VISA SECURITY ALERT

April 2016

THREAT LANDSCAPE: PIN PAD/POS SKIMMING

Distribution: Merchants, Acquirers, Risk Personnel

Incident Details

Visa Global Payment System Risk is aware of increasing incidents involving suspects placing skimming devices on point-of–sale (POS) terminals for the purpose of collecting payment card information, including PIN numbers. Perpetrators use this information to create counterfeit cards re-encoded with the stolen card information and make unauthorized ATM withdrawals. The primary targets for these recent skimming events are self-checkout terminals in supermarkets. However, any POS terminal may be at risk, including those that are often unattended, such as terminals near deli counters, coffee stands, etc. 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. Most entities targeted are using payment devices that have not yet been upgraded to accept EMV cards.

Placement of Skimming Devices

Skimming devices can be placed at any time of the day but placement usually occurs during 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 POS 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. In some instances, it was reported that the suspects created a distraction in the store by faking a medical incident or causing commotion that distracted the attention of store personnel away from the POS terminals. The skimming devices will mimic the look of the front of the POS terminal.

Recommended Inspection & Response Actions

1. **Prevention Through Device Inventory Management**
   - In accordance with PCI DSS Requirement 9.9, ensure implementation of security controls to protect POS devices 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 (i.e., self-checkout, deli counter, manned checkout).
     - ➢ Train personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

- 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.

2. **Physical Inspection of POS Devices**
   - Implement security procedures to inspect POS devices 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.
   - Please note some skimming devices are Bluetooth enabled and data can be captured without the device needing to be recovered.
   - 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.

3. **Device Recovery Response**
   - If a skimming device is discovered on a POS terminal, do not handle it, as evidence may be damaged.
   - Notify local law enforcement and the FBI or USSS office so they can recover the skimming device.
   - Protect 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.

Additional Resources
Visa’s What to Do If Compromised Procedures

PCI Security Standards Council Skimming Resource Guide
PCI Data Security Standard

For other questions, please contact Cyber Intelligence & Investigations via email at USFraudControl@visa.com