Phase 1: The Initial Email Notification

Per Section 8, you must send an email to the PCI SSC within the period of time specified in the VRA, upon discovering a security issue that impacts a validated product.

Subject: URGENT: Security Issue Notification – [Vendor Name] – [Software Product Name]

To: software@pcisecuritystandards.org

Body:

> **To the PCI Security Standards Council,**
>
> This email serves as an initial notification of a security issue identified in the following validated software product:
>
> - **Software Name:** [Insert Product Name]
> - **Version(s) Impacted:** [e.g., v2.1.x]
> - **PCI SSC Listing Number:** [Insert uniqueReference # from the PCI listing]
>
> We are currently performing a technical analysis and preparing a formal written notification. A preliminary assessment indicates a **CVSS Base Score** of [Insert Score, e.g., 7.5].
>
> We will provide the formal written document within the timeframe required by our Vulnerability Handling Policies.
>
> **Primary Point of Contact:** [Name and Email]
>
> Regards,
>
> [Your Name]
>
> [Your Title]

Phase 2: Formal Written Notification Template

This is the detailed document that must follow the initial email. It should be provided on company letterhead.

Vulnerability Disclosure Report

1. General Information

- **Vendor Name:** [Name]
- **Product Name:** [Product]
- **Affected Version(s):** [List all versions]
- **Date of Discovery:** [Date]

2. Vulnerability Description

Provide a clear, technical summary of the issue. Avoid local slang or idioms.

- **Issue Type:** [e.g., Buffer Overflow, Improper Access Control, Encryption Weakness]
- **Description:** [Describe what the vulnerability is and how it could potentially be used to access sensitive assets.]

3. Risk Assessment (CVSS Scoring)

PCI v2.0 requires the use of the Common Vulnerability Scoring System (CVSS), or other industry-accepted standard scoring, to standardize risk communication.

- **CVSS Base Score:** [e.g., 8.2]
- **CVSS Vector String:** [e.g., AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N]
- **Impacted Sensitive Assets:** [List the assets identified in your SAID document that are at risk.]

4. Mitigation and Remediation Status

- **Current Status:** [e.g., Investigating / Patch in Development / Patch Released]
- **Remediation Version:** [The version number that contains the fix, e.g., v2.1.5]
- **Temporary Workarounds:** [Steps customers can take now to reduce risk while waiting for the patch.]

5. Notification of Impacted Stakeholders

- **Customer Notification Date:** [Date or "Planned for Date"]
- **Communication Channel:** [e.g., Customer Portal, Email Security Advisory]

Guidance for Global Use

- **Use CVSS Strings:** The CVSS "Vector String" (the short code like AV:N/AC:L...) is a universal technical language. Including it ensures that security professionals in any country can understand the exact nature of the risk without needing a translation.
- **Reference the SAID:** Always link the vulnerability back to the **Sensitive Assets** you defined during your assessment. This helps the Council understand if the "core" of the payment security is at risk.
- **Translation Readiness:** When describing the vulnerability, use "Subject-Verb-Object" sentence structures (e.g., "The software allows unauthorized access") to make it easier for automated translation tools to work accurately.