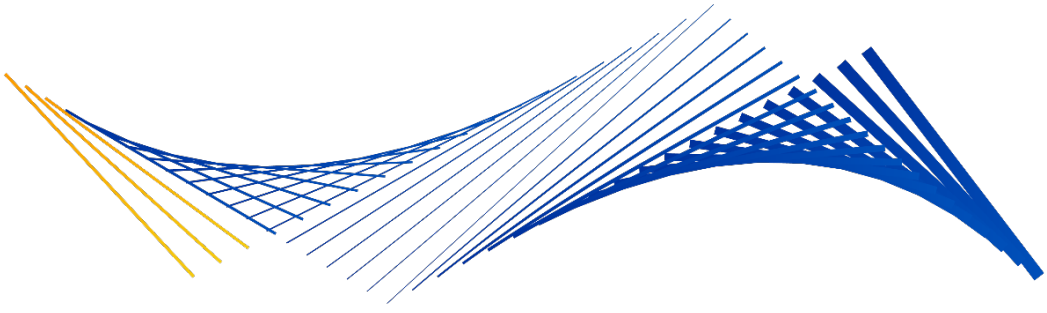
What To Do If Compromised

Visa Supplemental Requirements

Version 8.0

Effective: October 14, 2023



About Visa Supplemental Requirements

This document is a supplement of the *Visa Core Rules and 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 Visa Product and Service Rules*, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

Contents

Summary

Visa is dedicated to promoting the safe and sound long-term prosperity of the Visa payment ecosystem. To that end, Visa aims to ensure the timely resolution of external data compromise events, drive notification of at-risk accounts to stem fraud impacts, and synthesize forensic evidence, intelligence, and fraud analysis to formulate remediation plans that strengthen payment system security.

Protecting the payment ecosystem is a shared responsibility. Any entity that stores, processes, or transmits payment card data or has access to those systems or data, is required to adhere to and maintain compliance with all Payment Card Industry Data Security Standard (PCI DSS) requirements and (PCI) – PIN Security Requirements.

Visa's *What to Do if Compromised* (WTDIC) document is a requirements-based guide that applies to entities that suspect or have experienced an event that leverages, impacts, or compromises their payment systems, or payment systems they service or support. This includes, but is not limited to, all Visa Members (e.g., Issuers, Acquirers), Merchants, Processors, Gateways, Agents, Service Providers, Third-Party Vendors, Integrator Resellers, Fin Techs, Blockchain / Crypto or Digital Currency participants, and any other entities that operate or access a payments environment. This document reflects the risks of current and future threats to the payment ecosystem and is designed to provide guidance on each parties' obligations throughout a suspected or confirmed payment environment incident ("Compromise Event").

WTDIC establishes procedures and timelines for reporting and responding to a Compromise Event. To mitigate payment system risk during a Compromise Event, prompt action is required to prevent additional exposure, including ensuring containment actions and remediation such as the existence and proper functioning of PCI DSS and PCI PIN Security controls.

Section A: Requirements for Entities that Suspect or Have Confirmed a Compromise Event

Any entity that suspects or confirms unauthorized access to and/or misuse of any Visa cardholder data, including any entity that stores, processes, or transmits cardholder data or has access to a payments environment or systems, is required to adhere to the WTDIC requirements.

This includes, but is not limited to Merchants, Processors, Gateways, Agents, Service Providers, Third-Party Vendors, Integrator Resellers, FinTechs, Blockchain / Crypto or Digital Currency participants, and any other entities operating or accessing a payments environment.

> *Entities are required to report compromise events that involve payment systems or data. Visa requires an incident report for any suspected or confirmed Compromise Event that involves the potential or actual unauthorized access to payment system or data of any Visa payment ecosystem participant. If the entity is unsure whether a Compromise Event impacts payment systems or data, they should still report it to Visa using the regional contact information found in table 1.1 (below) and Visa will provide guidance on next steps.*

1. Submit Notification to Visa Within Three (3) Calendar Days

1.1. An entity that suspects or confirms unauthorized access to any Visa payment account data, or to any payment system that stores, processes, or transmits Visa payment account data, is required to ensure that the Compromise Event is reported to Visa's Global Risk Investigations group within three (3) calendar days of either:

a. The discovery of evidence sufficient to raise a reasonable suspicion of a Compromise Event, or
b. The discovery of evidence sufficient to confirm the existence of a Compromise Event.

Visa Members are responsible for ensuring compliance with this requirement by their affiliates, agents, and customers.

1.2 Visa Acquirers and Third-Party Processors with access to Visa's Global Investigation Management Tool (GIMT) must provide notice via GIMT.

Visa's Global Investigations Management Tool (GIMT) is an end-to-end case management solution that serves as the central repository for receiving and distributing investigation information for Compromise Events and other fraud schemes. Acquirers and their designated Third-Party Processors (TPPs) are required to use GIMT when managing or creating Visa cases. For additional details, please refer to *Visa's GIMT Acquirer User Guide* on Visa Online or in the Resources section within GIMT.

1.3 All other notifications must be provided to the appropriate regional Visa Global Risk Investigations group listed in table 1.1 (below).

Regional Contact Information - Table 1.1

Asia Pacific (AP)	APFraud@visa.com
Central and Eastern Europe, Middle East and Africa (CEMEA)	CEMEAFraudControl@Visa.com
Latin America & Caribbean (LAC)	LACFraudInvestigations@visa.com
North America (NA)	USFraudControl@visa.com
Europe (EU)	DataCompromise@visa.com
Risk Operations Center 24/7 Emergency Assistance	Toll Free: 1-844-847-2106 International 1-650-432-3379 ROC@Visa.com

2 Perform Initial Investigation and Provide Incident Report

2.1 Within three (3) calendar days of notifying Visa in accordance with Section A-1 (above), provide a report describing the event (the "Incident Report") to Visa and the Acquiring bank (if applicable). Please refer to Attachment A at the end of the document for an editable copy of the Incident Report. Entities should also provide supporting Payment Card Industry Data Security Standards (PCI DSS) compliance documentation when available or requested.

2.2 The information provided in the Incident Report aids Visa in understanding the compromised entity's network environment, potential scope of the incident, potential payment card data at risk, estimated financial exposure where known, and containment status of the Compromise Event. Documentation must include any steps taken to contain and remediate the Compromise Event, including the dates of the containment or remediation steps. For more guidance on the minimum criteria to meet the Incident Report requirement, please see Section B-1.

2.3 Visa Acquirers and Third-Party Processors with access to Visa's Global Investigation Management Tool (GIMT) must provide notice and relevant or requested documentation via GIMT.

All other Incident Reports must be provided to the appropriate regional Visa Global Risk Investigations group listed in Section A, Table 1.1.

3. Provide Notice to Other Relevant Parties

3.1. Immediately notify all relevant parties, including but not limited to the Issuing/Acquiring Bank (if applicable).

3.2. If the name and/or contact information for your Acquiring Bank is unknown, contact the appropriate regional Visa Global Risk Investigations group listed in Section A, Table 1.1.

3.3. It is strongly recommended that you also immediately notify:

3.3.1. Your internal incident response team and information security group.

3.3.2. Your PIN Entry Device (PED) manufacturer, your Point-of-Sale (POS) manufacturer or POS reseller/integrator, or shopping cart manufacturer if it is determined the incident involves a vulnerability in your payment processing system. Vendors of applications certified under the PCI SSC's Software Security Framework are required to notify the SSC of any application vulnerabilities.

3.3.3. Your legal department, particularly if applicable law mandates customer notification.

3.3.4. The appropriate local or national law enforcement agencies.

The United States Secret Service Electronic Crimes Task Forces (ECTF) if the Compromise Event is in the United States. The ECTF focuses on investigating financial crimes and can assist with incident response and mitigation of a Compromise Event.

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

4. Provide At-Risk Payment Account Data to Visa

4.1 Entities are required to ensure that all compromised Visa account numbers (known or suspected) are provided to Visa's Global Risk Investigations group via Visa's Global Investigation Management Tool (GIMT) or Compromised Account Management System (CAMS) within three (3) calendar days of any of the following scenarios:

a. Discovery of compromised account data.

b. The date Visa requests at-risk account numbers; or

c. A Window of Exposure (WOE) is determined.

4.1.1. Entities must work with their Acquirer of Record or Third-Party Processor to upload accounts to GIMT or CAMS, if applicable.

4.1.2. For more information or assistance, contact the appropriate regional Visa Global Risk Investigations group listed in Section A, Table 1.1.

5. Conduct PCI Forensic Investigation (PFI)

5.1. Visa may, at its discretion, require a potentially compromised entity to engage a Payment Card Industry (PCI) Forensic Investigator (PFI) to perform an investigation. Should Visa require an investigation by a PFI, Members or responsible parties will receive formal notification from Visa via the Global Investigations Management Tool (GIMT) or appropriate email channel. As outlined in the formal notification, the investigation must be performed by a PFI, and the following is required:

5.1.1. Within five (5) business days, execute a contract retaining a PFI to perform a PCI forensic investigation and inform Visa of the PFI company and lead investigator. If applicable, the entity shall also inform the Acquiring Bank that it has retained a PFI and include the name of the PFI company and lead investigator.

5.1.2. Provide thorough logistical and technical support to the PFI to facilitate timely completion of the investigation, including, but not limited to, providing access to system logs, images, and requested documentation, regular status updates, participation in all party conference calls, furnishing malware samples and Indicators of Compromise (IOCs), etc.

5.1.3. Within five (5) business days from when the entity has retained a PFI and signed a contract, provide Visa with the initial forensic (i.e., preliminary) report.

5.1.4. Within ten (10) business days of completion of the PFI investigation, provide Visa and its affected Acquirers with a final forensic report.

5.2. In addition to Members, certain circumstances involving non-Member entities which includes but is not limited to Level 1 and Level 2 Merchants, Processors, Gateways, Agents, Service Providers, Third-Party vendors, Integrator Resellers as well as other payment system participants operating or remotely accessing a payments environment, present an increased risk exposure to the payments ecosystem and are more likely to be required to retain a PFI for a PCI forensic investigation.

5.3. 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, within the past 3 years.

5.4. Visa will review, but not recognize forensic reports from a non-approved PFI company when a PFI is required.

5.5. Per the PCI PFI program rules, PFIs are required to provide forensic reports and investigative findings directly to Visa.

5.6. Visa reserves the right to reject PFI reports that do not satisfy the WTDIC requirements and to require a new PFI investigation by a different PFI company. A new PFI investigation will be at the expense of the entity and not at the expense of Visa.

A list of approved PFI organizations is available at:

www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

6. Conduct Independent Investigation

6.1. Not all Compromise Events necessitate a PFI. Visa may require the entity to conduct an Independent Investigation in lieu of, or prior to, a PCI forensic investigation. Should Visa require an Independent Investigation, Members or responsible parties will receive formal notification from Visa via the Global Investigations Management Tool (GIMT) or appropriate email channel. If advised that an Independent Investigation is required, an entity is required to do the following:

6.1.1. Within five (5) business days, execute a contract retaining an appropriately qualified investigator to perform the Independent Investigation (see 6.1.2.), and inform Visa of the Investigation company and lead investigator.

6.1.2. The Visa Member may use whatever resources they deem appropriate to contain an incident but must ensure that containment actions are validated by a competent and appropriately qualified individual or company. For example, a qualified company could be a PFI doing work in a non-PFI capacity or a company that can demonstrate a comprehensive understanding of current PCI DSS and strong methodology for discovery, containment, and remediation of a Compromise Event.

6.1.3. The company and investigator should not be a previously used security firm who was unable to identify or contain the Compromise Event or preformed previous QSA work or services within the past 3 years. Failure to contain the Compromise Event within sixty (60) business days may result in Visa requiring a PFI investigation of the entity and or non-compliance assessments.

6.1.4. Independent Investigators must be made available in a timely manner to address any outstanding or clarifying questions posed by Visa and are required to provide Independent Investigation reports and other investigative findings directly to Visa. The final report should detail at a minimum:

- The entity that validated containment, including their contact details.
- Key findings of the investigation.
- Window of exposure and data elements at risk.
- Actions taken to contain the breach.
- Any outstanding remediation actions to be taken under the supervision of the acquirer and the anticipated date for completion.

6.2. Visa reserves the right to reject Independent Investigation reports that do not satisfy the WTDIC requirements Section A-6 (above) and to require a PFI investigation if the WTDIC requirements are not fulfilled.

7. Preserve Evidence

7.1. To identify the root cause of a potential Compromise Event, facilitate investigations, and ensure the integrity of the system components and environment, it is critical to preserve all evidence.

Visa strongly recommends the following:

7.1.1. 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). The compromised system(s) should be disconnected from the internet immediately and not be used to process payments or interface with payment processing systems.

7.1.2. 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.

7.1.3. Identify and document all suspected compromised components (e.g., PCs, servers, terminals, logs, security events, databases, PED overlays etc.).

7.1.4. Document containment and remediation actions taken, including dates/times (preferably in UTC), individuals involved, and detailed actions performed.

7.1.5. Preserve and retain all evidence (including physical servers or devices) and logs (e.g., original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).

7.1.6. If using third-party service providers like hosting companies or cloud providers, request logs and system images to be retained and provided to the PFI or external security firm assisting in the investigation.

7.1.7. Preserving evidence in cloud computing environments carries its own specific challenges related to digital forensics. For More guidance visit the PCI SSC Cloud Guidelines: PCI SSC Cloud Guidelines.

Section B: Requirements for Visa Members

The *Visa Core Rules and Product and Service Rules* (Visa Rules available on Visa Online) and this *What To Do If Compromised* document requires all Visa Members (e.g., Issuers, Acquirers) 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 Merchants, Processors, Gateways, Agents, Service Providers, Third-Party Vendors, Integrator Resellers, FinTechs, Blockchain / Crypto or Digital Currency participants, and any other entities operating or accessing a payments environment on behalf of the Visa Member.

1 Submit Notification to Visa

1.1 Within three (3) calendar days, report to the Visa Global Risk Investigations group any suspected or confirmed unauthorized access to any Visa cardholder data or systems.

1.2 Visa Acquirers and Third-Party Processors with access to Visa's Global Investigation Management Tool (GIMT) must provide notice and relevant or requested documentation via GIMT.

Visa's Global Investigations Management Tool (GIMT) is an end-to-end case management solution that serves as the central repository for receiving and distributing investigation information for Compromise Events and other fraud schemes. Acquirers and their designated Third-Party Processors (TPPs) are required to use GIMT when managing Visa cases. For additional details, please refer to *Visa's GIMT Acquirer User Guide* on Visa Online or in the Resources section within GIMT.

1.3 All other notifications must be provided to the appropriate regional Visa Global Risk Investigations group listed in Section A, Table 1.1.

2. Perform Initial Investigation and Provide Incident Report

2.1. Within three (3) calendar days of notification of a suspected or confirmed Compromise Event, provide the Incident Report to Visa. Please refer to Attachment A at the end of the document for an editable copy of the Incident Report. Visa Members are required to perform an initial investigation and submit an Incident Report via Visa's Global Investigation Management Tool (GIMT), as detailed in Section B-1.2.

Visa Acquirers and Third-Party Processors with access to Visa's Global Investigation Management Tool (GIMT) must provide notice and relevant or requested documentation via GIMT.

All other Incident Reports and information must be provided to the appropriate regional Visa Global Risk Investigations group listed in Section A, table 1.1.

2.2. A Member of Record (e.g., Issuer, Acquirer) is responsible for engaging and managing its Merchants, Processors, Gateways, Agents, Service Providers, Third-Party vendors, Integrator Resellers, and any other entities, operating or accessing a payments environment on its behalf to investigate and fully address any potential Compromise Event. Unless otherwise disclosed to a Member of Record, all formal communications from Visa regarding a potential Compromise Event will be to the Acquirer or Issuer of record.

2.3. Within three (3) calendar days of notification of a Compromise Event, provide Visa with status of compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements and (PCI) – PIN Security Requirements at the time of the incident, if applicable.

2.4. The information provided in the Incident Report aids Visa in understanding the compromised entity's network environment, potential scope of the incident, potential data at risk, and in containing the Compromise Event. Documentation must include any steps taken to contain and remediate the account data Compromise Event.

2.5. A preliminary independent investigation report is not the same as a PFI preliminary report. Information regarding a PFI preliminary report is explained in Section B-4.3.2.

3. Provide At-Risk Payment Account Data

3.1. Visa Members (e.g., Issuers, Acquirers) are required to ensure that all compromised Visa account numbers (known or suspected) are provided to Visa's Global Risk Investigations group via Visa's Global Investigation Management Tool (GIMT) or Compromised Account Management System (CAMS), within three (3) calendar days of any of the following scenarios:

a. Discovery of compromised account data.

b. The date Visa requests at-risk account numbers; or

c. A Window of Exposure (WOE) is determined.

3.2. The known or suspected compromised account data must be based on authorization transaction records or other at-risk payment data (e.g., stored PAN's) and delineated by Point-of-Sale (POS) entry mode, where applicable (i.e., POS 90, POS 05, POS 01, etc.) and uploaded by separate files.

3.3. Members and their clients that upload at-risk accounts to CAMS are required to include the following information:

- 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.)
- Acquiring Identifier, Issuing Identifier, or VSS Processor (if applicable)
- Merchant Category Code (MCC) (if applicable)
- Investigator Name
- Incident Number (if applicable)

3.4. Members and their clients that upload at-risk accounts to GIMT are required to include the following information. All other information will be pre-populated by GIMT.

- Window of Exposure
- Data Elements At-Risk (e.g., Primary Account Number (PAN), Track 1 and / or Track 2, CVV2, PIN, Expiration Date, etc.)

3.5. All files are required to meet the following criteria:

- Files are required to be in plain text.
- Files cannot exceed 100 MB in size.
- Uploaded file must contain 11–19 digit account numbers only (one per row).

3.6. If Expiration date is applicable:

- Checkbox for the Expiration is required.
- Format of the date is required to be in YYMM.

For additional details, please refer to *Visa's GIMT Acquirer's Guide* available on Visa Online or in the Resources section within GIMT. The CAMS User Guide is also available on Visa Online.

4. Manage PCI Forensic Investigation (PFI)

4.1. Visa may, at its discretion, require a potentially compromised entity to conduct a PCI Forensic Investigation. Should Visa require a PFI, Members or responsible parties will receive formal notification from Visa via the Global investigations Management Tool (GIMT) or via the appropriate email channel. As outlined in the formal notification, the investigation is required to be performed by a PFI and the following is required:

4.2. Circumstances involving high-risk entities which includes but is not limited to Level 1 and Level 2 Merchants, Processors, Gateways, Agents, Service Providers, Third-Party vendors, Integrator Resellers as well as other payment system participants operating or remotely accessing a payments environment present a higher inherent risk to the payment ecosystem and may be required to retain a PFI for a PCI forensic investigation. In addition to high-risk entities, the following factors, among others, may lead Visa to require an entity to conduct a PFI investigation:

4.2.1. Fraud loss tied to Common Point of Purchase (CPP) reports.

4.2.2. Self-reported data Compromise Event potentially affecting payment credentials.

4.2.3. Sources, including law enforcement, reporting entity as potentially compromised.

4.2.4. Malicious and nefarious connections to payment system or platforms, including but not limited to Processor gateways, clearing and settlement systems, etc.

4.2.5. Failure to contain the initial Compromise Event or a previous Compromise Event (this may be determined through additional CPP reports, data analysis, or other means).

4.3. If advised that a PFI investigation is required, a Member is required to engage with its Merchants, Processors, Gateways, Agents, Service Providers, Third-Party vendors, Integrator Resellers, and any other entities, operating or accessing a payments environment to investigate and fully address any potential Compromise Event.

4.3.1. Within five (5) business days, ensure that a contract retaining a PFI to perform the PCI forensic investigation has been executed, and inform Visa of the PFI company and lead investigator.

4.3.2. Within five (5) business days from when the entity has retained a PFI and signed a contract, provide Visa with the initial forensic (i.e., preliminary) report.

4.3.3. Within ten (10) business days of completion of the PFI investigation, provide Visa and its affected Acquirers the final forensic report.

4.3.4. Provide thorough logistical and technical support to the PFI to facilitate timely completion of the investigation, including, but not limited to, regular status updates, participation in all party conference calls, furnishing malware samples and Indicators of Compromise (IOCs), etc.

4.3.5. The PFI company cannot be an organization that is affiliated with the compromised entity or has provided services to the compromised entity such as previous PFI investigation(s), Qualified Security Assessor (QSA), advisor, consultant, monitoring or network security support, etc., within the past 3 years.

4.3.6. Visa will review, but not recognize forensic reports from a non-approved PFI company when a PFI is required.

4.3.7. Per PCI PFI Program Rules, PFI's are required to release all PCI forensic investigation reports and findings directly to Visa. PFIs are required to address with Visa, the Member, and the compromised entity any discrepancies or outstanding issues prior to finalizing the report. Visa reserves the right to reject a PFI report if it does not meet the PFI requirements established in the PFI Program Guide or if it does not satisfy the WTDIC requirements. Failure to satisfy the PFI investigation requirements specified above may result in non-compliance assessments.

4.3.8. Visa reserves the right to require additional PFI investigations and/or directly retain a PFI to perform additional PFI investigations, if, in its sole discretion, it determines that the WTDIC requirements have not been satisfied. Any additional PFI investigations will be at the expense of the Member. Such expenses are in addition to any non-compliance assessments.

4.4. For more information on PCI 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)

List of approved PCI Forensic Investigators:

https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

4.5. Subsequent to the investigation, all compromised entities including but not limited to, all Visa Members (e.g., Issuers, Acquirers), Merchants, Processors, Gateways, Agents, Service Providers, Third-Party Vendors, Integrator Resellers and any other entities etc., as well as other payment system participants operating or accessing a payments environment, etc. are required to achieve the following: PCI DSS compliance and, if applicable, PCI PIN Security Requirements compliance validation per the *Visa Rules*.

Please visit www.pcisecuritystandards.org for more information on PCI DSS and the PCI PIN requirements.

5. Manage Independent Investigation

5.1. Not all Compromise Events necessitate a PFI. Visa may require a potentially compromised entity to conduct an Independent Investigation in lieu of, or prior to, a PCI led forensic investigation. Should Visa require an Independent Investigation, Members or responsible parties will receive formal notification from Visa via the Global Investigations Management Tool (GIMT) or appropriate email channel. If advised that an Independent Investigation is required, a Member is required to do the following:

5.1.1. Within five (5) business days, execute a contract retaining an appropriately qualified investigator to perform the Independent Investigation (see 5.1.2.), and inform Visa of the investigation company and lead investigator.

5.1.2. The Visa Member may use whatever resources they deem appropriate to contain the incident but must ensure that containment actions are validated by a competent and appropriately qualified individual or company. For example, a qualified company could be a PFI doing work in a non-PFI capacity or company that can demonstrate a comprehensive understanding of current PCI DSS and strong methodology for discovery, containment, and remediation of a Compromise Event.

5.1.3. Provide complete logistical and technical support to the Independent Investigator to facilitate timely completion of the investigation, including but not limited to regular status updates, participation in all party conference calls, furnishing malware samples and Indicators of Compromise (IOC's), etc.

5.1.4. The company and specific investigator should not be with a previously used security firm who was unable to identify or contain the Compromise Event or preformed previous QSA work or services within the past 3 years. Failure to contain the Compromise Event within sixty (60) business days may result in Visa requiring a PFI investigation of the entity and or non-compliance assessments.

5.1.5. Independent investigators must be made available in a timely manner to address any outstanding or clarifying questions posed by Visa, and independent investigators are required to provide Independent Investigation reports and other investigative findings directly to Visa. The final report should detail at a minimum:

- The entity that validated containment, including their contact details.
- Key findings of the investigation.
- Window of exposure and data elements at risk.
- Actions taken to contain the breach.
- Any outstanding remediation actions to be taken under the supervision of the acquirer and the anticipated date for completion.

5.2. Visa reserves the right to reject Independent Investigation reports that do not satisfy the WTDIC requirements Section B-5 and to require a PFI investigation if the WTDIC requirements are not fulfilled.

6. Requirements for a Suspected or Confirmed Compromise Event of Visa Members

6.1. Visa has observed an increase in attacks against Member financial institutions. Any Member that suspects or confirms unauthorized access to any Visa cardholder data, including those payment systems that store, process, or transmit cardholder data, must comply with this Section B-6.

6.1.1. Visa may require a Member to conduct a PFI investigation and provide the same deliverables described in Section B-4.

6.1.2. Not all instances necessitate a PFI. Visa may require the following in lieu of or prior to a PCI forensic investigation. These actions are required within three (3) calendar days:

- If Visa notifies the Member of malicious Internet Protocols (IPs) connections, the Member is required to confirm a firewall block is in place for outbound connections.
- The Member is required to check network logs for which machines connected to malicious IP addresses and provide access to logs, if requested.
- The Member is required to scan their network for suspicious activity and perform additional investigation on any machines observed communicating with malicious IPs. Visa may request IOCs e.g., malicious files, including malware samples to support the investigation.
- The Member is required to document above actions and provide an Incident Report to Visa.
- The Member is required to monitor and report any suspicious or fraudulent activity on any other payment systems the Member operates including but not limited to; SWIFT, ACH, B2B, and P2P services during the investigation.

Visa strongly recommends that an independent third-party validate the security of the Member's network. In certain cases, Visa may require third-party validation to confirm the Member's network is secure.

Section B1: Requirements for Members: Fraud Scheme Cases

7. Managing Payment Ecosystem Attacks and Fraud Scheme Cases

Visa has observed an increase in attacks that impact participants in the Visa payments ecosystem. These attacks can include, but are not limited to Ransomware Events, Supply Chain Attacks, Brute Force Attacks, Credential Take Over, Credential Stuffing, Merchant and Cardholder Collusion, Force Posting, Fraudulent Purchase Return (aka Credit Vouchers), Fraudulent Purchase Return Authorization or any other nefarious activity against or leveraging participants in the Visa Payment ecosystem.

Entities are not required to report compromise events that do not involve payment systems or data. However, for any suspected or confirmed event that could include a payment system or data of a Visa payment ecosystem participant, or potential access to payment card data, Visa does require an Incident Report. Visa may, at its discretion, require a PCI PFI or third-party Independent Investigation. If Visa becomes aware of a Compromise Event impacting a payment ecosystem participant, the entity is required to validate to Visa that the event did not impact their payment systems or place any cardholder data at risk. Even if the participant's payment systems, data, or services are not impacted, third-party independent validation may still be warranted.

The Incident Report should include a timeline of events which include but are not limited to a description of the event, root cause, what data was put at risk and when, as well as containment and remediation actions taken. The report should be thorough and clear enough that someone unfamiliar with the incident could read it and obtain a reasonable understanding of what happened and how it was resolved. At a minimum, the Incident Report must completely document the event by including at least the following information:

- Date when entity was first notified, or the activity was identified.
- How the event was identified and by whom.
- Root cause
- Contact information and titles of those involved with the incident response.
- When Visa was first notified.
- Any other parties notified, such as your Acquirer, third-party processor, law enforcement, government, and when they were notified.
- Whether a third-party incident response or forensic firm has been retained to assist with the investigation and, if so, the name of the firm and contact info.
- Whether the incident has been contained and if so, how. If ongoing, any actions that have been or are being taken to contain the event and what the expected timeframe to complete containment is.
- If contained, when the event was contained.
- The duration of the event.

- Any and all systems accessed or impacted (e.g., Corporate, Development Environment, Production Environment, Email, Payment Terminals, POS System(s), Webpage, Checkout Page, Call Center, Online Banking, Wallet, Payment Processing, Token Solution(s) Customer Service, Loyalty, Rewards, Third-Party Services, Hosting Environment, Cloud Environment, API, Plug In, Other, etc.).
- The types of data that was impacted (e.g., Intellectual Property, PII, Customer Records, Payment Data, etc.).
- If payment systems are impacted, a list of all entities and components affected (e.g., POS Terminal, POS System, Checkout Page, Back End Database, Token Solution / Provider Hosting Solution / Provider, Cloud Solution / Provider, API, Plug-in, Third-Party Service Provider, User Accounts Leveraged, Remote Solutions leveraged, etc.).
- If payment data is impacted, identification of all specific elements potentially put at risk (e.g., PAN, Token, Expiration Date, CVV, Cardholder Name, Cardholder Address, Cardholder Email, etc.).
- If there is payment data at risk, the transaction dates applicable to any at-risk data (e.g., range from oldest known impacted transaction to most recent known impacted transaction).
- Whether there was any interruption in business operations or payment processing. If yes, please provide all details of the impact and duration of the interruption including customer impact. If it is ongoing, please provide details on what is being done to address the interruption and timeframe by which normal business operations will resume.
- Any steps taken to resume normal business operations.
- Any additional steps being taken to remediate the event.
- If funds moved or fraud occurred, any actions taken to address recoveries. If recovery is not possible, please state why and provide losses (including averted losses) associated with the event.
- All known bad IP addresses.
- Any malware samples.
- Law Enforcement agency and contact info (if appropriate).

All information provided to Visa is Confidential and only available to approved Visa Staff, but it may be anonymized for security alerts.

Any failure to meet these requirements may be considered a violation of the rules and be subject to non-compliance assessments as outlined in Section B2-9.

Section B2: Investigation Fees and Non- Compliance Assessments for Members

8. Investigation Fees

(Effective: April 1, 2024, in the EU Region)
(Effective: as of 2020 in the AP Region, CEMEA Region, LAC Region, US Region, and Canada Region)

Visa is dedicated to promoting the safe and sound long-term prosperity of the Visa payment ecosystem and continues to make significant investments in payments technology to protect the payment ecosystem. To that end, Visa aims to ensure the timely resolution of Compromise Events, and drive notification of at-risk accounts to stem fraud impacts. In support of these objectives, Visa has developed Investigation Fees to incentivize entities to fully cooperate with Visa throughout each phase of the investigation lifecycle and to complete the investigation in a timely manner. Full cooperation during an investigation helps to quickly contain and mitigate a Compromise Event and minimize the resulting fraud impacting Visa clients.

PFI-led investigations may be subject to applicable fees. If a PCI forensic investigation is not completed within four (4) full calendar months from the date Visa provided notice of the requirement for a PFI, Visa may impose fees as follows:

8.1. A flat fee in the amount of USD 3,000 for investigations involving Level 3 and 4 merchant investigations, or

8.2. A recurring monthly fee in the amount of USD 10,000 for investigations involving Level 1 and 2 Merchants, VisaNet Processors, Members and Agent investigations until the investigation is properly completed.

The 4-month period begins on the 1st of the next month following the Member's receipt of notification from Visa that a PCI forensic investigation is required. Partial months are not included in the 4-month fee-free period or for the calculation of the fees.

The fee will be invoiced after the fifth (5^{th}) full calendar month of an open investigation.

Entity Type	Number of Annual Transactions	Investigation Duration Grace Period	Investigation Duration Fee Period	Investigation Fee
Issuers	N/A	Four full calendar months (partial months are not included)	Monthly fee starts with the fifth full calendar month and continues through every complete calendar month until investigation is complete	USD $10,000 per month
Acquirers	N/A			
VisaNet Processor	N/A			
Level 1—Merchants	> 6,000,000			
Level 1—Agents for Issuers or Acquirers	> 300,000			
Level 2—Merchants	1,000,001–6,000,000			
Level 2—Agents for Issuers or Acquirers	< 300,000			
Level 3—E-commerce Merchants	20,000-1,000,000	Four full calendar months (partial months are not included)	One-time fee effective the fifth full month	USD $3,000 flat fee
Level 4—Merchants	1-1,000,000			

9. Non-Compliance Assessments

A Member is subject to a non-compliance assessment of up to USD 100,000 per incident for failing to adhere to any of the below requirements:

- Within three (3) calendar days, report to the Visa Global Risk Investigations group any suspected or confirmed unauthorized access to any Visa cardholder data or payment system.
- Provide Visa with status of compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements and (PCI) – PIN Security Requirements within three (3) calendar days of the incident.
- Within three (3) calendar days from identification, Members are required to perform an initial investigation and provide to Visa the Incident Report documenting findings or conclusions. Continual investigation updates must be provided to Visa as additional information is obtained by the entity or requested by Visa related to the investigation.
- Within three (3) calendar days of any of the following scenarios: (a) discovery of compromised account data; (b) the date Visa requests account numbers; or (c) a Window of Exposure (WOE) is determined, Visa Members (e.g., Issuers, Acquirers) are required to ensure that all compromised Visa account numbers (known or suspected) are provided to Visa's Global Risk Investigations group via Visa's Global Investigation Management Tool (GIMT) or Compromised Account Management System (CAMS).
- Retain an approved PCI Forensic Investigator (PFI) within five (5) business days of notification of a suspected or confirmed Compromise Event, if requested by Visa.
- Within five (5) business days, ensure that a contract retaining a PFI to perform the PCI forensic investigation has been executed, and inform Visa of the PFI company and lead investigator as described in Section B4.3.1

- Within five (5) business days of executing the PFI contract, provide the initial forensic (i.e.,preliminary) report to Visa.
- Within ten (10) business days of completion of the PFI investigation, provide the final forensic report to Visa.
- Provide complete logistical and technical support to the PFI to facilitate timely completion of the investigation.
- Retain an Independent Investigator within five (5) business days of notification of a suspected or confirmed Compromise Event, if requested by Visa, as described in Section B-5.1.1.
- Within five (5) business days, ensure that a contract retaining an investigator to perform the Independent Investigation has been executed, and inform Visa of the company and lead investigator, as described in Section B- 5.1.
- Within ten (10) business days of completion of the investigation, provide Visa with the final report.
- Provide complete logistical and technical support to the Independent Investigator to facilitate timely completion of the investigation.

Attachment A: Incident Report

Visa Incident Report Page 1				
Legal Entity Name:				
DBA Entity Name:				
Type of Entity: *(e.g., Visa Member, Processor, Merchant, Agent, Service Provider, Resellers etc.)*				
List any direct processing relationships with Visa: *(e.g., VNP, Visa Direct, DPS, CyberSource)*				
Services, Solutions, or Product Provided by Entity:				
Entity Address:	City:	State / Province:	Postal / Zip code:	Country:
Primary Contact Name:	Phone:		Email:	

All Information Below to be Completed By Entity / Incident Response Team
Detailed Description of the Incident (what, how, who, when, and where): Note: If the incident involves multiple locations / entities, provide a list of the names, address, Merchant Banks, and Processors of the merchants / entities impacted:
List Window(s) of Intrusion and / or Exposure:
List Data Elements At Risk *(e.g,. Account Number, Expiration Date, Cardholder Name, CVV, CVV2, Address, Email, etc.)* If Account Data, List Number of Visa Accounts Impacted:
Detail all actions taken to investigate the suspected or confirmed incident (what, how, who, when, and where), including timeframes:
Have you enlisted the expertise of a third-party in this matter? ☐ Yes ☐ No If yes, please list and describe their role:
What type of remote access solution is used?
Is two-factor authentication in use for remote access? ☐ Yes ☐ No
Has the entity received complaints regarding fraudulent transactions from their customers? ☐ Yes ☐ No If yes, please describe:

Visa Incident Report Page 2

Has the entity been contacted by law enforcement? ☐ Yes ■ No
If yes, list date(s) and by which law enforcement agency and why: *(e.g., suspected Compromise Event of entity, fraudulent complaints from entities customers, etc.)*

Has the entity contacted law enforcement regarding the incident? ☐ Yes ☐ No
If yes, list date(s) and which law enforcement agency:

Has the Compromise Event been contained? ☐ Yes ☐ No
If yes, how and when?

If Merchant Please Include Details Below:

Merchant ID:	MCC:	PCI DSS Level:	Annual Transactions Volume:	Corporate or Franchisee:	# of Locations:

PCI Compliant ☐ Yes ☐ No Last PCI DSS Validation Date:

Acquiring Identifier, Issuing Identifier, or VSS Processor: (List all that are applicable):

List processor(s):	Provide Processor contact information:

Is the Point of Sale (POS) device EMV enabled? ☐ Yes ☐ No

Is the POS solution enabled with end to end encryption? ☐ Yes ☐ No

Is the ecommerce website hosted? ☐ Yes ☐ No
If yes, please provide name and contact information:

Identify responsible party(s) for the configuration and support of the Point of Sale (POS) solution *(e.g., Qualified Integrator, Reseller, or Agent).*	NAME	TITLE	CONTACT
	(If entity is an Integrator or Reseller, please attach a list all Acquiring Identifiers and all Merchant Names, Merchant Card Acceptor IDs, City and State.)		

Report Completed By:

Name	Title	Role

Email	Phone	Date Completed

Attachment B: Incident Report (Fraud Schemes)

Visa Fraud Schemes Incident Report Page 1				
Legal Entity Name:				
DBA Entity Name:				
Type of Entity: *(E.g., Visa Member, Processor, Service Provider, Agent, Merchant, etc.)*				
Services, Solutions, or Product Provided by Entity:				
Entity Address:	City:	State / Province:	Postal / Zip code:	Country:
Primary Contact Name:	Phone:		Email:	

All Fraud Scheme Information Below to be Completed By Reporting Entity / Incident Response Team
Fraud Scheme Type (e.g., Force Posting, Credit Vouchers, Purchase Return Authorizations, Combination Event, Fraudulent Merchant Onboarding, Bust-Out Scheme, Collusive Attack, Other, etc.)
Detailed Description of the Fraud Scheme (what, how, who, when, and where): *Note: If the incident involves multiple Acquirers, Issuers, merchants, etc. provide a file of transactions and a list of names, of the impacted entities:*
Detail all actions taken to investigate the Fraud Scheme (what, how, who, when, and where), including timeframes:

Fraud Scheme Impact
Number of Merchants Involved (Provide list including: Merchant Descriptor, BIN, CAID, MCC, etc.):
Number of Fraudulent Transactions Processed and Dollar Amount (USD) (provide detailed list of transactions including type (e.g., Force post, purchase return, etc.) if applicable):
Number of Issuers impacted (provide details if applicable):
Duration of Fraud Scheme:
Number of Visa Accounts Impacted:

Visa Fraud Schemes Incident Report Page 2		
What data was impacted *(e.g., Intellectual Property, PII, Customer Records, Payment Data, etc.)*?		
What systems were accessed or impacted *(e.g., Corporate, Payment Processing, Email, Checkout Page, Customer Service, etc.)*?		
Have you enlisted the expertise of a third-party in this matter? ☐ Yes ☐ No If yes, please list and describe their role:		
Has the entity contacted law enforcement regarding the incident? ☐ Yes ☐ No If yes, list date(s) and which law enforcement agency:		
Has the Event been contained? ☐ Yes ☐ No If yes, how and when?		
Report Completed By:		
Company Name		
Name	Title	Role
Email	Phone	Date Completed