

## What to Do If Compromised



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), PCI Payment Application Data Security Standard (PADSS), and PCI PIN Security Requirements.

1. Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:

- 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). Visa highly recommends compromised system not be used to avoid losing critical volatile data.
- Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
- Preserve evidence and logs (i.e., original evidence, security events, web, database, firewall, etc.)
- Document 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.

## 2. Alert all necessary parties immediately:

- Your internal incident response team and information security group.
- If you are a merchant, contact your merchant bank.
- If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately:

U.S. – (650) 432-2978 or [usfraudcontrol@Visa.com](mailto:usfraudcontrol@Visa.com)

- Notify the appropriate law enforcement agency. Contact the Visa Incident Response Manager above for assistance in contacting local law enforcement agency.
- The compromised entity should consult with its legal department to determine if notification laws are applicable.
- Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within ten (10) business days. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and nonpublic information.
- Within three (3) business days of the reported compromise, provide an Incident Report to the Visa client or to Visa. If you are a financial institution, provide the Incident Report to Visa. If Visa deems necessary, an independent forensic investigation by a Visa-approved Qualified Incident Response Assessor (QIRA) will be initiated on the compromised entity.

## **Steps and Requirements for Visa Clients (Acquirers and Issuers)**

### **Notification**

- Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region.
- Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.

### **Preliminary Investigation**

- Perform an initial investigation and provide written documentation to Visa within three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

## **Independent Forensic Investigation**

If Visa deems necessary, an independent forensic investigation must be conducted by a QIRA. Upon receipt of an initial independent forensic investigation notification from Visa, clients must:

- Identify the QIRA within five (5) business days.
- Ensure that the QIRA is engaged (or the contract is signed) within ten (10) business days.
- The QIRA must be onsite to conduct a forensic investigation within five (5) business days from the date the contract agreement is signed.

The Visa client or compromised entity should engage the QIRA directly. However, Visa, has the right to engage a QIRA to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the client in addition to any fine that may be applicable.

- If there is a suspected PIN compromise, the QIRA will perform a PIN security and key management investigation and a PCI PIN security assessment.
- Provide a preliminary forensic report to Visa within five (5) business days from the onsite review. The QIRA or the compromised entity can work with the appropriate region in the event that the preliminary report is delayed.
- Provide a final forensic report to Visa within ten (10) business days from the completion of the review. Visa has the right to review the forensic report and reject the report if it does not meet Visa's requirements.

## **PIN Security**

If there is a suspected PIN compromise, provide a PIN security report within ten (10) business days from the onsite review. This report should also review PIN-related cryptographic keys to determine if the keys might have been compromised.

## **Account Numbers**

Provide "at risk" account numbers to Visa within ten (10) business days from the date that Visa requests the account numbers.

## **Containment/Remediation**


Ensure that the compromised entity has contained the incident and has implemented security recommendations provided by the QIRA, including any non-compliance with the PCI PIN Security Requirements.

- If the entity is retaining full-track data, CVV2, and/or PIN blocks, ensure that the entity has removed the data (this includes any historical data). Validate that full-track data, CVV2, and/or PIN blocks are no longer being stored on any systems. Although this is the client's responsibility, Visa requires that the validation be performed by the QIRA.
- Submit a remediation plan to Visa within five (5) business days after receiving the final forensic report. As required by Visa, clients must provide a remediation plan with implementation dates related to findings identified by the QIRA. A revised remediation plan must be provided to Visa, as needed.
- Monitor and confirm that the compromised entity has implemented the action plan. Confirmation must be done by the QIRA or Qualified Security Assessor (QSA)

## PCI DSS Compliance

Ensure that the compromised entity achieves full PCI compliance by adhering to the PCI DSS, PCI PA-DSS and, if applicable, the PCI PIN Security Requirements.

**If you have any questions regarding the information in this bulletin, please contact your UMS Banking Customer Care Representative.**



**You Can't Talk Your Way Out Of This One.**

Expect to pay fines if you ignore the **July 2010 PCI PED compliance deadline.**

Merchants using never-approved devices can expect the worst. Upgrade immediately and avoid the risk altogether. Turn to VeriFone for the broadest range of PCI PED approved and PA-DSS accepted solutions.

