VISA Risk Guidance Sep. 2014

Digital Wallet Guidelines for Merchants

Digital wallets are a rapidly evolving, diverse set of solutions that enable consumer payments through mobile or cloud-based technology. The wide variety of product offerings, user experiences, and service providers makes it challenging to provide a simple definition; however, digital wallets are likely to share common features like:

- The ability to make payments at multiple merchants through one set of user credentials
- The ability to associate multiple payment methods, including multiple card brands
- Accessibility from multiple internet-connected devices, such as PCs, mobile phones, or tablets

Digital wallets are an emerging technology with the potential to connect consumers and merchants. However, merchants should be aware of the implications of integrating with a service provider, and guidelines to consider when doing so. For example:

- Data collected as part of a transaction may differ from other solutions. This may require adjusting processes and systems that depend on this data
- Technical vulnerabilities may be created if integration guidelines are incomplete or merchants do not follow them

Visa therefore offers the following recommendations to help ensure a successful integration, regardless of who the service provider is.

Goal	Guidelines
Limit use and ensure protection of sensitive data	**1. Minimize use of Payment Account Information** Merchant systems are a target for cyber-attacks by data thieves seeking payment data. Perpetuating use and storage of payment data, including Primary Account Number (PAN), expiration date and Cardholder Verification Value 2 (CVV2) increases the likelihood and impact of a merchant data breach. Merchants should determine if a service provider can help minimize this risk, by removing data shared with merchants, or substituting it with a tokenized value. Also, be aware that any entity that stores, processes or transmits PANs, is required to protect their systems and validate compliance with the Payment Card Industry Data Security Standard (PCI-DSS)[1]. The merchant's scope and complexity of compliance is reduced when PCI-DSS compliant service providers take a larger role in managing payment data on behalf of merchants. **2. Protect Sensitive Customer Data**

Goal	Guidelines
	Sensitive customer data includes any information that can personally identify an individual. Examples include user account name, contact information, and account data used to make purchases. It is often essential for service providers and merchants to exchange this data, and it should be protected by industry standards based on layered information security programs. Examples include ISO 27001 and PCI DSS. Using a PCI DSS compliant service provider does not absolve merchants from validating compliance with PCI DSS. Even if all PAN data routes through third parties, merchants should perform due diligence to ensure their service provider has validated compliance with PCI DSS. This can be done by requesting an Attestation of Compliance (AOC) and checking Visa's Global Registry Service Providers at http://www.visa.com/splisting/index.html. **3. Use Strong Authentication** Merchants should verify that a service provider does not authenticate a consumer's identity solely upon public or semi-public information such as email address, phone number, date-of-birth, mother's maiden name, any part of a government ID, or any part of a cardholder's Primary Account Number. Service providers should use multiple means to govern access to a digital wallet account. Preferred methods include: • Risk-based analysis to detect unusual behavior • Dynamic data, such as one-time-passwords • Step-up authentication based on questions and answers not found in public records or easily guessed
Practice effective fraud management	Integration with a service provider may affect existing fraud operations, including the ability to receive certain data, and change risk management rules. Merchants should therefore understand their current fraud trends, risk tolerances, controls and data dependencies prior to integration. **1. Engage internal fraud team from the beginning of integration** Introducing new payment methods can initially attract attempted fraud campaigns, particularly in eCommerce channels. These campaigns may drop off rapidly soon after, however merchants should prepare by ensuring all appropriate fraud and risk management resources are available and activated in advance. **2. Analyze current fraud control systems and processes** Integration with a service provider may affect existing fraud operations, including the ability to receive certain data, and change risk management rules. Incomplete data may result in higher fraud penetration and chargebacks. Therefore, Merchants may need to ensure service provider data aligns with their internal systems.

Goal	Guidelines
	3. Leverage service provider's controls Merchants may be able to extend their own fraud detection capabilities by incorporating service provider data. Digital wallet service providers see behavior across a wider population of consumers and merchants, and therefore may have capabilities a single merchant may not. This may allow a service provider to generate risk scores based on inputs like: • **Account Data –** analysis of information associated with previous fraud such as account names, email addresses, shipping addresses, and credit card accounts. • **Device Identification –** supports recognizing devices not previously associated with an account holder, or configurations associated with riskier behavior. • **Velocity Checks –** designed to detect unusual behavior over a set duration. Examples include multiple failed login attempts, an unusually high number of purchases, or multiple accounts created from a single computer. If a service provider does offer risk scores, determine whether reports are available to illustrate effectiveness. For example, correlation of high risk transactions, to fraud and chargeback rates.
Ensure effective integration of systems and processes	**1. Follow the service provider's integration procedures** Service providers should provide specific steps for integration, including details on security controls for authentication, key management, and application security. Merchants should thoroughly review and adhere to these detailed integration procedures. **2. Perform testing prior to live integration** Merchants should use testing environments (aka "sandboxes") offered by service providers to help identify issues prior to making a digital wallet available to their customers. Prior to launching, merchants should perform their own security testing for application vulnerabilities, and simulate manual processes, such as customer support scenarios in order to identify and close gaps. **3. Perform monitoring** Merchants should establish a baseline understanding of how an environment behaves prior to integration. Additional monitoring should be performed immediately following an integration in order to establish familiarity with any new behaviour, and develop the ability to detect and respond to anomalies.

Additional Information

- **Visa E-Commerce Merchants' Guide to Risk Management -** Tools and Best Practices for Building a Secure Internet Business: http://usa.visa.com/download/merchants/visa_risk_management_guide_ecommerce.pdf

Feedback

As a leader in the payments industry, Visa has developed these guidelines to support the growth of the emerging digital wallets channel. As such, Visa welcomes any feedback on these best practices. To provide feedback or comments on this document, send an e-mail to inforisk@visa.com with "Digital Wallet Guidelines for Merchants" in the subject line.