MEMBER AND ENTITY OBLIGATION TO REPORT SUSPECTED OR CONFIMRED ACCOUNT DATA COMPROMISES

Visa has observed an increase in network intrusions involving service providers, re-breaches of merchant payment environments and skimming incidents involving Point of Sale (POS) device overlays. Visa is issuing this alert to make Members and entities aware of their obligations to investigate and immediately report all data compromise events.

Protecting the payment system is a shared responsibility. The Visa Rules and the 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).

At a minimum, all organizations that store, transmit, access and process cardholder data, as well as those that provide payment card services must maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) and PCI PIN Security Requirements. Compliance with the PCI DSS is the foundation of Visa data security programs and is key to protecting cardholder data. Visa also strongly encourages the use of payment technologies that eliminate card data, secure data in storage and transit, and devalue remaining information via dynamic authentication.

Upon identification or notification of a suspected or confirmed account data compromise, an impacted entity must immediately notify its acquirer (e.g. the merchant bank) and Visa, and initiate a preliminary investigation of all potentially impacted systems and those of any third-party service providers. Within three (3) business days[1], entities must share the findings with Visa as well as the acquirer, if applicable. A preliminary investigation is not the same as a Payment Card Industry Forensic Investigator (PFI) preliminary report. The procedures and timelines for account data compromises apply to network intrusions as well as compromises involving Point of Sale (POS) PIN Entry Device (PED) tampering or “skimming”.

What To Do If Compromised

The What to Do If Compromised document contains required procedures and timelines for reporting and responding to a suspected or confirmed account data compromise. These procedures include, but are not limited to:

- **Notification:** Immediately report to Visa any suspected or confirmed unauthorized access to any cardholder data environment.
- **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.
- **Engage a Payment Card Industry Forensic Investigator (PFI):** Entities investigating a data compromise may be required to engage a PFI. Visa has the right to reject a PFI report if it does not conform to the requirements established in the PFI Program Guide.
- **Provide All Exposed Accounts:** Entities are required to coordinate submissions of at-risk account through their acquiring bank. For more information about Visa’s Compromise Account Management System (CAMS) contact Visa at: VAA_VRM@Visa.com

Retain a Payment Card Industry Forensic Investigator (PFI)

Visa may require a compromised entity to engage a PFI to perform an independent forensic investigation. If a forensic investigation is required, the following timeline must be followed:

- Visa will not accept forensic reports from forensic organizations not certified as a PFI.
- Engage a PFI (or sign a contract) within five (5) business days of Visa's notification.
- Provide Visa with the preliminary forensic report within five (5) business days from PFI engagement (or the contract is signed). A preliminary PFI report is not the same as the preliminary investigation.
- Provide Visa with a final forensic report within ten (10) business days of completion of the review.
- The PFI may not be an organization that is affiliated with the compromised entity or has provided services to the compromised entity such a Qualified Security Assessor (QSA)
    - Visa disallows a PFI Company from being engaged if the company has performed a PFI investigation for the breached entity within the preceding twelve (12) months. A PFI Company that has provided QSA or ASV Assessment or a QIR installation within the preceding three (3) years of the current engagement is also disqualified.
    - PFI firms hired in a non-PFI capacity (e.g. under privilege, for incident response only, etc.) may not transition from non-PFI work to a PFI engagement.

Important Resources

- The Visa Rules and What To Do If Compromised Guide are available on Visa.com
- Visit www.pcisecuritystandards.org for more information on approved PFI organizations, PCI DSS and PCI PIN Requirements.
- Report Data Compromises to Relevant Parties:
    - Acquirer (Merchant Bank)
    - Visa Global Investigations Team
        - Asia Pacific (AP) and Central and Eastern Europe, Middle East and Africa (CEMEA) – VIFraudControl@visa.com
        - Canada CanadaInvestigations@visa.com
        - Europe datacompromise@visa.com
        - Latin America & Caribbean LACFraudInvestigations@visa.com
        - U.S. USFraudControl@visa.com
- For the latest on Visa security programs bulletins go to: www.Visa.com/CISP

[1] Visa Europe maintains separate **What To Do If Compromised** timelines. Members and compromised entities operating in Europe should contact datacompromise@visa.com for more information.

.