

Incident Response Report Requirements

This report must be provided to card issuing association within 14 days after initial report of an incident to the card issuing association. The following report content and standards must be followed when completing the incident report. This report must be securely distributed to the card issuing association and the Credit Card Processor. The card issuing association will classify the report as “Sensitive Data”.

I. Executive Summary:

- Provide overview of the incident
- Include Risk Level (High, Medium, Low) during forensic analysis
- Specify if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures

- Include forensic tools used during investigation

V. Findings

- Specify number of accounts at risk, identify those stored and compromised
- State type of account information at risk
- Identify all systems analyzed. Include the following:
 - DNS names
 - IP addresses
 - OS version
 - Function of system(s)
- Identify all compromised systems. Include:
 - DNS names
 - IP addresses
 - OS version
 - Function of system(s)

- State timeframe of compromise
- Describe any data exported by intruder
- Explain established how and source of compromise
- Include evidence that all potential database locations have been checked to ensure that no CVV2, Track 1, or Track 2 data is stored anywhere, whether encrypted or unencrypted—e.g., in duplicate or backup tables or databases, databases used in development, stage or testing environment data on software engineers’ machines, etc.).
- If full track data is being stored by a third-party application, identify the following:
 - Vendor Name
 - Contact Information
 - Product Name
 - Product Version
 - Name of file(s) within application where full track is being retained
 - Reason for storage and how long full track is being retained
- If Vendor provided a patch or utility to remove full track data, identify the Product Name, Product Version/Fix, and a brief description of patch or utility.
- If product is supported by a reseller, identify the following:
 - Reseller Name
 - Contact Information
- If applicable, review VisaNet endpoint security and determine risk.

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation