VISA Risk Guidance 14 March 2013

Digital Wallet Guidelines for Merchants

BACKGROUND

Digital wallets are services used by consumers for managing payments and related functions. Features may include:

- The ability to store multiple payment methods, including multiple card brand accounts
- The ability to make purchases in both face-to-face and eCommerce settings
- Access from any internet-connected device, such as mobile phones, PCs or tablets
- Authentication through a common set of user credentials
- Value-added functions such as coupons, loyalty programs or transaction alerts

Visa expects digital wallets to become increasingly common as electronic payments blend with mobile and cloud-based technology, social networking, and internet search engines. Solutions vary widely in implementation, technology, and business models, and in many cases require merchants to integrate with a service provider in order to participate.

Digital wallets are an emerging technology offering great potential for connecting 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:

- Control over certain services such as fraud management may shift, but liability may not. Merchants should identify how they may be impacted
- Data collected as part of a transaction may be different with a digital wallet. This may require adjusting processes with dependencies on this data
- Technical vulnerabilities may be created if integration guidelines are incomplete or merchants do not follow them

Visa offers the following guidance to help merchants integrate with a digital wallet, regardless of who the service provider is.

Goal	Guidelines
Identify and close fraud management gaps	**1. 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. Merchants should therefore understand their current fraud trends, risk tolerances, controls and data dependencies prior to integration. **2. Identify service provider's controls** Service providers may extend or replace a merchant's existing fraud controls by drawing upon a large set of data, account information, and rules to evaluate risk based on inputs such as: • **Account Data;** including information associated with previous fraud such as account names, email addresses, shipping

Goal	Guidelines
	addresses, and credit card accounts. • **Device Analysis;** including recognizing devices not previously associated with an account holder, or configurations associated with riskier behavior. • **Velocity Checks;** including a high number of unusual behaviors over a set duration. Examples include multiple failed login attempts, an unusually high number of purchases, or multiple accounts created from a single computer. Because digital wallet service providers see behavior across a wider population of consumers and merchants, they may have capabilities a single merchant may not. However, they may lack capabilities found in highly customized systems. Ensure familiarity with the full range of capabilities offered by the service provider. **3. Adjust and Implement fraud controls** Although a digital wallet service provider may greatly enhance fraud management capabilities, merchants should not assume that by integrating they are no longer responsible fraud generated through this channel. Liability for fraud may or may not lie with a merchant participating in a digital wallet. Merchants should therefore continue to play an active role in managing their fraud, and should ensure essential controls are available either through internal systems, a service provider, or a combination of both.
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 minimize this risk by removing it from transaction 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]. This burden is shifted to service providers who take a larger role in managing payment data on behalf of merchants. **2. Protect Sensitive Customer Data** Sensitive customer data includes any information that can

[1] PCI DSS Applicability Information: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Goal	Guidelines
	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. **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
Ensure Secure 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

- **Verified by Visa -** A global program designed to make shopping on the Internet safer and more secure for both shoppers and merchants: http://usa.visa.com/merchants/risk_management/vbv.html
- **Digital Wallet Security: Just "LOK" It -** Visa's guidance to consumers on protecting Digital Wallets. http://www.visasecuritysense.com/en_US/_media/digital-wallet-best-practices.pdf

Best Practices Feedback

As the leader in the payments industry, Visa has developed these best practices 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 these best practices, send an e-mail to inforisk@visa.com with "Digital Wallet Best Practices for Merchants" in the subject line.