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, 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.)*

<table>
<tr><td>Name of payment application(s) and version(s):</td><td colspan="3"></td></tr>
<tr><td rowspan="5">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="3">(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="3"></td></tr>
<tr><td>Is the terminal PC-based or is it connected to a PC-based environment?</td><td colspan="3"></td></tr>
<tr><td>Is there remote access connectivity to the entity's environment?</td><td colspan="3">☐ Yes ☐ No
If yes, which organizations have remote access?</td></tr>
<tr><td>What type of remote access solution is used?</td><td colspan="3"></td></tr>
<tr><td>Is remote access always on or is it enabled upon request?</td><td colspan="3"></td></tr>
<tr><td>Is the Point of Sale device EMV enabled?</td><td colspan="3">☐ 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="3">☐ Yes ☐ No
If yes, provide details.</td></tr>
<tr><td>Does the entity accept PIN?</td><td colspan="3">☐ Yes ☐ No</td></tr>
</table>

Is the entity's PIN entry device (PED), PCI PTS approved and listed on the PCI SSC website?	☐ 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.
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?