What to do if you're compromised by a security incident

A 2015 guide for merchants

Introduction

What constitutes a security incident? The answer to this question is crucial to any organisation looking to minimise the impact of an incident and immediate action procedures should be included in any business continuity/incident management plan.

In general, security incidents may be defined as deliberate electronic attacks on communications or information processing systems. Whether initiated by a disgruntled employee, a malicious competitor, or a misguided hacker, deliberate attacks often cause damage and disruption to the payment system. How you respond to and handle an attack on your company's information systems will determine how well you will be able to control the subsequent costs and consequences. For these reasons, the extent to which you prepare for security incidents and work with Visa Europe will be vitally important to the protection of your company's key information.

In the event of a security incident, Visa Europe members and their merchants must immediately:

- report the incident (details overleaf);
- obtain professional assistance to investigate and contain the incident.

These steps will help limit the exposure of cardholder data.

VISA always on

Identifying and detecting security breaches

It is often difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion is a critical part of maintaining a secure payment processing environment.

Security breaches come in many different forms and, while detecting them may be challenging, there are certain signs that tend to appear when a security breach has occurred:

- Unknown or unexpected outgoing internet network traffic from the payment card environment
- Presence of unexpected IP addresses on store and wireless networks
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Unknown files, software and devices installed on systems
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Failed login attempts in system authentication and event logs
- Vendor or third-party connections made to the cardholder environment without prior consent and/or a trouble ticket
- SQL Injection attempts in web server event logs
- Authentication event log modifications (i.e., unexplained event logs are being deleted)
- Suspicious after-hours file system activity (i.e., user login or after-hours activity to Point-of-Sale ("POS") server)
- Presence of .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data
- Systems rebooting or shutting down for unknown reasons
- If you are running Microsoft software, check Windows registry settings for hidden malicious code. (Note: Make sure you back up your registry keys before making any changes and consult with Microsoft Help and Support).

Steps and requirements for compromised entities

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS) and PCI Payment Application Data Security Standard (PA-DSS).

1. Immediately contain and limit the exposure and minimise data loss. Prevent the further loss of data by stopping taking Visa card transactions and divert payments to a known secure channel such as telephone.

2. Immediately report the suspected or confirmed security breach directly to your acquirer (merchant bank). If you do not know the name and/or contact information for your acquirer (merchant bank), notify the Visa Europe Data Compromise Team: +44 (0) 20 7795 5031 or email: datacompromise@visa.com

3. Immediately engage a PCI SSC accredited Forensic Investigation company (PFI) – a list can be found on the PCI SSC website: www.pcisecuritystandards.org

4. The PFI will conduct a thorough investigation of the suspected or confirmed security breach, but it is vitally important that the compromised environment or payment channel remains untouched and intact to preserve evidence and facilitate the investigation. As a guide:
   - Do not access or alter compromised system(s) (i.e., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT)
   - Do not turn the compromised system(s) off. Instead, isolate the compromised systems(s) from the network (e.g. unplug network cable)
   - Preserve logs (e.g. security events, web, database, firewall, etc)
   - Log all actions taken
   - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised)
   - Be on 'high' alert and monitor traffic on all systems with cardholder data.

VISA always on