Consumers

The loss of consumers’ trust in their payment brand and the payment system is not good for anyone involved in the payment chain. Not only must consumers deal with the inconvenience of compromised account data but they are also challenged to return to their normal payment practices after such an event. This loss of trust is leading to strained relationships between merchants, merchant-servicing financial institutions, and the various payment networks. Some observed consumer behaviors after a skimming incident are very disconcerting for both financial institutions and merchants. They include but are not limited to changes in buying patterns, changes in shopping locations, self-reduction of credit lines, movement to alternate payment methods and their respective cost management (cash), and less use of direct debit card products at the point of sale (specifically when PINs are also compromised).

Examples of Terminal Fraud

The following photographs are designed to assist in understanding the attack techniques used by criminals at merchant locations.

<table>
<thead>
<tr>
<th>Image</th>
<th>Attack Technique</th>
</tr>
</thead>
</table>
| ![Image 1](image1.jpg) | **Image 1**
Terminals will have a sticker attached to the underside, which provides details of the product and will include a serial number. The majority of terminals will also have a method of displaying the serial number electronically.

As part of your regular checks, note the serial number on the back of the terminal and check this against the electronic serial number.

Additionally, run your finger along the label to check that it is not hiding a compromise. |
The intent of this document is to provide supplemental information. Information provided here does not replace or supersede PCI security standards and requirements.

<table>
<thead>
<tr>
<th>Image</th>
<th>Attack Technique</th>
</tr>
</thead>
</table>
| ![Image 2](image2.jpg) | **Image 2**  
Terminals often have security stickers, or company stickers placed over screw holes or seams that will act as indicators if the case has been opened.  
Criminals often remove these labels when compromising terminals and may replace them with their own printed versions.  
When you first receive the terminal, make careful note of label position, colour, and materials used. Taking a picture of the device is a good practice.  
Also look for any signs that the label may have been removed or tampered with. |
| ![Image 3](image3.jpg) | **Image 3**  
Skimming devices hidden within the terminal will not be visible, and neither the merchant staff nor the cardholder will know that the card has been skimmed.  
This picture shows a skimming device inserted in a terminal. This would have been hidden by the SIM card cover plate. |
The intent of this document is to provide supplemental information. Information provided here does not replace or supersede PCI security standards and requirements.

<table>
<thead>
<tr>
<th>Image</th>
<th>Attack Technique</th>
</tr>
</thead>
</table>
| ![Key Logger](image4.png) | **Image 4**  
Key loggers are used to record all keystrokes made, in this case by an electronic cash register.  
Key loggers can be very small and can look like part of the normal cabling. It is therefore essential to pay close attention to detail when performing any inspection. |
| ![Changes to terminal connections](image5.png) | **Image 5**  
Changes to terminal connections can be difficult to spot.  
In these images, the criminals completely changed the cable used to connect the terminal to the base unit.  
This was to incorporate the additional wires required to capture card data. |
| ![Modern digital cameras](image6.png) | **Image 6**  
The modern digital cameras used to record the cardholder entering his or her PIN are very small when removed from their cases.  
This makes them very easy to hide or disguise at the merchant location.  
This type of miniature camera can easily be hidden in a ceiling tile above the terminal. |
<table>
<thead>
<tr>
<th>Image</th>
<th>Attack Technique</th>
</tr>
</thead>
</table>
| ![Image 7](image7.png) | **Image 7**  
Staff should also be aware of additional, unfamiliar electronic equipment connected to the terminal, the cash register, or the network connections.  
This device records and decrypts ISDN data. |
| ![Image 8](image8.png) | **Image 8**  
Handheld skimmers used by corrupt staff are very small, fitting in the palm of one’s hand.  
Despite their size, these devices can store a significant amount of card data. |
| ![Image 9](image9.png) | **Image 9**  
In this picture, the criminal entered the merchant location posing as a service engineer.  
He stated that to prevent credit card fraud the terminal must be placed in this secure box. He then gave the staff a sheet of printed instructions.  
The box contained a card skimmer and miniature camera.  
**Be cautious of unannounced service visits.** |
| ![Image 10](image10.png) | **Image 10**  
These devices were used to connect into the telephone exchange of a shopping mall to record all transmissions from the stores to the merchants’ financial institutions.  
Such devices usually consist of voice recorders or MP3 players with very large memories. Often they have external batteries for improved life. |
<table>
<thead>
<tr>
<th>Image 11</th>
<th>This aerial view clearly shows how Wi-Fi signals can extend far beyond the four walls of the merchant location, allowing anyone to intercept the signal. Data should never be sent unencrypted over any wireless connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 12</td>
<td>Staff should also be aware of the addition of overlays. An overlay can be a small sticker that forms to the device and covers the keyboard area. Overlays may hide damage due to tampering or wires that can allow for keyboard logging. Overlays should not be used.</td>
</tr>
</tbody>
</table>
The intent of this document is to provide supplemental information. Information provided here does not replace or supersede PCI security standards and requirements.

<table>
<thead>
<tr>
<th>Image</th>
<th>Attack Technique</th>
</tr>
</thead>
</table>
| ![Image 13](Image) | **Image 13**
3D printers have made duplicating plastics easier. In these examples, an overlay that included a card-data and PIN skimmer was added to the device.

It is important to be aware that if the device remains off or unattended for a period of time, it should be checked periodically.

The staff should be aware and report actual or suspected changes in the operation of the device. If something is not right, report it.
The intent of this document is to provide supplemental information. Information provided here does not replace or supersede PCI security standards and requirements.

<table>
<thead>
<tr>
<th>Image</th>
<th>Attack Technique</th>
</tr>
</thead>
</table>
| ![Image 14](image14) | **Image 14**  
In an NFC attack, an NFC reader (in this case a smartphone) is placed between the terminal and the customer to capture the card data during a tap transaction. Additional equipment should not be placed near or around terminals. |
| ![Image 15](image15) | **Image 15**  
EMV or chip cards are not immune to skimming. Staff and consumers should be aware of modifications or wires to the smart-card slot. If anything appears different with the device, it should be reported immediately. |
Criminals may not use a single attack against a device, but can use a combination of attack scenarios.

In this attack we see an overlay has been placed on the ATM’s card reader to capture the card data, and an additional overlay was added to the plastic that allowed for a hidden camera to capture the PIN.

Again, it is important to be aware that if the device remains off or unattended for a period of time, it should be checked periodically.

The staff should be aware and report actual or suspected changes in the operation or look of the device. If something is not right, report it.