Australian Payments Network

Issuer and Acquirer Best Practice Guidelines for Card Not Present Transactions

7 March 2017

About this document

This document has been prepared by Australian Payments Network Limited (AusPayNet).

Contact

AusPayNet
Manager, Payments Innovation
Level 23, Tower 3, International Towers Sydney
300 Barangaroo Avenue
Sydney NSW 2000

Publication

Information in this document is subject to change without notice. No part of it may be copied, reproduced or translated without prior written permission from Australian Payments Network Limited.

Written and published in Sydney, Australia by te Australian Payments Network Limited.

TABLE OF CONTENTS

1. INTRODUCTION 3

2. ONLINE PAYMENTS IN AUSTRALIA 3

2.1 Australia's Payments Mix 3

2.2 eCommerce in Australia 3

3. CARD NOT PRESENT FRAUD 4

4. SOLUTIONS TO CARD NOT PRESENT FRAUD 5

5. PROPOSED SOLUTION – GUIDELINES 6

5.1 Guidelines Introduction and scope 6

5.2 Objectives and Principles 6

5.3 Glossary 7

6. Cardholder data and its security 10

6.1 Protect Cardholder data 10

6.2 Maximise the use of available data 10

6.3 Privacy – Treatment of data generated during transactions 11

7. Cardholder Authentication 12

8. Fraud Detection 14

9. Tokenisation 15

10. Cardholder Education and Merchant Fraud Prevention 16

1. INTRODUCTION

The increasing importance of online commerce, which provides convenience and efficiency benefits to both merchants and consumers, means that the volume of digital transactions continues to increase. Online transactions are primarily carried out by either a cardholder entering their payment card number into the merchant website, the merchant keeping the cardholder's details on file from a previous transaction or in-app. Such card-not-present (CNP) transactions provide increased scope for fraud, as there is greater potential for the transaction to be facilitated by someone other than the cardholder. As a result, the significant increase in e-commerce and online transactions has corresponded with a substantial increase in payments fraud.

Different jurisdictions worldwide have attempted to solve this problem in markedly different ways. Mandating a single solution appears to be sub-optimal since a single solution would not necessarily cover all of the facets of fraud mitigation: fraud detection; cardholder authentication and the security of cardholder data.

In contrast, industry best-practice guidelines can address a range of potential solutions and implementation issues. They can also enable non-technical aspects, such as merchant choice, and the education of cardholders and merchants on preventions to be covered. Another advantage of industry guidelines is that they can be reviewed regularly – by AusPayNet – to ensure they remain relevant and fit-for-purpose. This is especially important given predicted changes in the eCommerce space.

2. ONLINE PAYMENTS IN AUSTRALIA

2.1 Australia's Payments Mix

The Australian payments market is characterised by a clear long term trend away from cash to electronic payment methods, such as direct entry and debit, credit and charge cards. The digital economy continues to drive a decline in traditional payment methods such as cheques and cash, with both consumers and businesses continuing to reduce their use of such methods[1]. Current data regarding the use of different payment channels in Australia is available on the AusPayNet website.

2.2 eCommerce in Australia

These trends have been driven in part by the increasing importance of online commerce, which provides convenience and efficiency benefits to both merchants and consumers. The remote and 'always on' nature of online commerce is attractive to merchants and consumers alike.

For merchants, it enables:
(a) a massive geographic reach without having to invest in multiple physical points of presence (both lowering costs and increasing the size of the available market);
(b) sales to occur 24 x 7; and
(c) small merchants to compete like large merchants.

For consumers, it enables:
(a) the ability to comparison shop across a vast array of offers, both domestic and overseas;
(b) purchases to occur 24 x 7; and
(c) the convenience of shopping from the home / the office / anywhere.

[1] APCA Milestones Report - The Digital Economy - November 2016.

Hence, the ever increasing importance of the internet has meant a burgeoning online economy with online payments growing alongside it. The Reserve Bank of Australia (RBA) estimated that online payments more than doubled between 2007 and 2014[2].

3. CARD NOT PRESENT FRAUD

Online transactions inherently involve the card not being physically available for the merchant to inspect at the time of the transaction. Such CNP transactions include online transactions and mail order or telephone transactions, but with the vast majority being online transactions. Online transactions are primarily carried out by either a cardholder entering their payment card number into the merchant website, the merchant keeping the cardholder’s details on file from a previous transaction or in-app.

CNP transactions provide increased scope for fraud, as there is greater potential for the transaction to be facilitated by someone other than the cardholder. As a result, the significant increase in e-commerce and online transactions has corresponded with a substantial increase in payments fraud.

Payments fraud in the context of a CNP transaction (CNP fraud) can arise in a number of contexts including through cardholder information being:
(a) obtained illegally through card theft, malware on the cardholder's device or merchant database hacking;
(b) intercepted through communications systems; or
(c) obtained by cardholder deception such as through 'phishing' scams, in which fake communications (i.e. emails) that purport to come from a genuine source are used to encourage cardholders to provide information.

Fraud statistics published by AusPayNet[3] indicate that in 2015:
(a) total CNP fraud affecting Australian Merchants and Cardholders reached $398m; and
(b) CNP fraud made up 83 per cent of all payments card fraud in Australia by value.

A factor contributing to the growth in CNP fraud has been successful security initiatives in relation to card present transactions, including the introduction of chip cards (which are currently the most effective technology for preventing counterfeit fraud) and mandatory use of PIN authentication (which reduced lost and stolen card fraud). These increased security measures have made CNP fraud relatively easier for criminals to engage in than at physical point of sale.

Online payments fraud is an issue of concern both across the payments industry as well as for consumers. Consumers are impacted by online payments transaction fraud in four important ways:

(a) consumers meet the cost of fraud through increases in the price of goods purchased online and the cost of payments services;

(b) consumers are inconvenienced by fraud through meeting the cost of fraudulent transactions that they do not identify, the need to request the reversal of fraudulent transactions, obtain new cards, re-establish direct debits on the new card account;

(c) consumers experience undermined confidence in the online payments system and the loss of efficiencies through utilising online payments; and

[2] The Changing Way We Pay: Trends in Consumer Payments - June 2014.
[3] The Australian Payments Fraud Report 2016.

(d) consumers face significant risks associated with fraud through the disclosure of personal information and potentially identity theft.

Research commissioned by AusPayNet and conducted by IDCARE in 2016 has shown that the impact of such fraud on consumers can be significant:

(a) Cardholders spend on average 1.3 hours consulting with financial institutions and redirecting payment arrangements in response to a compromise; and

(b) 42% of consumers immediately ceased transacting online usually within 72 hours of the event. 79% of these typically re-engaged within a week and the remaining 21% often within a month.

4. SOLUTIONS TO CARD NOT PRESENT FRAUD

Different jurisdictions worldwide have attempted to solve this problem in markedly different ways. Research conducted by AusPayNet has shown that:

(a) The scope of various approaches across different geographies is greater than just authentication and now also covers detection and data security;

(b) Co-ordination of authentication analytics (across digital identity, geo-location, device proximity, biometrics and social media analytics) also needs to be considered; and

(c) Collaboration and respect of merchant choice is key.

In addition, the nature of eCommerce and the associated CNP fraud is likely to change markedly over coming years. Separate research commissioned by AusPayNet and conducted by IDCARE in 2016 suggests that the payment landscape is changing:

(a) Card payments will continue to rise and become the majority of total payment mix in 2020;
(b) mCommerce is expected to account for more than 60% of online payments;
(c) Of this percentage, a significant majority (over 75%) is predicted to be funded via stored card information;
(d) Entry of card information into a browser will reduce to represent 20% or less of transactions by 2020;
(e) As mobile device usage increases, authentication will shift towards more user friendly biometrics.

AusPayNet is therefore of the view that mandating a single solution would be sub-optimal since there are many possible solutions to cover all of the facets of fraud mitigation: fraud detection; cardholder authentication and the security of cardholder data.

In contrast, industry best-practice guidelines can address a range of potential solutions and implementation issues.

In addition, guidelines cover non-technical aspects, such as merchant choice, and the education of cardholders and merchants on prevention.

Another advantage of guidelines is the ability for them to be reviewed regularly by AusPayNet to ensure they remain relevant especially given predicted changes in the eCommerce space. Indeed, the guidelines need to enable the growing use of solutions such as tokenisation, online and in-app wallet services, and authentication techniques such as digital identity, geo-location, device proximity, biometrics and social media analytics.

5. PROPOSED SOLUTION – GUIDELINES

5.1 Guidelines Introduction and scope

(a) These Guidelines set out a range of best practices for Australian Card Issuers and Acquirers in relation to acceptance and processing of CNP transactions. They focus on the following main areas:

(i) Secure collection, storage and transmission of Card data;

(ii) Cardholder authentication;

(iii) Fraud detection;

(iv) Tokenisation;

(v) Cardholder and Merchant education on prevention.

(b) These Guidelines are intended to complement or improve existing systems and practices to further secure the CNP environment.

5.2 Objectives and Principles

(a) The Guidelines are intended to represent best practice for Card Issuers and Acquirers, enabling CNP Transactions to take place with minimal disruption to the Cardholder whilst managing the security of Card data.

(b) The Guidelines are not intended to, and do not, of themselves:

(i) affect the rights of any Card Scheme administrator to establish scheme rules in relation to CNP fraud management;

(ii) affect the right of any Card Issuer or Acquirer to exercise commercial freedom in the selection of third party service providers or partners;

(iii) affect the obligations of any Card Issuer or Acquirer as a subscriber to the ePayments Code or to its Cardholders more generally; or

(iv) affect the right of any Card Issuer or Acquirer to determine to apply different requirements or standards to those set out in the Guidelines.

(c) The Guidelines are technology neutral and are not to be construed as promoting, endorsing or impeding any particular fraud solution or service provider(s).

(d) AusPayNet does not enforce any Acquirer or Card Issuer's adoption or use of, or compliance with, these Guidelines.

(e) AusPayNet will monitor and review periodically these Guidelines to ensure they remain effective and relevant; particularly as global standards develop.

5.3 Glossary

In this document:

Acquirer means a body corporate which provides transaction acquiring services on behalf of a Merchant.

AFCX means the Australian Financial Crimes Exchange.

AusPayNet means Australian Payments Network Limited (ABN 12 055 136 519).

AS2805 means the authorisation protocol used in Australia for payment Card transaction messages.

Authentication means the act of confirming either a transaction or a person's identity is genuine and not originating from a fraudulent source.

BIN means the bank identification number allocated in accordance with ISO/IEC 7812.

Card means any payment Card, device, application or identifier provided by a Card Issuer, which is linked to an account or credit facility operated by them.

Cardholder means a customer of a Card Issuer who is issued with a Card and PIN or other authentication method or process.

Card Issuer means a body corporate which, pursuant to the rules of a Card Scheme, issues a Card to a Cardholder and, in connection with any Card transaction effected using that Card assumes obligations to the relevant Cardholder.

Card Scheme means the set of functions, procedures, arrangements and rules that enable a Cardholder to make payment transactions with a third party other than the Card Issuer. For the avoidance of doubt, a Card Scheme may be a three-party scheme or a four-party scheme.

CNP means card not present.

CNP Transaction means a transaction which is initiated by a Cardholder using a Card to make a purchase from a Merchant not in the same physical location. For example, over the internet (including via a mobile browser) or in app.

CVM means Cardholder Verification Method, used to evaluate whether the person presenting a payment instrument, such as a payment Card, is the legitimate Cardholder.

ePayments Code means the electronic payments code published by the Australian Securities and Investments Commission (ASIC), as amended from time to time.

EMV is the payment specification standard published by EMVCo that is used on electronic payment Cards incorporating an integrated circuit microchip.

EMVCo means EMVCo, LLC, the global technical body formed in 1999 that defines the standards for EMV payment Card processing.

FIDO Alliance means the Fast Identity Online Alliance, a not for profit organisation that develops standards for authenticating users of online services. Further information on the work carried out by the alliance can be found on their website: www.fidoalliance.org

Frictionless Authentication means Authentication without any interruption to the consumer during their online shopping experience.

IAC means the Issuers and Acquirers Community, AusPayNet's industry forum for the development and administration of industry standards and policy for card payments in Australia.

ISO means the International Standards Organisation, responsible for ISO 7812 for the issuance of payment Card ranges to individual organisations and ISO 8583 for systems that exchange electronic transactions made by Cardholders using payment cards and other payment standards.

Jailbroken Device means a smartphone or other electronic device where restrictions imposed by the manufacturer or operator were removed, allowing the installation of unauthorised software or application.

MCC means Merchant Category Code, used to classify the Merchant by the type of goods or services it provides.

Merchant means a trading entity that has an agreement with an Acquirer to process and settle their Card payment transactions.

PA DSS means Payment Application Data Security Standard for Card payment applications, as amended from time to time.

PAN means Primary Account Number. The number assigned by a Card Issuer to a debit or credit Card.

Payment Account Reference (PAR) provides a means by which systems that made use of the original PAN such as fraud pattern detection systems or a Merchant loyalty scheme can continue to be effective without the PAN data being available. PAR was introduced to the EMV Payment Tokenisation Technical Framework[4] to provide stakeholders in the payment value chain with a means by which they could link multiple payment tokens that reference back to one or multiple Cards.

PCI DSS means the Payment Card Industry Data Security Standard for Card transactions, as amended from time to time.

PCI SSC means the Payment Card Industry Security Standards Council, the overarching body responsible for producing payment Card security standards such as PCI DSS.

Phishing means the fraudulent practice purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit Card numbers, online.

POS means the Point Of Sale in a Card present environment, utilising a POS device where the customer pays.

Privacy Act means the *Privacy Act 1988 (Cth).*

Static Authentication means Authentication using a method, such as a code, that is unchanging and remains the same over multiple requests. Such codes are more vulnerable to compromise as they can be re-used by fraudsters.

[4] *EMV specification bulletin No.167, January 2016*

Token Requestor means an entity in the payment chain requesting the Token Service Provider to issue a token in place of a PAN. Merchants, Card Issuers, Digital Wallet providers or other parties can all perform the role of Token Requestor.

TSP means Token Service Provider, an entity that provides a token service, comprising a token vault and related processing, and which has the ability to use licensed ISO BINs as token BINs to issue payment tokens for PANs that are submitted in accordance with EMVCo's Payment Tokenisation Specification.

W3C means the World Wide Web Consortium, responsible for the development of global web standards. Further information on the work carried out by the consortium can be found on their website: www.w3.org

CARD ISSUER AND ACQUIRER BEST PRACTICE GUIDELINES

6. CARDHOLDER DATA AND ITS SECURITY

6.1 Protect Cardholder data

(a) Acquirers and Card Issuers should ensure the protection of the Cardholder's Card data during transactions. This includes during any correspondence, written or electronic, to prevent any unauthorised party gaining access to it. Where reference to the Primary Account Number (PAN) is required, a truncated version of it should be used where possible. Each Acquirer and Card Issuer should ensure that any third party service provider engaged in transaction processing also meets the requirements in this section.

(b) Each Acquirer should have a plan in place to ensure PCI DSS requirements are met by their online Merchants in accordance with PCI Data Security Standards v3.2 (published April 2016 and effective 1st February 2018).

(c) Each Acquirer and Card Issuer should aim to provide Merchants with solutions which will assist them in reducing their PCI SSC obligations such as tokenisation or hosted payment page solutions and to decrease the risk of Card data being lost or stolen.

(d) Each Acquirer and Card Issuer should consider the use of EMV payment tokens to protect the PAN in the environments in which payment tokens may be used. For further information on tokenisation, refer to section 4.

6.2 Maximise the use of available data

(a) It is noted that construction of the authorisation message (AS2805 / ISO8583) is based on data elements which effectively limit the data available to support authorisation. However, each Acquirer and Card Issuer should consider inclusion of additional information that could be used to assess the risk of a transaction. For example, Acquirers and Card Issuers should consider capturing information on the use and behaviour of the device initialising the payment to provide further input to decision making.

(b) Each Card Issuer should consider leveraging the data obtained between Cardholder application, authorisation and authentication systems so that each environment has as much visibility and data for assessing risk as possible.

(c) Each Card Issuer should consider leveraging the data available from cross-channel banking systems (such as mobile transaction banking application activity) to provide a broader view of any suspicious account activity when assessing each transaction request for risk.

(d) Each Acquirer and Card Issuer should consider the value of leveraging data sharing entities to detect and prevent further fraud through the sharing of data on compromised accounts or methods of operation. For example, AFCX has recently been established to facilitate information sharing.

(e) Each Card Issuer and Acquirer should consider the use of external data sources to validate the Cardholder such as the geolocation capabilities of Digital Wallets and/or the biometric and device proximity capabilities of smartphones.

6.3 Privacy – Treatment of data generated during transactions

(a) Compliance with the Privacy Act:

All entities which collect, use and disclose Cardholder personal information in Australia are bound by their respective obligations under the Privacy Act.

(b) Disclosure of transaction data to Card Issuer:

Acquirers should have effective arrangements in place with Merchants to ensure that they can lawfully disclose authentication and geolocation transaction data generated during a CNP Transaction to Card Issuers for effective investigation and resolution of CNP fraud events.

(c) Terms and Conditions on merchant website

Acquirers should ensure that merchant terms and conditions reflect these practices within their Merchant Services Agreements.

7. CARDHOLDER AUTHENTICATION

(a) The Card Issuer is responsible for determining the appropriate CVM and therefore should:

(i) ensure the CVM method selected for a Card is in accordance with any applicable Card Scheme rules;

(ii) avoid Static Authentication for Cardholders. Static Authentication is not recommended for CNP Transactions as unsuspecting Cardholders may disclose this information without knowledge, allowing the data to be re-used by unauthorised persons for subsequent transactions;

(iii) consider delivery of one time passcodes (OTPs) via a method other than SMS to reduce the threat of interception (e.g. digitally certified push notifications); and

(iv) if SMS is used, then additional controls should be in place to identify and/or mitigate the risk of intercepted SMSs.

(v) consider the use of additional fraud tools where OTP is delivered by SMS.

(b) Each Card Issuer should consider Frictionless Authentication to verify a transaction where possible, through the capture of data such as (but not limited to) device ID, geo-location, device proximity, Wi-Fi connectivity and time of day.

(c) In circumstances where messages are exchanged between Acquirers and Card Issuers to authenticate Cardholders:

(i) the Card Issuer should consider the implementation of access control servers that support enhanced data collection to perform risk based authentication using techniques such as device and user profiling;

(ii) the Card Issuer should ensure that where risk based authentication is in place, there is sufficient monitoring in place to ensure the risk scoring accuracy is upheld; and

(iii) the Acquirer and Card Issuer should also consider implementing industry standard message protocols for improved risk analysis to facilitate Frictionless Authentication and support multiple device form factors.

(d) Each Acquirer should encourage Merchants to implement a Risk Based Approach (RBA) to authenticating the Cardholder so as not to impact low risk transactions but to provide an additional level of verification for higher risk transactions.

(e) Each Card Issuer should consider the use of dynamic data that is stored outside of the integrated circuit or magnetic stripe on the Card and that could be included as part of the CNP authorisation message, for example data that can be provisioned via a Card Issuer smartphone application.

(f) Each Card Issuer should ensure that any third party vendors of authentication solutions support local Australian requirements (such as network selection for multi-network Cards).

(g) Each Card Issuer and Acquirer should consider making available cardholder authentication options for each individual payment channel including but not limited to POS terminals, internet and in app payment.

(h) Each Card Issuer and Acquirer should consider emerging online global standards currently under development. This includes (but is not limited to) the work being undertaken by the likes of W3C and the FIDO Alliance.

8. FRAUD DETECTION

(a) Each Acquirer and Card Issuer should ensure the integrity of the data provided in the authentication message is present and the data is verified as valid. As much of this data as possible should be captured by the fraud detection system to provide better visibility of the transaction scenarios.

(b) Each Acquirer and Card Issuer should make use of real-time fraud detection systems.

(c) Each Acquirer and Card Issuer should ensure sufficient monitoring of fraud detection systems is in place to maintain their effectiveness.

(d) Where feasible, each Acquirer and Card Issuer should make use of data available outside of the traditional authorisation message – such as unexpected variations to device ID history or non-financial events (e.g. recent change of account holder's phone number or address) – to profile each transaction request with increased accuracy and to highlight any potential risks.

(e) Each Acquirer and Card Issuer should consider the use of additional Card Scheme services that support network level analysis on transactional and other available data.

(f) The use of external data from telecommunication networks may also be leveraged by each Acquirer and Card Issuer as part of its risk assessment to validate whether the phone number of a Cardholder has been recently ported.

(g) Data sharing opportunities can allow for Card Issuers to be alerted by Merchants of any high risk transactions that may have been stopped by the Merchant's own fraud tools prior to it being sent to the Card Issuer. This data could be used to alert the Card Issuer should the same Card be attempted to be used to pay for goods at another Merchant that may be less prepared to identify the risk.

(h) In the same way defined in section 1.2, the Card Issuer should consider the use of shared data to alert Merchants of suspicious activity on, or the compromise of, specific Cards.

(i) Each Card Issuer and Acquirer should consider sharing any identified fraud data with the AFCX and/or other data sharing organisations to prevent fraudulent activity across different entities in the payment value chain.

(j) Each Card Issuer should consider the use of transaction history from other domains such as POS or telephone orders as well as cross channel banking activity in any risk scoring.

(k) Each Card Issuer and Acquirer should make use of validation services on specific data types to ensure details provided are not fictitious and are related to the Cardholder.

(l) Each Acquirer should consider promoting the benefits of real-time fraud detection approaches to their Merchants.

9. TOKENISATION

(a) Each Card Issuer and Acquirer should consider the use of payment tokens and benefit from a reduced risk of fraud exposure in the event of a Merchant data breach. It may also prevent the expense and inconvenience of needing to re-issue Cards and address Cardholder enquiries.

(b) Each Card Issuer should consider the following:

(i) To ensure the integrity of tokens is maintained, each Card Issuer should provision payment tokens limited for usage via individual devices, channels or Merchants. This includes (but is not limited to):

- Location, such as domestic country of issue, a list of allowed countries or select Merchants;
- Network – use of one token per payment network to facilitate the multi-network operations;
- Goods & services – the token may be restricted to be used for payments in only selected MCCs (i.e. travel, retail or financial services);
- Payment channel such as contact EMV (Card chip), NFC for contactless payments via mobile phone, or eCommerce (also referred to as “domains”);
- Device – use of one token per payment device e.g. smartphone, wearable, tablet or plastic Card; and
- Limiting the number of times a specific token can be used for payment.

(ii) EMV tokenisation services may be provided by one or more certified Token Service Provider (TSP) such as scheme, or the Card Issuer may choose to implement a token provisioning platform of their choice. Card Issuers should take into consideration:

- Certification efforts with the various stakeholders in the payments value chain (Card Schemes, Acquirers, TSPs and others); and,
- Tokenisation at the farthest point possible in the payment chain (the Card Issuer) eliminates the exposure of the PAN to all other entities thus reducing the impact of any Merchant data breach.

(iii) Card Issuers and Acquirers should ensure that the PAR Data is passed in all relevant token and transaction messages to ensure the integrity and efficacy of fraud detection systems as Cardholder data is replaced by one or more payment tokens.

(c) Where the Acquirer or Card Issuer fulfils the role of the Token Requestor the level of appropriate Cardholder authentication during enrolment should be carefully considered.

10. CARDHOLDER EDUCATION AND MERCHANT FRAUD PREVENTION

(a) Card Issuers should use reasonable endeavours to educate their Cardholders around the risks of CNP Transactions, both in app and online. Cardholders should be given clear and accessible information in relation to:

(i) protection of the device(s) used to make remote purchases e.g. PC, smartphone, tablet etc. This should include topics such as exercising caution around the installation of unknown applications to reduce the risk of malware, anti-virus protection, and the use of Jailbroken Devices. Information should also cover the impact these can have to the Cardholder's security and data privacy;

(ii) enrolment in any authentication solution provided by the Card Issuer;

(iii) potential techniques used by fraudsters to obtain personal and financial details and how best to avoid them (e.g. only providing their Card details on secure websites, avoiding following links sent via SMS or email, Phishing techniques and identity theft);

(iv) the potential risks of placing purchases at non-reputable or unfamiliar websites; and

(v) the importance of regularly checking industry led initiatives, such as education forums about online safety to keep abreast of current developments.

(b) Acquirers should pro-actively educate their Merchant customers about online fraud and techniques available to combat it. In particular, Acquirers should focus on those MCCs that are exposed to a high risk of fraud and make use of available resources such as those available on AusPayNet's website e.g. "Get smart about Card fraud online.

(c) Acquirers should endeavour to provide alerts to their Merchants if vulnerabilities become known to applications, systems, processes or other components used in the Merchant operating environment to prevent further loss of Cardholder data.

(d) In the absence of a Merchant-owned fraud detection and prevention strategy, Acquirers should encourage their Merchant customers to adopt suitable fraud detection and authentication solutions offered by their chosen payment service provider.

(e) Acquirers should consider the benefits of educating Merchants around their selection of third party providers of online products such as shopping cart software. Acquirers and Merchants should focus on ensuring that product vendors meet PCI SSC standards, such as PCI DSS and PA DSS.