraudsters to commit card crime, thereby allowing consumers to enjoy peace of mind when using their payment of choice.

Taken together, these best practices should significantly reduce the risk of device tampering and compromise. Though the chance of a consumer becoming a victim of card fraud remains low, we can never be too vigilant when it comes to customer data security and brand reputation.

About VeriFone Systems, Inc. (www.verifone.com) VeriFone Systems, Inc. (“VeriFone”) (NYSE: PAY) is the global leader in secure electronic payment solutions. VeriFone provides expertise, solutions and services that add value to the point of sale with merchant-operated, consumer-facing and self-service payment systems for the financial, retail, hospitality, petroleum, government and healthcare vertical markets. VeriFone solutions are designed to meet the needs of merchants, processors and acquirers in developed and emerging economies worldwide.

www.verifone.com