Visa Best Practices for Payment Application Integrators and Resellers

Recent data compromises have demonstrated the need for third party payment application integrators and resellers to maintain security processes that go beyond providing software that is compliant with the Payment Application Data Security Standard (PA-DSS).

The following best practices help defend against poor implementation, maintenance and support processes that have led to merchant and agent data compromises. Visa advises acquirers, merchants, agents and payment application vendors to contact their licensed integrators and resellers, and insist that these best practices be immediately adopted. Merchants and agents should also consider including these best practices as a condition of their service level agreements with third party integrators and resellers.

Goal	Best Practices
Provide customers with security assurances	1. Sell and install only those payment application versions that fully meet the latest version of the PA-DSS requirements. 2. Do not sell, install or support 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[1] after authorization). 3. When upgrading a payment application, verify that any historical sensitive authentication data stored by previous versions of the payment application is securely wiped. 4. Ensure that new employees and contractors who need 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). 5. Take disciplinary action against employees and contractors who fail to securely access, install, maintain or support payment applications (and any connected systems) in accordance with industry data security best practices and standards.
Maintain secure processes when accessing customer sites	6. Require all employees and contractors with access to customer sites to strictly follow secure access, installation, maintenance and support processes outlined in the product vendor's latest PA-DSS implementation guide. 7. Train employees and contractors with access to customer sites on how to access, install, maintain and support payment applications (and any connected systems) in accordance with industry data security best practices and standards.
Limit exposure of customer payment systems and card data	8. Use remote management software only when absolutely necessary, and in a secure manner, to access customer sites for the purposes of installation, support and maintenance: a. Restrict site access and authentication credentials to only those personnel who need access. b. Restrict site access to a limited number of trusted IP addresses; provide customers with a list of those IP addresses. c. Use strong two-factor authentication. d. Use unique, complex and secure authentication credentials for each customer. e. Ensure that data transmissions are always encrypted. f. Advise customers to turn on remote management only when necessary, and to turn off access immediately thereafter. 9. After completing an installation, verify that the payment application and its respective systems are correctly installed and configured; unique user IDs must be used for each customer site and for secure authentication functions. 10. When debugging or troubleshooting for customers, verify that any cardholder data, if necessary to resolve a problem, is collected in limited amounts, encrypted while stored and securely wiped immediately after use.

[1] Sensitive authentication data is defined as the full contents of magnetic stripe, CVV2 or PIN data; Visa rules and the PCI DSS prohibit this data from being stored following a payment authorization.

Visa is providing this information solely to build awareness of the industry's best practices. On their own, these best practices may not be appropriate or sufficient depending on an entity's information technology infrastructure and business needs. It is important that all payment system participants maintain ongoing compliance with the Payment Card Industry Data Security Standards (PCI DSS).

In the event of a data compromise, integrators and resellers must not tamper with evidence and must fully cooperate with the merchant or agent, acquirer, payment card brands and law enforcement on the investigation.

Related Document

What To Do If Compromised: Visa Inc. Fraud Control and Investigations Procedures