Beware the Digital Pickpocket: Fraud Risk in Digital Wallets

Device-based digital wallets have never been more popular. They ensure payment is fast, convenient and hygienic. As a result of the global pandemic, tap-and-go contactless has become the go-to payment method for merchants because it is clean and efficient. Housebound consumers are benefitting, too, making more purchases from their devices without reaching for their credit card. Digital wallets are also great for banks because they use tokenization, which increases security.

What is tokenization? In short, it replaces the sensitive information on a card with a digital alias unrecognizable to prying eyes. Tokenization begins when a cardholder registers for a digital wallet on their device and enters their card details. A token is instantly generated (if approved), linked to that card and device, and used in place of the card number (PAN) for future purchases. This increases the security of the payment by limiting the exposure and use of the real PAN, therefore reducing the risk of the cardholder's account being compromised.

However, fraudulent transactional activity can still occur on a token, similar to that on a plastic card. An added consequence is that issuers and merchants may perform less rigorous fraud monitoring if they believe that thorough cardholder authentication was performed at the time of card provisioning. In other words, if a fraudster can successfully enter a stolen card into their own digital wallet by passing the issuer authentication checks, they have cleared a major security hurdle. Let's be clear - fraud on tokenized transactions is consistently lower than non-tokenized transactions, but there is still enough fraud volume to prompt issuers to be more stringent in their identification and verification processes.

The process of provisioning a card PAN into a digital wallet is relatively straightforward for the cardholder, but can be technically complex for an issuing bank. As a fairly recent component of consumer banking, it introduces new intricacies that can take time to become familiar with. Due to consumer demand, some banks have quickly enabled the tokenization of their card portfolio – a great thing for technological advancement – without preparing adequately for risk. Mastercard data has shown that in this rush to conform, cracks have emerged in customer authentication and in the education of call centre staff, allowing fraudsters to slip through and exploit the weaknesses.

To reduce fraud on tokenized transactions, there are a number of things that should be observed and monitored at the time of provisioning to ensure that it is the genuine cardholder attempting to digitize their card and not a fraudster. Some examples are:

- Decline any requests with a CVC 2 mismatch
- Decline any suspicious activity, and/or request additional authentication by way of, for example, an activation code sent to the cardholder's device.
- Set up velocity checks on devices, IP addresses and card PANs
- Make use of the extensive wallet provider data and advice sent within the provisioning request message
- Ensure adequate call center training to avoid social engineering and phishing exploitations

Mastercard continues to provide advice and detailed information on the available data, configuration and fraud best practices through our publications and communications available in MC Connect. Stopping fraudsters before they transact is the ultimate solution for digital wallet security and will ensure that tokenization continues to grow and keep its status as the most secure and robust tool against digital pickpockets.