

Cardholder Data Security Best Practices for VisaNet Processors

Since 2001, VisaNet Processors (VNPs) and third party agents that store, process and/or transmit cardholder data are required by the *Visa International Operating Regulations* to maintain ongoing compliance with the Payment Card Industry Data Security Standard (PCI DSS). In addition to maintaining ongoing compliance 24 hours a day, 365 days a year, some payment processors have implemented security measures that go above and beyond the PCI DSS to proactively detect suspected breaches, eliminate unnecessary data and prevent against card data compromises

Through a series of discussions with these payment processors, Visa has compiled a list of best practices for maintaining cardholder data security at all times. VNPs and other agents should consider enhancing their security measures by implementing these recommendations. This article provides a detailed overview of these best practices. Many of these practices are closely linked to PCI DSS requirements but are typically designed to go beyond the basic requirement. Entities reviewing this document should assess their environment and determine how it may be improved with implementation of these recommendations.

Identify Business Processes and Define Scope

Entities should identify their organization's lines of business as well as the processes involved in storing, processing and/or transmitting cardholder data. By accurately identifying all business processes that handle cardholder data, processors can better define the scope of the cardholder data environment and ensure its adequate protection. These steps will enhance an entity's preparation for their annual PCI DSS review. To help identify business processes and scope, processors should:

1. Create a data matrix detailing all of the business lines and processes that handle cardholder data. Explain the need for such data and note whether the data is being stored, processed and/or transmitted.
2. Specify which elements of card data are being stored, processed and/or transmitted for each business line and process. Identify the protection method being used for each element (e.g., the access control method, the method used to render data unreadable, any compensating controls, etc.).
3. Specify all of the resources (including networks, systems, applications, databases, services, components and users) for each business line and process that have access to card data and explain the need for that access.
4. Detail all of the resources (including networks, systems, applications, databases, services, components and users) that may be shared with or accessed by corporate environments, external networks, third parties and other business lines, as well as the impact to card data and the need for such access.
5. Maintain the data matrix as part of your organization's overall security policy. Make necessary changes throughout the year as significant events occur (e.g., acquisitions/ mergers, new products or services, additions or modifications to resources including networks, systems, applications, databases, services, components and users, etc.).

Find and Eliminate Unnecessary Card Data; Reduce Scope

When implemented and configured properly, technologies that actively search for cardholder data can enhance the identification of business processes and the scoping of a cardholder data environment. Processors can use these findings to decrease the scope of the environment by eliminating unnecessary card data and processes that handle cardholder data.

To enhance the security of payment transactions across the overall payment system, processors should consider adopting and supporting processes and technologies that do not require storing cardholder data. Processors should also consider implementing the following measures to assist in finding and eliminating unnecessary card data, and to obfuscate or replace card data in certain environments:

1. Adopt data loss prevention (DLP) solutions to actively locate card data in real time across the organization's resources (including networks, systems, applications, databases and components). Some DLP solutions can alert designated individuals when unauthorized and unprotected card data storage is found, and prevent attempted, unauthorized transmission of card data out of the cardholder data environment.
2. Eliminate unnecessary cardholder data that is stored, processed and/or transmitted across all resources (including networks, systems, applications, databases, services and components).
3. Truncate cardholders' primary account number (PAN) when business processes do not require use of the full PAN.
4. Ensure for issuer processing that Card Verification Value (CVV) and CVV2 is calculated instead of storing sensitive authentication data for authentication of payment card transactions.
5. Ensure for acquiring processing that only the latest message specifications are used so that cardholder data and sensitive authentication data are not sent or required unnecessarily. (Legacy message specifications may have led to the unnecessary transmission of cardholder data and sensitive authentication data.)
6. Support unique identifier tokens (e.g., a Visa Transaction ID is used in some regions) for recurring payments and dispute resolutions, thereby eliminating merchants' storage of PAN data and reducing scope for acquirer processing systems where use of the full PAN is unnecessary.
7. Provide acquirer processing and key management for merchants using encryption payment solutions (also known as "end-to-end encryption") that meet the [Visa Best Practices for Data Field Encryption](#). When properly implemented, encryption payment solutions can reduce data "sniffer" compromise exposure for merchant and acquirer processing systems.
8. Provide an encryption service and/or private lines or private connections for the transmission of cardholder data to entities that need card data and are directly connected to you.

Maintain Oversight, Ongoing Security Awareness, and Response

A data security program based on and maintained against a robust security policy within an organization's oversight structure is critical to securing sensitive data. Processors should consider implementing these guidelines to maintain oversight and ongoing security awareness:

1. Entrust a security champion at the senior executive level to lead the organization's data security efforts, including the development and maintenance of the security policy and its strict adherence across the organization. Senior executive management (e.g., Chief Information Officer, Chief Technology Officer or Chief Information Security Officer) should be central to the oversight of the organization's data security policies, programs and procedures.

2. Use third party resources that provide security alerts (such as Visa Data Security RSS feeds and communications, U.S. CERT bulletins, MITRE's CVE database, SANS/CWE Top 25, OWASP Top 10, Microsoft, Symantec and others) to remain actively aware of the latest network, system, application, database, service and component vulnerabilities.
3. Perform vulnerability scans and penetration tests more frequently than required by the PCI DSS for critical resources (e.g., monthly, weekly or more often). Scan all resources including networks, systems, applications, databases, services and components for vulnerabilities and perform penetration tests to determine the effectiveness of current security controls.
4. Respond to and remediate all identified issues and address compromise trends in a prioritized manner according to criticality and exposure to cardholder data. Security escalation, remediation, vulnerability management and incident response procedures must be included as part of the data security policy.
5. Monitor the cardholder data environment by using log harvesting, parsing and alerting tools. Log management solutions provide scalable and centralized processes that can collect, normalize, aggregate, compress and encrypt log data from resources including networks, systems, applications, databases, services and components. Some log management solutions can generate reports and send alerts to designated individuals when an anomalous event or glitch occurs.

Conduct Internal Reviews and Third Party Assessments

To define the scope of internal reviews and third party assessments, processors should have an accurate understanding of their entire cardholder data environment. All VNPs must demonstrate full compliance with the PCI DSS, using an external third party Qualified Security Assessor (QSA).

However, processors should not solely rely upon an annual assessment by a QSA to identify where cardholder data is being handled or to uncover any lapses in security controls. Instead, third party assessments completed by a QSA should support the processor's existing security programs and regular internal reviews. When conducting internal reviews and setting selection criteria to be used by the QSA when assessing the cardholder data environment, processors should:

1. Examine the following areas and consider additional safeguards for network and system controls including, but not limited to, adequate cardholder data environment resource (e.g., networks, systems, applications, databases, services and components, etc.), segmentation from corporate environments and other business lines, proper configuration and access for Hardware Security Module (HSM) protection of PIN-based transactions, automated detection for unapproved software processes on critical systems, protection of authentication systems (e.g., domain controllers), and limited remote access for necessary vendors and third parties only.
2. Examine the following areas and consider additional safeguards for application controls including, but not limited to, SQL injection prevention for all web-based applications, database segmentation by not using shared databases, proper configuration and deployment of application firewalls, code reviews for internally developed software, and a three-tiered architecture for all web-based applications.
3. Review the Visa Security Bulletin, "Critical Vulnerabilities Identified to Promote Awareness," found at www.visa.com/cisp, which details risk mitigation measures for critical vulnerabilities that can lead to card data breaches.
4. Use only approved QSA companies found at www.pcisecuritystandards.org. The PCI Security Standards Council (SSC) has implemented a quality assurance program that reviews QSA companies. Identified issues will require remediation and may lead to sanctions culminating in revocation (if left unresolved).
5. Ensure that the QSA understands your acquirer and/or issuer processing environments and has full knowledge of the intricacies of your card processing environments. Verify that the QSA has completed at least three VNP PCI DSS assessments and has sufficient security experience and payment processing knowledge. Request referral contacts specifically for the assessor dedicated to your assessment.

6. Ensure that the QSA has attended a Visa PIN Security training seminar or a Visa Key Management training seminar every three years. These trainings reinforce knowledge of the complex processing environments and systems found at VNPs.
7. Require the QSA to maintain certification as a Payment Application QSA (PA-QSA) to ensure the QSA's knowledge of payment applications and the impact that improperly coded, installed or configured applications can have on a payment environment. Determine whether the assessor conducting your assessment has reviewed acquirer/issuer processing applications.

Actions Requested

The risk of being breached can be mitigated by achieving and maintaining PCI DSS compliance at all times. Processors must secure their cardholder data environments and immediately address vulnerabilities that may lead to a compromise of the network or sensitive systems. To enhance existing security programs, VNPs and other agents should implement the best practices outlined within this article.

In the event of a security incident, VNPs and agents are required to take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa and their sponsoring bank, and report investigation findings. Additionally, entities that suspect a security breach should contact law enforcement and consult with their legal department regarding local and country notification laws.

The protection of cardholder data is a responsibility shared by all participants in the Visa payment system. To prevent and quickly detect card data breaches, Visa is committed to providing educational information to its VNPs, agents and key stakeholders on best practices, data security alerts, vulnerabilities and compromise trends.

Related Documents

If a compromise is suspected, please refer to the *What To Do If Compromised* document available at www.visa.com/cisp.

For More Information

Contact the VisaNet Processor and Agent team at agentregistration@visa.com.