What To Do If Compromised

Visa Supplemental Requirements

Version 5.0 (Global)

Effective August 2016

Visa Public

Note: This document is a supplement of the Visa Core Rules and the Visa Product and Service Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Core Rules and the Visa Product and Service Rules, the Visa Core Rules and the Visa Product and Service Rules shall govern and control.

Contents

Summary

Protecting the payment system is a shared responsibility. At a minimum, all parties involved in handling payment card data, as well as those that provide services that can impact payment card data, must maintain compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements. Entities that suspect or have confirmed an account data compromise must take prompt action to prevent additional exposure of payment card data and ensure proper PCI DSS and PCI PIN Security controls are in place and functioning correctly. Account data compromises are not limited to network intrusions and the procedures and timelines also apply to compromises involving Point of Sale (POS) PIN Entry Device (PED) tampering or "skimming".

This document contains required procedures and timelines for reporting and responding to a suspected or confirmed account data compromise.

Required Steps for Potentially Compromised Entities

Preserve Evidence

To identify the root cause and facilitate investigations, it is important to ensure the integrity of the system components and environment by preserving all evidence.

- Do not access or alter compromised system(s) (e.g., do not log on to the compromised system(s) and change passwords; do not log in with administrative credentials). Visa strongly recommends that the compromised system(s) be taken offline immediately and not be used to process payments or interface with payment processing systems.
- Do not turn off, restart, or reboot the compromised system(s). Instead, isolate the compromised systems(s) from the rest of the network by unplugging the network cable(s) or through other means.
- Identify and document all suspected compromised components (e.g. PCs, servers, terminals, logs, security events, databases, PED overlay's etc.).
- Document containment and remediation actions taken, including dates/times (preferably in UTC), individuals involved, and detailed actions performed.
- Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).

Provide Visa Initial Investigation Report

Within three (3) business days of a suspected or confirmed account data compromise, provide the Visa Initial Investigation Report—beginning on page 4—to the acquiring bank or directly to Visa.

Execute Notification Plan

Immediately notify all relevant parties, including your:

- Internal incident response team and information security group
- Merchant bank (also known as your acquirer or acquiring bank)
  - If you do not know the name and/or contact information for your merchant bank, contact the Visa Risk team for assistance:

    U.S. – +1 (650) 432-2978 or USFraudControl@visa.com

    Canada – +1 (416) 860-3872 or CanadaInvestigations@visa.com

    Latin America & Caribbean – +1 (305) 328-1593 or LACFraudInvestigations@visa.com

    Asia Pacific (AP) and Central and Eastern Europe, Middle East and Africa (CEMEA) – VIFraudControl@visa.com

- Manufacturer of the impacted payment device if you have determined that the incident involves the compromise of a PIN Entry Device (PED), specifically if it is a PCI PTS-approved device.
- Legal department to determine if laws mandating customer notification are applicable.

It is strongly recommended that you also immediately notify:

- The appropriate law enforcement agency in the event of an account data compromise.
- Federal law enforcement if the compromise is in the United States. The United States Secret Service Electronic Crimes Task Forces (ECTF) focuses on investigating financial crimes and can assist with incident response and mitigation of an account data compromise.

  Visit www.secretservice.gov/investigation for ECTF field office contact information.

Perform Forensic Investigation

Visa may require a compromised entity to engage a Payment Card Industry Forensic Investigator (PFI) to perform an independent forensic investigation. If advised that a forensic investigation is required, the following timeline must be followed.

Upon discovery of an account data compromise, or receipt of an independent forensic investigation notification, an entity must:

- Engage a PFI (or sign a contract) within five (5) business days
- Provide Visa with the initial forensic (i.e. preliminary) report within ten (10) business days from when the PFI is engaged (or the contract is signed)
- Provide Visa with a final forensic report within ten (10) business days of completion of the review

The PFI cannot be an organization that is affiliated with the compromised entity or has provided services to the compromised entity such as previous PFI investigation, Qualified Security Assessor (QSA), advisor, consultant, monitoring or network security support, etc.

Visa will not accept forensic reports from non-approved PFI forensic organizations. PFIs are required to provide forensic reports and investigative findings directly to Visa.

A list of approved PFI organizations is available at:
www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

Provide All Exposed Accounts

All compromised Visa accounts (known or suspected) must be uploaded to Visa's Compromised Account Management System (CAMS) within five (5) business days from the first to occur of the following events: (a) the date Visa requests account numbers, (b) a Window of Exposure (WOE) is determined, or (c) discovery of compromised account data is identified.

- Entities should work with their acquiring bank to upload accounts
- For more information or assistance, contact Visa at: CAMS@Visa.com

Visa Initial Investigation Report

Upon notification of a suspected or confirmed account data compromise, compromised entities must initiate a preliminary investigation of all potentially impacted systems and those of any third-party service providers. Compromised entities must share the findings with Visa as well as their acquiring bank, if applicable. A preliminary investigation is not the same as a PFI preliminary report. The initial investigation will assist Visa in understanding the compromised entity's network environment and potential scope of the incident.

To comply with Visa's investigation requirements, the entity must submit securely (e.g., encryption, PGP encryption, Visa Online Secure Email, etc.) the following information within three (3) business days of a suspected or confirmed account data compromise:

Visa Investigation Report	
Name of entity:	
Type of entity:	
Acquirer BIN(s): (List all that are applicable.)	
Does the entity send transactions to a payment processor?	☐ Yes ☐ No *(If yes, attach a list of processor(s) and provide name and contact information. If reporting entity is a Processor, please provide a list of all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City and State.)*
Entity PCI DSS Level *(e.g. Level 1-4):*	
Entity PCI DSS Compliance Status:	*(If compliant, please attach proof of PCI DSS compliance documentation.)*
Approximate number of Visa transactions processed per year	• ATM • POS PIN/Debit • Credit
Is merchant entity corporate-owned or an individual franchise?	*(If merchant has other locations, please attach a list.)*
Name of payment application(s) and version(s):	• • • •

<table>
<tr><td rowspan="4">Identify responsible party(s) for the configuration and support of the Point of Sale (POS) solution
(e.g. Integrator, Reseller, or Agent).</td><td>NAME</td><td>TITLE</td><td>CONTACT</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="4">(If entity is an Integrator or Reseller, please attach a list all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City and State.)</td></tr>
<tr><td>Is this a corporate or franchise mandated payment application and version?</td><td colspan="4"></td></tr>
<tr><td>Is the terminal PC-based or is it connected to a PC-based environment?</td><td colspan="4"></td></tr>
<tr><td>Is there remote access connectivity to the entity's environment?</td><td colspan="4">☐ Yes ☐ No
If yes, which organizations have remote access?
•
•
•</td></tr>
<tr><td>What type of remote access solution is used?</td><td colspan="4"></td></tr>
<tr><td>Is remote access always on or is it enabled upon request?</td><td colspan="4"></td></tr>
<tr><td>Is the Point of Sale device EMV enabled?</td><td colspan="4">☐ Yes ☐ No
If yes, provide name and model number.</td></tr>
<tr><td>Is the POS solution enabled with point-to-point encryption?</td><td colspan="4">☐ Yes ☐ No
If yes, provide details.</td></tr>
<tr><td>Does the entity accept PIN?</td><td colspan="4">☐ Yes ☐ No</td></tr>
<tr><td>Is the entity's PIN entry device (PED), PCI PTS approved and listed on the PCI SSC website?</td><td colspan="4">☐ Yes ☐ No
Provide the PED model, hardware, firmware and application and version numbers. Visit www.pcisecuritystandards.org/pin for the list of PCI-approved PIN entry devices.</td></tr>
</table>

Is the entity co-located or hosted?	If hosted, provide name and contact information of the hosting provider.
Provide the shopping cart application and version information, if applicable.	
Describe any recent changes to the network and/or systems.	• Payment application upgrades ☐ Yes ☐ No • Installation of a firewall ☐ Yes ☐ No • Installation of an anti-virus program ☐ Yes ☐ No • Changes to remote access authentication ☐ Yes ☐ No OTHER: • • •
Has the entity received complaints regarding fraudulent transactions from their customers?	☐ Yes ☐ No Is yes, please describe.
Has entity been contacted by law enforcement regarding fraudulent transactions?	☐ Yes ☐ No If yes, list date(s) and by which law enforcement agency. • • •
If Account Data Compromise is Confirmed Provide the Following	
How and when was the incident identified?	
How did the compromise take place?	Attach documentation of the following, if known: • List of vulnerabilities that caused or contributed to the compromise • Sample of any phishing emails • Details of unauthorized activity • List of malicious IPs • Malware information, if applicable

Did entity notify law enforcement?	☐ Yes ☐ No If yes, which agency and when were they notified? Provide contact information if applicable.
If known, how many Visa cards were compromised (accounts made vulnerable as a result of a data security breach)?	
Have the impacted accounts been uploaded to CAMS?	
What data elements were compromised and/or exposed?	☐ Primary Account Number (PAN) ☐ Expiration Date ☐ Full Track 1 and/or 2 ☐ PIN ☐ CVV2 Cardholder personally-identifiable information (PII) ☐ Cardholder Name ☐ Social Security Number ☐ Date of Birth ☐ Other:
Has the compromise been contained? If yes, how?	☐ Yes ☐ No If yes, how?

Steps and Requirements for Visa Members

The *Visa Core Rules and Product and Service Rules* (Visa Rules) and this *What To Do If Compromised* document require Visa Members to conduct a thorough investigation of suspected or confirmed loss, theft, or compromise of Visa account or cardholder information involving either their own network environment or that of their merchant(s) or agent(s).

The Visa Rules contain enforcement mechanisms that Visa may use for violations of the Visa Rules. The Visa Rules specify the procedures for the investigation of violations and the rules and schedules for non-compliance assessments.

The Visa Rules are available on Visa.com.

Notification

1. Immediately report to the Visa Risk Management group any suspected or confirmed unauthorized access to any Visa cardholder data.
2. Within 48 hours, provide Visa with status of compliance with PCI DSS and, if applicable, PCI Payment Application Data Security Standard (PA-DSS) and PCI PIN Security requirements at the time of the incident.

Initial Investigation (within 3 business days)

3. Members must perform an initial investigation and provide the Visa Initial Investigations Report, documenting findings or conclusions to Visa within three (3) business days. The information will help Visa understand potential exposure and assist in containing the incident. Documentation must include any steps taken to contain the incident.

Independent Forensic Investigation

4. Visa may, at its discretion, require a compromised entity to conduct an independent forensic investigation for any case of suspected cardholder data exposure. The investigation must be performed by a Payment Card Industry Forensic Investigator (PFI). The following factors, among others, may lead Visa to require the compromised entity to conduct a PFI investigation:
    - Fraud loss tied to Common Point of Purchase (CPP) reports
    - Self-reported data security breach affecting payment cards
    - Number of sources reporting entity as potentially compromised
    - Law enforcement or other credible source reports of a data security breach affecting payment cards
    - An entity that has not contained the initial or previous incident (this may be determined through additional CPP reports, data analysis, or other means).
    - Service Provider, Agent, Integrator, Reseller, etc., with remote access to multiple locations

5. A Visa Member or compromised entity must engage a PFI to perform a forensic investigation. Visa will NOT accept forensic reports from non-approved forensic companies. It is the Visa Member's responsibility to ensure its merchant or agent engages a PFI to perform a PFI forensic investigation.
6. Visa has the right to directly engage a PFI to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the appropriate Visa Member. Investigative costs may be in addition to any applicable non-compliance assessments by Visa.
7. Upon discovery of an account data compromise, or receipt of an independent forensic investigation notification from Visa, a Member must:
   - Ensure that the PFI is engaged (or the contract is signed) within five (5) business days
   - Ensure initial work is underway and provide the initial forensic (i.e., preliminary) report to Visa within ten (10) business days from when the PFI is engaged (or the contract is signed)
   - Provide a final forensic report to Visa within ten (10) business days of completion of the review
8. PFI's must release all forensic investigations reports and findings to Visa.
9. Note: Visa has the right to reject a PFI report if it does not meet the PFI requirements established in the PFI Program Guide. PFIs are required to address with Visa, the acquirer, and the compromised entity any discrepancies before finalizing the report.
10. For more information on forensic investigation guidelines, please refer to the PCI Forensic Investigator (PFI) Program Guide, located in the PCI SSC document library: www.pcisecuritystandards.org/document_library (Filter by: PFI)
11. List of approved PCI Forensic Investigators: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
12. If there is a suspected PIN compromise, the PFI must perform a PIN security and key management investigation and a PCI PIN security assessment.
13. Note: If the PFI engagement is not done according to the requirements stipulated above, it will be deemed a violation of the Visa Rules and this document and non-compliance assessments may be levied.

Exposed Account Data

14. Provide All Exposed Accounts – All compromised Visa accounts (known or suspected) must be uploaded to Visa's Compromised Account Management System (CAMS) within five (5) business days from the first to occur of the following events: (a) the date Visa requests account numbers, (b) a Window of Exposure (WOE) is determined, or (c) discovery of compromised account data is identified.

    For assistance or access, contact Visa at: CAMS@Visa.com

    All parties that upload at risk accounts, must include:

    - Entity name
    - Window of Exposure

- Data elements at risk (e.g. Primary Account Number (PAN), Track 1 and / or Track 2, CVV2, PIN, Expiration Date, etc.)
- Bank Identification Number (BIN) (if applicable)
- Merchant Category Code (MCC) (if applicable)
- Law Enforcement Investigator Name and Incident Number (if applicable)
- Investigator name (if applicable)
- Incident number (if applicable)

PCI DSS Compliance

15. Compromised entities must achieve full PCI compliance by validating to the PCI DSS, PCI PA-DSS and, if applicable, PCI PIN Security Requirements Compliance validation per the Visa Rules.

    Note: In the event a compromised entity had a PCI DSS audit performed by a QSA and subsequently suffered an account data compromise, Visa will require that the entity engage a different QSA to perform the ensuing PCI DSS audit required after all remediation items have been completed.

    Please visit www.pcisecuritystandards.org for more information on PCI DSS and the PCI PIN Entry Device Testing Program.

    For more information on PCI PIN Security Requirements, please visit www.visa.com/pinsecurity.

Appendix: Quick Lookup by Topic

Compromised Entity

Evidence	See Preserve Evidence, page 2
Investigations	See Provide Visa Initial Investigation Report, page 2 and Perform Forensic Investigation, page 3
Upload Exposed Accounts	See Provide Exposed Accounts, page 3
PCI DSS	See PCI DSS Compliance, page 10

Visa Member

Visa Rules	See Steps and Requirements, page 8
Notification	See Notification, page 8
Investigations	See Initial Investigation & Independent Forensic Investigation, page 8
Provide Exposed Accounts	See Exposed Account Data, page 9
PCI DSS	See PCI DSS Compliance, page 10