Visa Top 10 Best Practices for Payment Application Companies, Version 1.0

Introduction

Recent payment card data compromises have demonstrated the critical need for payment application companies to maintain mature software processes for their customers that go beyond Payment Application Data Security Standard (PA-DSS) compliant software. Acquirers, merchants and agents should review Visa's best practices and insist that their payment application vendors, integrators and resellers fully adopt these practices.

Visa Top 10 Best Practices for Payment Application Companies, Version 1.0

The following best practices should be reviewed by acquirers, merchants and agents to ensure that their payment application vendors, integrators and resellers mitigate security issues leading to data compromises. On their own, these best practices may not be appropriate or sufficient depending on the implementation of an entity's information technology (IT) infrastructure and business needs.

Visa provides this information solely to build awareness of the industry's best practices. It is important that all payment system participants remain diligent and maintain compliance with the Payment Card Industry Data Security Standards (PCI DSS) at all times.

Domain	Best Practice
Organizational Security	1. Perform background checks on new employees and contractors prior to hire
	2. Maintain an internal and external software security training and certification curriculum
Mature Software Development	3. Adhere to a common software development life cycle across payment applications
	4. Ensure that newly released payment application versions are Payment Application Data Security Standard (PA-DSS) compliant
Product Vulnerability Management	5. Conduct application vulnerability detection tests and code reviews against common vulnerabilities and weaknesses prior to sale or distribution
	6. Actively identify payment application versions that store sensitive authentication data and/or retain critical security vulnerabilities, and notify all affected customers

Secure Implementation	7. Maintain customer service level agreements stating that only PA-DSS compliant payment application versions will be sold and supported
	8. Implement an installer, integrator and reseller training and certification program that enforces adequate data security processes when supporting customers
Emerging Payment Technologies	9. Adhere to industry guidelines for data field encryption and tokenization and PAN elimination across payment applications that use these technologies
	10. Support capability of dynamic data solutions across payment applications

Top 10 Best Practices In Detail

1. Perform Background Checks on New Employees and Contractors Prior to Hire

Intent: Reduce the likelihood of hiring employees with a criminal record who may intentionally add malicious code to payment applications or circumvent procedures used to support customers, leading to a data compromise.

Best Practice: Perform background checks including, but not limited to, previous employment history, academic history, credit history and reference checks (within the constraints of local laws) on all new employees and contractors prior to hire. Background checks may be limited to payment application developers, installers and support personnel. All new employees and contractors must pass background checks before being offered employment.

2. Maintain an Internal and External Software Security Training and Certification Curriculum

Intent: Prevent employees with poor software security coding practices from unintentionally adding vulnerabilities into payment applications and exposing customers to risk of data compromise.

Best Practice: Maintain, at minimum, an annual internal and external software security training and certification curriculum for all payment application developers.

- Software security training and certification curriculum materials adhere to industry-recognized secure coding standards or best practices (i.e., CERT Secure Coding Standards, Microsoft Security Development Lifecycle, SANS Secure Programming Exam Blueprints).
- Curriculum is continuously updated to address and demonstrate proper coding methods to prevent repeat occurrences of vulnerabilities and weaknesses found during vulnerability detection tests and code reviews.
- All payment application developers must pass certification curriculum with high proficiency and possess current industry knowledge in secure software development.

3. Adhere to a Common Software Development Life Cycle Across Payment Applications

Intent: Adopt and consistently adhere to common methodologies across the company's payment applications, assuring customers that software is being properly developed and managed.

Best Practice: Adhere to a common software development life cycle approach based on ISO 12207, which addresses all stages of software development including planning, documentation, implementation, maintenance, testing, deployment and support.

- Payment application product managers (or equivalent) adhere to a common planning and documentation process for requirements gathering, design, and product documentation.
- Payment application developers (or equivalent) adhere to a common implementation and maintenance process for software code development, enhancements and updates.
- Quality assurance personnel (or equivalent) adhere to a common testing process for identifying software vulnerabilities.
- Installation and support personnel (or equivalent) adhere to a common deployment and support process, which supports all direct customers' PCI DSS compliance.

4. Ensure that Newly Released Payment Application Versions are PA-DSS Compliant

Intent: Provide customers with only PA-DSS compliant payment applications and ensure that implementation guides are available to help customers configure their systems to be PCI DSS compliant.

Best Practice: Ensure that all newly released payment application versions are, at minimum, PA-DSS compliant; annually validate through a Payment Application Qualified Security Assessor (PA-QSA) at least one version for each payment application.

- Ensure that all payment application versions have an up-to-date, accurate PA-DSS implementation guide, available and accessible to all stakeholders (i.e., customers, resellers and integrators); ensure that stakeholders know how to access the implementation guide, understand its purpose, and know the importance of following adequate data security processes to maintain ongoing PCI DSS compliance.

5. Conduct Application Vulnerability Detection Tests and Code Reviews Against Common Vulnerabilities and Weaknesses Prior to Sale or Distribution

Intent: Test payment applications against common vulnerabilities and fix all identified issues prior to release, thereby reducing compromise exposure to customers' systems.

Best Practice: Conduct application vulnerability detection tests and code reviews on new payment application versions prior to sale or distribution, using automated or manual techniques against common vulnerabilities and weaknesses.

- Application vulnerability detection tests and code reviews are, at minimum, based on the *CWE/SANS Top 25 Most Dangerous Programming Errors*.
- Individuals that perform automated or manual techniques to conduct application vulnerability detection tests and code reviews must be highly proficient in application penetration testing, application security, code reviews, vulnerability detection and remediation activities.
- All identified vulnerabilities and weaknesses are corrected and verified through iterative application vulnerability detection tests and code reviews.
- All identified vulnerabilities and weaknesses are, at minimum, incorporated into the internal software security training and certification curriculum to prevent future occurrences.

6. Actively Identify Payment Application Versions that Store Sensitive Authentication Data, Retain Critical Security Vulnerabilities, and Notify All Affected Customers

Intent: Eliminate vulnerable payment applications from the overall marketplace.

Best Practice: Actively identify all payment application versions, including previously sold or distributed versions that store sensitive authentication data (i.e., full contents of the magnetic stripe data, card validation codes, PIN data or chip card equivalents) after authorization or retain other critical security vulnerabilities that pose a risk of data compromise. Notify integrators, resellers and all affected customers within 30 days of identification.

- Notifications to integrators, resellers and customers should state that affected payment application versions:
  - Must no longer be sold
  - Place customers at a high risk of compromise if they continue to operate on the affected version, and must be upgraded to a PA-DSS compliant payment application
  - Will no longer be supported and will be sunset in a specified short-term time frame (or have already been replaced by a PA-DSS compliant version)

7. Maintain Customer Service Level Agreements Stating that Only PA-DSS Compliant Payment Application Versions will be Sold and Supported

Intent: When purchasing payment applications, assure customers that only PA-DSS compliant versions will be sold and supported.

Best Practice: Maintain service level agreements with all customers (new, modified and renewed contracts) that at minimum, state that only PA-DSS compliant payment application versions will be sold and supported.

8. Implement an Installer, Integrator, and Reseller Training and Certification Program that Enforces Adequate Data Security Processes when Supporting Customers

Intent: Ensure that customers are not being exposed to data compromise due to poor implementation, maintenance or support processes employed by internal installers, independent integrators or resellers. Always enforce data security requirements when accessing customer sites.

Best Practice: Implement an internal installer, independent integrator and reseller training and certification program to enforce adequate data security requirements when supporting customers.

- Ensure that installers, integrators and resellers maintain adequate data security requirements in accordance with all PCI DSS and PA-DSS requirements, in addition to:
  - Ensuring that all new employees and contractors with access to customer sites pass background checks including, but not limited to, previous employment history, academic history, credit history and reference checks (within the constraints of local laws) before being offered employment.
  - Ensuring that employees and contractors with access to customer sites are trained on how to adequately access, install, maintain and support payment applications (and any connected systems) in accordance with industry data security best practices and standards.
  - Not selling, installing or supporting any vulnerable payment applications listed on the Visa list of Payment Applications that Store Sensitive Authentication Data (or any other known payment application that stores sensitive authentication data after authorization).
  - Ensuring that the latest PA-DSS implementation guide is understood and adhered to by all employees and contractors with access to customer sites.
  - Verifying at the completion of an installation that the payment application and its respective systems were correctly installed or configured; unique user IDs must be used for each customer site and for secure authentication functions.
  - When upgrading the payment application, verifying that all historical sensitive authentication data, if stored by previous versions of the payment application, is securely wiped.
  - When debugging or troubleshooting for customers, verifying that sensitive authentication data, if necessary to resolve a problem, is collected in limited amounts, encrypted while stored, and securely wiped immediately after use.

- Ensuring that remote access to any customer's site for the purposes of installation, support and maintenance is always done securely by:
  - Restricting access to customers' sites and authentication credentials to only those personnel who need access.
  - Limiting access from a limited number of trusted IP addresses and providing customers with a list of those IP addresses.
  - Using strong two-factor authentication.
  - Using unique, complex and secure authentication credentials for each customer.
  - Ensuring that data transmissions are always encrypted.
  - Advising customers to turn on remote access technologies only when necessary and needed, and to turn off access immediately thereafter.
  - Instructing customers to install and properly configure a firewall, limiting remote access only to IP addresses where remote access is needed.
- At minimum, installers, integrators and resellers must certify to these data security requirements through an internal vendor program requiring quarterly reports, which include employee training, certification and ongoing compliance to the requirements. For any installer, integrator or reseller who fails to maintain compliance and is found to have played a direct role in a customer's compromise, immediate dismissal or revocation will occur.

9. Adhere to Industry Guidelines for Data Field Encryption and Tokenization and PAN Elimination Across Payment Applications that Use these Technologies

Intent: Reduce the risk of compromise by reducing cardholder data in customers' environments.

Best Practice: Adopt data field encryption and tokenization and PAN elimination best practices across payment applications that incorporate these technologies.

- Payment applications (as distributed "out-of-the-box" to customers) adhere to *Visa Best Practices for Data Field Encryption, Version 1.0*, *Visa Best Practices for Tokenization, Version 1.0* and *Visa Best Practices for Primary Account Number Storage and Truncation, Version 1.0*.

10. Support Capability of Dynamic Data Solutions Across Payment Applications

Intent: Devalue transaction data by supporting the capability of dynamic data solutions, rendering card data that may be compromised useless for fraudulent purposes.

Best Practice: Support dynamic data through authentication technologies (e.g., EMV chip, Visa contactless chip, 3-D Secure) across payment applications.

- At minimum, payment applications used in card present transactions (as distributed "out-of- the-box" to customers) provide support for EMV chip-capability in accordance with *EMV Integrated Circuit Card Specifications for Payment Systems* or support for Visa contactless in accordance with the *Visa Contactless Payment Specification.*

- Payment applications used in card-not-present transactions (as distributed "out-of-the-box" to customers) provide support for 3-D Secure in accordance with the 3-Domain Secure protocol.

Conclusion

To stay on top of recent compromise trends, Visa has developed a set of best practices to help payment application companies address critical software processes. As part of their due diligence, acquirers, merchants and agents should ensure that the payment application companies they use have passed a rigor of mature software processes including the Visa Top Ten Best Practices for Payment Application Companies. To raise awareness of these best practices, Visa is working with the SANS Institute to offer security training courses to payment application companies that are tailored to address Visa's best practices. SANS is one of the most trusted sources for security training, with courses that are developed by industry leaders in numerous fields including network security, forensics, audit, security leadership and application security. For more information on these courses please visit www.sans.org/visatop10.