Third party digital wallet security: Card Issuer guidelines

24 May 2016

About this document

These Guidelines have been prepared by the Australian Payments Clearing Association Limited.

Contact

APCA
Email: digitalwallets@apca.com.au
Level 6, 14 Martin Place
Sydney NSW 2000

Publication

Written and published in Sydney, Australia by the Australian Payments Clearing Association Limited.

Amendment Certificate

Version	Date	Author / Comments
1.0	24 May 2016	APPROVED for publication

Best practice guidelines for Card Issuers in relation to third party mobile wallet security

A. CONTEXT

Introduction

APCA is Australia's peak payments industry association. We work with our members and other payments industry stakeholders to identify and manage security risks in payment systems and payment technologies.

APCA supports payments technology innovation that meets Australian security requirements and that preserves consumers' confidence and trust in the payments system. Mobile banking and payment services, mobile / digital wallets and third party digital wallets are emerging features of the global and Australian payments landscape that potentially offer significant consumer benefits.

Digital or mobile wallets are software applications on consumer devices which act as a repository for payment and other cards, and which by provisioning encrypted payment card data, effectively enable 'card present' mobile payment transactions at POS and in application. Third Party Digital Wallets are those which may be provided by a third party using multiple Card Issuers' payment Card data, customer relationships and existing payment networks, as well as various intermediaries and service providers. Australians are well-served by a robust consumer protection framework for mobile banking and mobile payment services - the *ePayments Code* – which attributes primary liability for unauthorised transactions made by use of such facilities to the Card Issuer subscriber which has promoted or endorsed that facility, even where the liability might be attributable to another party in the shared network.

These Guidelines have been issued by APCA as *industry best-practice* to help Card Issuer members of the IAC to understand and proactively manage potential fraud and security risks in the provision of Third Party Digital Wallet services. They are voluntary.

As an adjunct to the Guidelines, APCA will periodically convene open mobile payments industry fora, develop publications and white papers and invite consultation to promote understanding of, and consider developments in, mobile payments security and fraud management issues.

B. SCOPE

The Guidelines focus on the issues which typically require consideration by a Card Issuer in the context of provisioning its Cards to third party mobile wallets, including customer identification and verification, authentication of transactions and management of token generation and Card data security.

These Guidelines are not intended to address the issues of liability apportionment between Cardholders, Card Issuers, Digital Wallet Providers and other parties to a

Third Party Digital Wallet transaction: this is a proprietary matter for parties to resolve.

The Guidelines do not apply to software applications that process payments solely using card-on-file data provided directly by a Cardholder to the payment service provider, where 'card-not-present' liability arrangements apply.

The Guidelines have not been drafted to apply to Card Issuers' proprietary mobile banking applications or proprietary wallet services, being those provided by a Card Issuer solely for its own customers. The responsibility for managing fraud and security of proprietary wallet services, and the liability for, and reputational risk associated with, losses resulting from use of proprietary products, rests entirely with the Card Issuer. A Card Issuer may choose to apply aspects of these Guidelines to its proprietary mobile banking applications and wallet services where appropriate.

C. OBJECTIVES

1. The purpose of the Guidelines is to assist Card Issuers with establishing their respective security and data privacy requirements for Third Party Digital Wallets to promote the integrity and security of these services.

2. The Guidelines are voluntary and are intended to represent industry best practice for security and tokenisation of mobile payment transactions and for privacy and limited permitted disclosure of Cardholder and mobile payments data.

3. The Guidelines are not intended to, and do not, of themselves:

    (a) presume, affect or prescribe the terms of any arrangement established by any Card Issuer with any Digital Wallet Provider/s;

    (b) affect the rights of any Card Scheme administrator to establish scheme rules for provisioning its co-branded Cards to Digital Wallets or the obligations of any Card Issuer under those rules;

    (c) affect the right of any Card Issuer to exercise commercial freedom in the selection of mobile payments services processors and partners;

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

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

4. The Guidelines are technology neutral and are not to be construed as promoting, endorsing or impeding any particular service provider/s.

5. Card Issuers are encouraged to promote awareness of the Guidelines amongst Digital Wallet Providers, Card Scheme administrators, and other participants in the provision of Digital Wallet services.

6. Card Issuers are encouraged to ensure that the provisioning of Cards to a Third Party Digital Wallet does not affect or derogate from the intrinsic capabilities and functions of Cards, or any priority network arrangement that applies to them.

7. APCA does not monitor or enforce any Card Issuer's adoption or use of, or compliance with, these Guidelines.

8. APCA will periodically review these Guidelines to ensure they remain effective and relevant, particularly as international standards for mobile payments develop, and may amend them from time to time.

D. GLOSSARY

In this document:

APCA means Australian Payments Clearing Association Limited (ABN 12 055 136 519).

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

Card means any card, device, application or identifier provided by an Issuer, which is linked to an account or credit facility with the Card Issuer.

Cardholder means a customer of an 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, which obligations are in the first instance discharged on its behalf by an acquiring institution.

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.

CVM means Cardholder verification method.

Digital Wallet means a software application on a digital device that:

(a) functions as a digital container for payment Cards, tickets, loyalty cards,

receipts, vouchers and other forms of payment; and

(b) provisions and uses the encrypted Card data associated with an enrolled payment Card.

For the avoidance of doubt, a software application that processes payments solely using 'card on file' data is not a Digital Wallet for the purposes of these Guidelines.

Digital Wallet Provider means a body corporate which is a third party provider of Digital Wallet services to its, and a Card Issuer's, mutual customers/Cardholders.

ePayments Code means the electronic payments code published by ASIC, as amended from time to time.

EMV Card means a Card issued by a Card Issuer that contains an integrated circuit that conforms to EMV specifications, in respect of which the EMV Issuer Country Code data element (tag 5F28) is equal to "036".

IAC means the Issuers and Acquirers Community constituted by the Regulations.

ID&V means identification and verification.

PAN means primary account number.

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

Regulations mean the regulations for the IAC, as prescribed by APCA, as amended from time to time.

Third Party Digital Wallet means a Digital Wallet that is provided by a Digital Wallet Provider.

TSP means 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 EMV Co's *Payment Tokenisation Specification*, version 1.0 (March 2014).

Guidelines

1 Security

1.1 Customer identification and authentication on enrolment

(a) The Card Issuer is responsible for making the decision as to whether a particular Card can be enrolled in a Third Party Digital Wallet.

(b) The Card Issuer is responsible for determining appropriate ID&V methods and the data elements required to support enrolment of its Cards into Third Party Digital Wallets. In determining appropriate ID&V levels, the Card Issuer should have regard to the following criteria:

(i) Enrolment ID&V for Third Party Digital Wallets should achieve levels of security that are, as a minimum, equivalent to ID&V used in the Card Issuer's proprietary digital wallets and/or Card Issuer mobile banking applications;

(ii) any 3D Secure processing standards which may apply (if a Card-based ID&V process is to be used); and

(iii) any relevant global industry best practices for ID&V.

(c) The Card Issuer may outsource key parts of its ID&V process to a third party (including the Digital Wallet Provider), but should ensure the third party meets the requirements in this section 1.1.

(d) The Card Issuer may authorise the enrolment of a particular Card in more than one Third Party Digital Wallet.

1.2 Customer authentication at the time of transaction

(a) The Card Issuer is responsible for determining the appropriate CVM for authenticating transactions made using the Card Issuer's issued Cards in accordance with any relevant Card Scheme rules in place for those Cards. To the extent the Card Issuer has the right to exercise discretion when determining appropriate CVMs, the Card Issuer should do so having regard to the following criteria:

(i) CVM for transactions in Third Party Digital Wallets must achieve levels of security which are as a minimum equivalent to CVM for transactions made using EMV Cards;

(ii) industry best practice; and

(iii) any list of CVMs that may have been approved by APCA for Card payments in Australia.

(b) The Card Issuer should not use a CVM which is:

(i) inconsistent with the CVMs prescribed by the relevant Card Scheme rules applicable to the Card; or

(ii) not in APCA's approved list of CVMs for Card payments in Australia.

(c) The Card Issuer may outsource key parts of the CVM process for Third Party Digital Wallet transactions to a third party, but should ensure the third party meets the requirements in this section 1.2.

2 Tokenisation

2.1 Use of Tokenisation Services

(a) Tokenisation is not compulsory for transactions made using a Third Party Digital Wallet if the Third Party Digital Wallet includes an embedded secure element solution. In this case, it is up to the Card Issuer to decide if tokenisation services are appropriate for Third Party Digital Wallet transactions made using the Card Issuer's issued Cards.

(b) Tokenisation should be used for transactions made using a Third Party Digital Wallet if:

(i) mandated by applicable Card Scheme rules; or
(ii) the Third Party Digital Wallet does not include an embedded secure element solution.

2.2 Selecting Tokenisation Services

(a) The Card Issuer is responsible for selecting token service provider/s, and may choose the tokenisation services of any TSP or supply its own tokenisation service, provided the chosen service conforms to the minimum standards prescribed by section 2.3.

(b) The Card Issuer may choose to use the tokenisation services of more than one TSP.

2.3 Minimum standards

The Card Issuer should ensure that any TSP it engages to provide tokenisation services meets the minimum standards set out in EMVCo's *Payment Tokenisation Specification – Technical Framework*, version 1.0 (published March 2014).

3 Privacy – Treatment of data generated during transactions

3.1 Compliance with Privacy Act

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

3.2 Disclosure of Transaction Data to Card Issuers

It is advisable that the Card Issuer has effective arrangements in place to ensure that Digital Wallet Providers and, if applicable, other parties in a shared mobile payments network:

(a) have obtained Cardholders' informed consent to the disclosure of any authentication data and any geolocation data which may be collected by that Digital Wallet Provider or party in relation to a transaction effected using a Third Party Digital Wallet; and

(b) will disclose such information to the Card Issuer if it reasonably requests such information, from time to time, for the purposes of investigation and resolution of fraud, disputed and unauthorised transactions and Cardholder complaints.