VISA SECURITY ALERT

December 2016

THREAT LANDSCAPE: SKIMMING IN A CHANGING ENVIRONMENT

Distribution: Merchants, Acquirers, Risk Personnel

Skimming Landscape

As the US market migrates to EMV chip, the fraud threat from criminals placing skimming devices on or in attended and unattended point-of–sale (POS) devices for the purpose of collecting payment card information, including PIN numbers, increases. Perpetrators use skimmed payment information to quickly create counterfeit cards re-encoded with the stolen card information typically resulting in ATM withdrawals. Any POS terminal may be at risk, including those that are often unattended, such as terminals near deli counters, coffee stands as well as unattended self-check-out lanes, Automated Fuel Dispensers (AFD) and kiosks. Most entities targeted are still using payment devices that have not been upgraded to accept EMV cards including POS terminals, AFDs, kiosks and ATMs. The perpetrators are mobile and will target multiple stores within a geographic area for a period of time before moving on to a new location. Further, some skimming devices are Bluetooth-enabled allowing the suspects to remotely recover payment card data.

Placement of Skimming Devices

Skimming devices can be placed at any time of the day but placement usually occurs during the slower times of business when the perpetrators can go undetected by employees or other customers. The perpetrators will usually work in teams of two or more with one person being a lookout, one person placing the skimming device on the payment terminal and another creating a barrier so that no one can observe the skimming device being placed. Perpetrators have been known to use large items such as packs of paper towels to block the view of POS terminals or in the instances of gas pump skimming large vehicles such as trucks or commercial vans have been used. In some instances, it was reported that the suspects created a distraction in the store by being overly engaging with the store personnel to draw their attention away from the payment terminals.

Recommended Inspection & Response Actions

1. **Prevention Through Device Inventory Management**
   - In accordance with PCI DSS Requirement 9.9 and PCI PIN Security Requirements control objectives 6 and 7, ensure implementation of security controls to protect POS and PIN entry devices (PED) from tampering and substitution. Examples include:
     - ➢ Maintain a list of devices including the device serial number or other method of unique identification.
     - ➢ Keep a list of device location either by store or physical location within the store itself (e.g. self-checkout, deli counter, manned checkout).

    - ➢ Train personnel to be aware of suspicious behavior and to report tampering or substitution of devices.
    - ➢ Only use approved PEDs and follow Visa's PED usage and retirement mandates detailed on www.visa.com/cisp under the PIN Security section. Comply with Visa's mandatory PED sunset dates www.visa.com/pin
    - ➢ Be aware of who has access to your payment terminals including
        - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
        - Be aware of who has access to your payment terminals and through what process they can be accessed through (i.e. if a key is needed to access a gas pump be aware if the key is generic in nature or specific to one location. Generic keys can make a business a target for skimming devices.)

2. Physical Inspection of POS and PIN entry Devices

- Implement security procedures to inspect POS and PIN entry devices (PED) at least twice each day and at random times.
- Physically examine the device. Skimming devices are typically attached with minimal adhesive allowing them to be place and removed with ease, so devices may be detected by giving the front of the POS/PED a good grab-and-pull. Weighing the devices may also identify tampering.
- Some skimming devices are Bluetooth enabled which allows the capture of data without recovering the device.
- Simple abnormalities — a missing seal or screw, or extra wiring or holes, for instance — could be the first step to uncovering fraud. You should also look out for added labels, decals or other materials that may be masking damage inflicted by tampering.
- If possible, when inspecting devices, use backup security personnel to monitor from a distance as suspects may watch compromised terminals and suspects are trained in counter surveillance to avoid detection/arrest.
- Skimming devices placed inside of AFDs can be detected by following the ribbon tape that is inside the pump self. All connectors should be in use and if factory connections are not plugged in the pump should be inspected further. Gas pumps should also be inspected for any devices that may be sealed in shrink wrap or electrical tape as most of the skimming devices we are aware of are secured in that manner.
    - ➢ Be familiar with how your pump should look under normal operation to detect abnormalities
    - ➢ PCI SSC PTS program has secure solutions that should be implemented and that can help to prevent against such internal attacks

3. Device Recovery Response

- If a skimming device is discovered, do not handle it, as evidence may be damaged.
- Notify local law enforcement and the FBI or USSS office so they can properly recover the skimming device.
- Maintain any video surveillance that may be used to identify any perpetrators and confirm timing of when the device was placed on the POS terminal.
- Initiate incident response procedures and notify your Acquirer so that Visa can assist with the investigation. If a window of exposure can be established as to when the device was place and removed, the at-risk Visa accounts and the suspected data elements at risk (e.g. track data and or PIN data) must be sent to Visa via the CAMS system by the financial institution.

- Review security procedures to identify if any gaps exist that allowed the skimming incident to occur and make necessary changes to protect payment data.

Additional Resources
Visa's What to Do If Compromised Procedures

PCI Security Standards Council Skimming Resource Guide
PCI Data Security Standard
www.visa.com/pin
www.visa.com/cisp

For other questions, please contact Payment Intelligence via email at paymentintelligence@visa.com