How can merchants reduce fraud risk?

30 YEARS | Australian Payments Network

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS defines the minimum security controls required when cardholder data is stored, processed or transmitted. The goal is to increase security controls and minimise the card data compromised in the instance of an attack (such as a data breach).

Compliance with PCI DSS can be a significant undertaking and online merchants may wish to investigate the use of hosted solutions provided by a PCI DSS-compliant service provider.

Use tools that help authenticate customers

Strong Customer Authentication should be used for transactions identified as higher risk (including high value transactions), to ensure the person requesting the transaction is the legitimate card owner.

In addition to other risk-based fraud controls used by merchants, the 3DS 2.0 protocol includes an ability to share greater data to inform a more assured risk-based decision by the card issuer and reduce declines.

Invest in tokenisation

Merchants holding sensitive payment information can become targets for the theft of card data, through hacking or other data breaches. Tokenisation replaces the original payment credential with a unique digital identifier (a token). This means that even if there is a data compromise of a merchant's systems, the card information cannot be misused.

The card schemes and financial institutions now offer tokenisation services, based on the EMV Payment Token specification. Payment tokens offer an additional layer of security, and deliver unique identifiers across different channels, linking back to the original 16-digit card Personal Account Number of the payment card.

MOTO transactions

Mail Order/Telephone Order (MOTO) transactions – in which the cardholder provides card details over the phone to the merchant – are susceptible to fraud, because it is difficult for the merchant to verify the identity of the cardholder. Merchants should be cautious processing MOTO transactions, especially where unusually large value items, or multiple duplicate orders for the same item, are concerned.

Overseas cards

It is possible to use fraud management selectively and apply rules to different transactions based on, for example, transaction value, product purchased and shipping destination. Rules can also be set on card issuing country, so that you can choose to evaluate overseas card transactions more thoroughly.

EMV chip technology

The global shift to EMV chip technology is proving effective in preventing face-to-face fraud.

A small number of cards (e.g. some overseas, prepaid) may not have chip. If a signature is required, check it carefully against the card signature.

Merchants should encourage cardholders to insert chip cards for contact transactions or tap cards for contactless transactions (with or without PIN).

Avoid refunds to alternative cards

The card schemes define the rules and processes for disputing a transaction.

All refunds should be processed onto the same card that was used to make the original purchase. Requesting a refund to a different card is a common fraudster tactic.

Contact: Toby Evans – Head of Economic Crime, AusPayNet | ecf@auspaynet.com.au