

## VISA Europe Device Skimming: Attacks & Defences

Today's fraudsters are organised, geographically spread and highly sophisticated. In recent months, Visa Europe has received reports that criminal gangs are actively targeting payment acceptance devices to steal payment card details, in particular, the data from the magnetic stripe of a payment card.

These attacks, often referred to as "skimming" attacks, typically involve either merchant personnel using a small portable card reader to surreptitiously capture a customer's card details or fraudsters modifying Point of Sale devices to insert an electronic "bug" to capture card data (including PINs) whilst the card is being processed as part of a normal transaction.

The impact of card skimming can be significant for all parties involved in payment services. Skimming attacks can undermine the integrity of the payment system as well as consumer trust in your business. Based upon this emerging threat, it is important that you take proactive steps to secure your device estate and ensure that your business continues to accept card payments in a safe and secure manner.

### Mitigating Techniques

Skimming attacks can be very sophisticated and difficult to detect. However, effective management of your Point of Sale devices and increased vigilance can significantly reduce the likelihood of such attacks occurring. Diligently following the simple guidance below will help make your organisation considerably more secure. Please note that these controls should be implemented in conjunction with each other (rather than in isolation) to form a layered approach to system defence.



To support increased payment security, Visa Europe is providing best practices to assist merchants and other stakeholders in protecting against common causes of system breaches. Whilst every reasonable effort has been made to ensure the accuracy of information provided by Visa Europe, Visa Europe shall not be held liable for any inaccurate information of any nature, however communicated by Visa Europe.

---

**Know your Point of Sale systems**

Merchants should track and monitor details of all payment acceptance devices that accept Visa cards. As part of this, merchants should regularly examine devices to identify anything abnormal, such as missing or altered seals or screws, extraneous wiring, holes in the device or the addition of labels or other material that could be used to mask damage from device tampering. Merchants should at a minimum check the following:

- Is the terminal in its designated location?
- Is the manufacturer's name correct?
- Is the model number correct?
- Is the serial number printed on the label and displayed on the screen correct?
- Is the colour and general condition of the terminal as described, with no additional marks or scratches (especially around the seams)?
- Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
- Are the manufacturer's security markings and reference numbers as described?
- Are any expected ultra-violet markings present and as described?
- Are all connections to the terminal as described, using the same type and colour of cables and with no loose wires or broken connectors?
- Is the number of connections entering the terminal as expected?
- Is the total number of terminals in use the same as the number of terminals officially installed?

To assist in this process, a merchant may wish to photograph and/or weigh their devices upon receipt and then use this information as a reference during inspection. If a merchant, upon review of their device(s), believes they have been subject to a skimming attack, they should contact their acquirer immediately and review the document "what to do if compromised", a link to which can be found in the appendix.

---

**Know your environment**

Many criminals use the area surrounding the PoS device to install a camera to record customer PIN entry. Merchants should verify there are no additional or unknown items such as charity boxes, display material etc. in the area surrounding their device(s). Where possible this should include the examination of the ceiling area to check for signs of tampering.

The use of CCTV can act as a deterrent to criminals and help to protect the security of PoS devices and the surrounding areas. Cameras should be positioned in such a way that they monitor the location of devices, but are not in a position to record PIN entry at the device. CCTV recordings should be retained for a minimum of 90 days.

---

**Secure your devices**

Where possible, merchants should follow vendor recommendations for physically securing their devices to prevent the substitution of devices and protect against tampering. Where permitted by the design of the device, cables connecting to terminals should be protected using a conduit or held within a physically secure structure. Note, physically securing devices should be carried out in accordance with any relevant disability legislation for the country in which the device is deployed.

---

**Implement Employment Policies**

Where legally permissible, all employees should be subject to background checks prior to hiring and made aware of their responsibilities to protect your payment devices.

---

**Use approved devices**

Merchants should only use PIN entry devices that are currently approved by the PCI SSC. A list of such devices can be found at: [www.pcisecuritystandards.org/pin](http://www.pcisecuritystandards.org/pin)

---

**Control access by Support Staff**

Merchants should develop and implement a policy and procedures to train staff to validate the identity of all payment system repair technicians. Unauthorised or unexpected service personnel should be denied access unless fully validated and authorised. Authorised and validated repair technicians should be escorted and monitored at all times.

---

**Appendix A – Additional Resources for Merchants****PCI Security Standards Council**

- PCI approved devices  
<https://www.pcisecuritystandards.org/pin>
- Skimming Prevention – Best Practices for Merchants  
[https://www.pcisecuritystandards.org/education/info\\_sup.shtml](https://www.pcisecuritystandards.org/education/info_sup.shtml)

**UK Cards**

- Security guidance for card acceptance devices deployed in the face-to-face environment  
[http://www.theukcardsassociation.org.uk/files/ukca/security\\_guidance\\_for\\_card\\_acceptance\\_devices\\_-\\_nov09.pdf](http://www.theukcardsassociation.org.uk/files/ukca/security_guidance_for_card_acceptance_devices_-_nov09.pdf)

**Visa Europe**

- What to do if compromised  
[http://www.visaeurope.com/en/businesses\\_\\_retailers/payment\\_security/downloads\\_\\_resources.aspx?](http://www.visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx?)