CNP FRAUD MITIGATION FRAMEWORK SUMMARY

Australian Payments Network

Card-Not-Present (CNP) fraud represents approximately 85% of all card fraud on Australian-issued cards. In the 2017/2018 financial year, this cost the e-commerce industry $478 million.

AusPayNet's CNP Fraud Mitigation Framework is designed to reduce fraud in online, CNP channels, while ensuring that online transactions continue to grow. The Framework defines the minimum requirements for an Issuer or Merchant (or Acquirer or Payment Gateway) to authenticate CNP transactions online, establishing authentication as best practise to reduce fraud in online, CNP channels.

GUIDING PRINCIPLES

- Leverage global standards and best practises from other jurisdictions
- Consistently apply Strong Customer Authentication (SCA)
- Be technology neutral to provide choice and ease of implementation
- Act now, plan for the future (review scope and thresholds annually)

IN SCOPE

- Online CNP transactions
- AUS acquired transactions on AUS issued cards
- Settled transactions
- Fraudulent transactions as reported to the Schemes

OUT OF SCOPE

- MOTO transactions
- Card present channels and other payment rails
- Corporate cards, gift cards, pre-paid cards
- Overseas acquired and/or issued transactions

REPORTING

Issuers and Acquirers are obliged to provide quarterly reporting to AusPayNet outlining Fraud Rates and Fraud Rate breaches.

IMPLEMENTATION

The Framework will be effective as of 1 July 2019 with the first quarterly reports due on 15 July 2019, covering the Q2 reporting period (April, May, June 2019).

If you are an active participant in e-commerce and would like a copy of the Framework, please email us at mitigateCNPfraud@auspaynet.com.au.

AUTHENTICATION

Risk Based Analysis assesses the characteristics of a transaction to create a risk profile. The level of authentication required can then be set proportionally to that risk profile: a high-risk transaction requires a higher level of authentication; a low-risk transaction requires little to no authentication.

Strong Customer Authentication (SCA) is also known as two-factor or multi-factor authentication. At least two factors must be used from at least two different categories:

- Something you have – e.g. a card, token or device
- Something you know – e.g. a PIN, password or pattern
- Something you are – e.g. biometrics – a fingerprint, voice print or facial recognition

Risk Based Analysis and SCA are commonly used in an integrated approach, however the Framework only has obligations mandating the use of SCA, not Risk Based Analysis.

Some low risk transaction types, including recurring payments, trusted customers and wallet transactions, are exempt from authentication.

OBLIGATIONS

The Framework will be enforced through AusPayNet's Issuers and Acquirers Community Code Set. It will work by defining fraudulent transaction value and volume thresholds that all Merchants and Issuers must remain below. Breaches of these thresholds will trigger obligations for Merchants or Issuers to take action. Repeated breaches over a period of time could ultimately result in financial penalties for Issuers or Merchants' Acquirers.

The **initial Merchant Fraud Threshold is set to 20bps and $50,000** in fraud losses, per quarter

- The Merchant Fraud Rate is calculated using the value of fraudulent, settled, online CNP transactions, each quarter.
- To trigger a breach of the threshold, in addition to exceeding the 20bps Fraud Threshold, a Merchant must also have more than $50,000 in fraud losses for the reporting quarter

The initial **Issuer Fraud Threshold is set to 15bps**

- The Issuer Fraud Rate is calculated using the value of fraudulent, settled, online CNP transactions that were sent to an Issuer for authentication, each quarter.