Australian Payments Network

Issuers and Acquirers Community

Device Approval Process

Version 2.0

Issuers and Acquirers Community Device Approval Process

Version No: 2.0
Effective: 25 March 2022

Table of Contents

Change History

Version	Effective Date	Change
1.0	16/12/2021	Approved by the IAF – 25 November 2021
2.0	25/03/2022	Endorsed by the IAF – 3 March 2022 Enabling Registration via Structured Risk Assessment for non-standard technologies and various other amendments.

PART 1 INTRODUCTION

1.1 Operation

This document sets out the Australian Payments Network's (the Company) process for approval of Devices, Solutions, and Non-Standard Technologies and the requirements for Device Approval Applicants. This document operates as follows:

(a) It does not form part of the IAC Code Set and may be varied by the Chief Executive Officer without the need to obtain the approval of the IAF or any other person.

(b) By submitting an approval application or a delta approval application, a Device Approval Applicant agrees to comply with the applicable terms of this document as in force on the date the application was lodged and, where relevant, ensure the Vendor (or any other relevant third party) provides any necessary information and cooperation required for the Device Approval Process.

1.2 Interpretation

(a) The words defined in Part 1.3 of the IAC Code Set Volume 4 have the same meaning in this document unless a contrary intention appears. Where there is an inconsistency between a definition reproduced below and a definition in the IAC Code Set, the IAC Code Set definition will prevail. The following definitions are reproduced from the Code Set:

(i) "**Approval Period**" means the period of approval for a Device, Solution or Non-Standard Technology as stated in the Letter of Approval or otherwise notified by the Company to a Device Approval Applicant.

(ii) "**Approved Device**" means a Device, Solution or Non-Standard Technology that has been approved for use within the IAC by the Company in accordance with clause 3.1 of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management;

(iii) "**Approved Devices List**" means the list of Approved Devices published on the AusPayNet website.

(iv) "**Device**" means a device used for payment acceptance, transfer of keys or processing of cryptographic data. This includes but is not limited to a Secure Cryptographic Device

(v) "**Device Approval Applicant**" means the applicant seeking approval of a Device, Solution or Non-Standard Technology in accordance with the Device Approval Process.

(vi) "**Device Approval Process**" means the process for approval of Devices, Solutions and Non-Standard Technology published by AusPayNet on its website, as updated from time to time. To avoid doubt, the Device Approval Process is not an operative part of the IAC Code Set and may be varied by the Chief Executive Officer without the need to obtain the approval of the IAF or any other person

(vii) "**Letter of Approval**" means a letter, issued by the Company, approving the use of a Device, Solution or Non-Standard Technology within IAC or any other notification of device approval contemplated in the Device Approval Process.

(viii) "**Non-Standard Technology**" means a Device, Solution or other technology that by nature of its design is unable to meet accepted standards defined in the Device Approval Process.

(ix) "**Solution**" means wholly infrastructure-based methodology used for payment acceptance, transfer of keys or processing of cryptographic data.

(b) Words that are capitalised but not defined in Part 1.3 of the IAC Code Set Volume 4 have the following meaning:

(i) **Accepted Standards** means the following documents and all published annexures:

(A) Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements;

(B) Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Security Requirements;

(C) Payment Card Industry (PCI) Contactless Payments on COTS (CPoC) Security and Test Requirements;

(D) Payment Card Industry (PCI) Software-Based PIN Entry on COTS (SPoC) Security Requirements;

(E) Payment Card Industry (PCI) Software-Based PIN Entry on COTS (SPoC) Test Requirements.

(ii) **Application for Registration** means the application form published on the Company's website from time to time for registration in accordance with this document.

(iii) **Approved Standards Entity** means PCI SSC.

(iv) **Attestation of Compliance** means a digitally signed statement (including a letter of approval or an attestation of validation) from an Approved Standards Entity confirming compliance to an Accepted Standard.

(v) **Delta Registration** means registration of an Approved Device following approval by an Approved Standards Entity of changes to an existing Approved Device

(vi) **Documentation Pack** means the system documentation, scheme reports, other laboratory reports, internal testing results and any other documents requested by the Company under the Structured Risk Assessment Process.

(vii) **NST Process** means the Company's approval process for Non-standard Technology applicable prior to the introduction of the Structured Risk Assessment Process and described as 'Process for Considering Non-Standard Technologies'.

(viii) **Pilot** means deployment of a Device, Solution or Non-Standard Technology, assessed under the Structured Risk Assessment Process to have security vulnerabilities requiring mitigation prior to

consideration of registration, for a defined period of time and subject to certain conditions detailed in the Pilot Letter.

(ix) **Pilot Letter** means a letter, issued by the Company, detailing the terms and conditions of the Pilot.

(x) **Registered Device** means a Device, Solution or Non-Standard technology which is approved via the registration process set out in this Device Approval Process.

(xi) **SRA** means a structured risk assessment undertaken as part of the Structured Risk Assessment Process.

(xii) **SRA Questionnaire** means the request for information provided by the Company to the Device Approval Applicant under the Structured Risk Assessment Process.

(xiii) **SRA Tool** means the Company's proprietary tool to undertake SRA.

(xiv) **Structured Risk Assessment Process or SRA Process** means the process outlined in Annexure A to this document for evaluating Devices, Solutions and Non-Standard Technology that do not have an Attestation of Compliance.

(xv) **Vendor** means the Device, Solution or Non-Standard Technology manufacturer.

1.3 Purpose

Part 1.1 of IAC Code Set Volume 4 states that the purpose of the IAC is to develop, implement and operate effective standards, policies, and procedures to promote the efficiency, security and integrity of Australian Card Payments. In the context of Approved Devices, that purpose includes balancing the interest of maintaining the security and integrity of Australian Card Payments with the interest of promoting innovation and competition.

PART 2 APPROVAL PROCESS, DEVICE APPROVAL APPLICANTS AND REGISTERED DEVICES

2.1 Approval Process

The Company may approve a Device, Solution or Non-Standard Technology (including a delta application of an Approved Device) for the purpose of IAC Code Set either through:

(a) Registration with an Attestation of Compliance described in Part 3 below; or

(b) Registration via the Structured Risk Assessment Process described in Part 4 below.

2.2 Device Approval Applicant

The Device Approval Applicant:

(a) for Registration with an Attestation of Compliance, may be the Acquirer, Third Party Provider, Device manufacturer or any third party; or

(b) for Registration via the Structured Risk Assessment Process must be the Acquirer.

2.3 Approved Devices

An Approved Device for the purpose of the IAC Code Set includes:

(a) a Registered Device from the date of the Letter of Approval; and

(b) a Device, Solution or Non-Standard Technology in Pilot in accordance with the Pilot Letter.

2.4 Term of Approval

An Approved Device:

(a) will remain approved, subject to clause 5.5, for the Approval Period stated in the Letter of Approval or the term of the Pilot as stated in the Pilot Letter; and

(b) may be renewed, if required, as set out in clause 6.

2.5 Transition period

Where an application for approval of a non-standard technology commenced under the NST Process and a decision has not been provided by the Company at the date of publication of Device Approval Process version 2.0:

(i) the application will transition to an application for registration via the Structured Risk Assessment Process;

(ii) the Company and the Device Approval Applicant will agree the process for transition relative to the maturity of the NST Process application and the requirements under the SRA Process.

PART 3 REGISTRATION WITH AN ATTESTATION OF COMPLIANCE

3.1 Operation of this clause 3

A Device Approval Applicant may apply to the Company for registration of a Device, Solution or other technology which has an Attestation of Compliance in accordance with this clause 3.

3.2 Application for Registration with Attestation of Compliance

The Device Approval Applicant must submit to the Company via email (PAG@auspaynet.com.au) an Application for Registration and the relevant Attestation of Compliance.

3.3 Check validity of Attestation of Compliance

The Company will examine the Attestation of Compliance for validity, including, by reviewing the Attestation of Compliance:

(a) against the relevant Accepted Standard current at the date of the Application for Registration; and

(b) the Approved Standards Entity's list of approved devices.

The Company does not examine to determine if the Device or Solution is EMV certified.

3.4 Confirmation of registration and publication of registration on website

If the Application for Registration is complete and the Attestation of Compliance is validated in accordance with clause 3.3, within six weeks of receiving the Application for Registration, the Company will:

(a) issue to the Device Approval Applicant a Letter of Approval as described in clause 5.1(a); and

(b) publish the Approved Device on the Approved Devices List, setting out the minimum details contained in the Letter of Approval.

If the Application for Registration is not complete or the Attestation of Compliance is not validated the Company may decline the application and notify the Device Approval Applicant as provided in clause 5.4.

3.5 New Registration for new version of Accepted Standard

Any Attestation of Compliance issued against a new version of an Approved Standard for a previously Approved Device must be submitted to the Company with a new Application for Registration under this Part 3.

PART 4 REGISTRATION VIA THE STRUCTURED RISK ASSESSMENT PROCESS

4.1 Operation of this clause 4

A Device Approval Applicant may apply to the Company for registration of a Device, Solution or Non-standard Technology that does not have an Attestation of Compliance under the Structured Risk Assessment Process in accordance with this Part 4 and Annexure A to this document.

4.2 Application for Registration via the Structured Risk Assessment Process.

The Device Approval Applicant must submit to the Company via email (PAG@auspaynet.com.au) an Application for Registration.

4.3 Structured Risk Assessment Process

Subject to clause 4.5 below, if the Application for Registration is complete, the Company will undertake the Structured Risk Assessment Process outlined in Annexure A.

4.4 Notification of decision and publication

The Company will:

(a) notify the Device Approval Applicant in writing of its decision as provided in clause 5 below; and

(b) where a Device, Solution or Non-Standard Technology is registered or is approved for Pilot, publish, as appropriate:

  (i) on the Approved Devices List, the Approved Device, setting out the minimum details contained in the Letter of Approval, or

  (ii) on the extranet, details of the Pilot setting out the name of the Device Approval Applicant, the device, solution or non-standard technology accepted for Pilot and the term of the Pilot.

4.5 Repeat applications

If an application for Registration via SRA of a Device, Solution or Non-Standard Technology has been declined, as provided in clause 5.4 below, the Company will only accept a repeat application and undertake the SRA Process again if the Device Approval Applicant can demonstrate a documented change in the security landscape or change in the Device, Solution or Non-Standard Technology justifying, in the Company's absolute discretion, reconsideration of one or more of the reasons for the Company's original decision.

PART 5 DECISIONS

5.1 Approval

(a) If the Company approves for registration a Device, Solution or Non-Standard Technology (including delta approval), the Company will issue a Letter of Approval to the Device Approval Applicant, in a form to be determined by the Company from time to time, but such letter will contain at a minimum:

  (i) the name of the Device Approval Applicant;

  (ii) the Approved Device;

  (iii) the registration date;

  (iv) the Approval Period; and

  (v) the conditions, if any, associated with the approval.

(b) If the Company approves for Pilot a Device, Solution or Non-Standard Technology, the Company will issue a Pilot Letter to the Device Approval Applicant, in a form to be determined by the Company from time to time, but such letter will contain at a minimum:

  (i) the name of the Device Approval Applicant;

(ii) the Device, Solution or Non-Standard Technology approved for Pilot;

(iii) the security vulnerabilities identified in the SRA Assessment Report that are required to be mitigated before the technology can be registered;

(iv) the term of the Pilot; and

(v) the conditions of the Pilot including the liability shift to the Acquirer in accordance with the Structured Risk Assessment Process.

5.2 Approval Period – Registered Devices

Subject to clause 5.5 below, the Approval Period for Registered Devices will be as specified below:

(a) For Registered Devices with an Attestation of Compliance, the Approval Period will be from the date of registration to the expiry date noted on the Attestation of Compliance, or such further expiry date as the Approved Standards Entity subsequently determines.

(b) For Registered Devices via the Structured Risk Assessment Process, the Approval Period will be five years from the date of registration, or such other period as determined by the Company.

5.3 Outcomes from Pilot

Following completion of a Pilot, or in response to a request from the Device Approval Applicant at any stage during a Pilot, if agreed to by the Company in its absolute discretion, the Company will:

(a) repeat the SRA; and

(b) decide whether to accept the Device, Solution or Non-Standard Technology for registration in accordance with the SRA Process.

5.4 Decline

If the Company declines to approve a Device, Solution or Non-Standard Technology (including delta approval), the Company will notify the Device Approval Applicant in writing of the reasons for its decision, including the details of the unacceptable results.

5.5 Revocation

(a) Approval of Devices or Solutions approved before 16 December 2021, or Registered Devices with an Attestation of Compliance, may be revoked by the Company prior to expiry of the Approval Period if approval of the Device or Solution or underlying technology has been withdrawn or revoked by an Approved Standards Entity.

(b) The Company may:

(i) having regard to changes in security technology, applicable standards, security threats and/or other knowledge of security issue conduct periodic assessments of any Approved Device that does not have an

Attestation of Compliance as and when the Company (in its absolute discretion) deems appropriate; and/or

(ii) revoke approval for any Approved Device that does not have an Attestation of Compliance prior to the expiry of the Approval Period if the Company assesses (in its absolute discretion) that the Approved Device is vulnerable to a significant security threat and determines that the Approved Device should no longer be approved.

(c) If the Company revokes an approval prior to expiry of the Approval Period, the Company will:

(i) notify the Device Approval Applicant in writing of the reasons for its decision; and

(ii) remove the Approved Device from the Approved Devices List or the extranet (as applicable).

PART 6 RENEWAL OF DEVICE APPROVAL

6.1 Registered Devices with an Attestation of Compliance

(a) The registration of a Registered Device will continue for as long as the Attestation of Compliance remains in effect pursuant to clause 5.2(a).

(b) If the Attestation of Compliance for a Registered Device is no longer valid the Company will notify the Device Approval Applicant and will remove the Approved Device from the Approved Devices List. An Acquirer may apply to the Company under the Exemption Process in Volume One Part 3.3 to continue to use the Device or Solution.

(c) If an Attestation of Compliance is issued against a new version of an Approved Standard, the registration process in Part 3 will apply, pursuant to clause 3.7.

6.2 Renewal process for Registered Devices via the Structured Risk Assessment Process and Approved Devices under the NST Process

(a) Prior to expiry of the current Approval Period, the Company may in its sole discretion:

(i) conduct a period check as outlined in clause 5.5(b)(i); and

(ii) extend the Approval Period for a period of five years or such other period as the Company deems appropriate having considered the current security landscape, security threats and risk exposures; or

(iii) require that an Approved Device under the NST process proceed through the SRA Process by submitting an Application for Registration.

(b) If the Approval Period is extended, the Company will:

(i) send the Device Approval Applicant an updated Letter of Approval including the new Approval Period; and

(ii) update the Approved Devices List.

(c) If the Approval Period is not extended, the Company will notify the Device Approval Applicant in writing including the reasons for not extending the approval and will remove the Approved Device from the Approved Devices List.

6.3 Renewal process for Approved Devices under the standard device approvals process in force prior to December 2021

(a) If the Approved Device is covered by an Attestation of Compliance:

(i) the Company will register the Approved Device as a Registered Device upon receipt of an Application for Registration and validation of the Attestation of Compliance following the process specified in clause 3.2;

(ii) any existing deployment conditions or additional security requirements beyond the Attestation of Compliance attached to the approval of the Approved Device prior to this renewal will no longer apply;

(iii) the Approval Period for the Registered Device will align with the period of approval of the current Attestation of Compliance;

(iv) the Company will send the Device Approval Applicant an updated Letter of Approval, advising the registration date and the Approval Period and noting the removal of any previous deployment conditions; and

(v) the Company will update the Approved Devices List to reflect the current Letter of Approval.

(b) If the Approved Device is not covered by a current Attestation of Compliance prior to expiry of the current Approval Period the Company may in its sole discretion:

(i) conduct a period check as outlined in clause 5.5(b)(i); and

(ii) extend the Approval Period for such period as the Company deems appropriate having regard to changes in security technology, applicable standards, security threats and/or other knowledge of security issues; or

(iii) require that the Device or Solution be renewed by submitting an Application for Registration and following the SRA Process.

(c) If the Approval Period is extended, the Company will:

(i) send the Device Approval Applicant an updated Letter of Approval including the new Approval Period; and

(ii) update the Approved Devices List.

(d) If the Approval Period is not extended, the Company will notify the Device Approval Applicant in writing including the reasons for not extending the approval and remove the Approved Device from the Approved Devices List.

PART 7 DISPUTE RESOLUTION PROCESS

7.1 Reviewing a decision

(a) The Device Approval Applicant or Acquirer may request review of a Company decision.

(b) Any request for review must be made to the Company, in writing, within 30 days of the Company's notification to the Device Approval Applicant. The request must properly detail the reasons for the requested review, including by reference to the Company's reasons for its decision.

7.2 Company response

Within a reasonable period after receiving the request for review (reasonableness to depend upon the subject matter of the review request), the Company must review and respond in writing to the request for review and may request the parties must meet to resolve the dispute.

PART 8 GOVERNANCE

8.1 Review

The Company will review this Device Approval Process at least annually.

Annexure A: Structured Risk Assessment Process

A1. Process for registration of Non-Standard Technologies

A1.1 SRA Steps

By way of summary, the SRA contains the following stages:

(a) Identification:

i. The Company issues to the Device Approval Applicant an SRA Questionnaire.

ii. Upon receiving the completed SRA Questionnaire, the Company identifies, and then requests from the Device Approval Applicant, a Documentation Pack, listing the information required by the Company to undertake an SRA, together with a Vendor Consent and a Non-Disclosure Agreement.

(b) Review

Following receipt of the documentation the Company meets with the Device Approval Applicant to review the material provided.

(c) SRA:

The Company uses the SRA Tool to undertake the SRA and produce an Assessment Report.

(d) Decision:

i. The Company determines on the basis of the Assessment Report whether the Device, Solution or Non-Standard Technology should be:
   - Registered
   - Registered with Conditions
   - Accepted for Pilot
   - Declined.

ii. Devices, Solutions and Non-Standard Technology that are registered (with or without conditions) or accepted for Pilot are Approved Devices for the purpose of the Code Set.

A1.2 Application for Registration and SRA Questionnaire

(i) Every Application for Registration via the Structured Risk Assessment submitted in accordance with the Device Approval Process will be reviewed by the Company.

(ii) If the Application for Registration is complete, the Company will issue to the Device Approval Applicant an SRA Questionnaire.

(iii) The Device Approval Applicant must complete the SRA Questionnaire and forward it to the Company to enable the Application for Registration to proceed.

A.1.3 Document Pack, Vendor Consent and Confidentiality Agreement

(i) The Company will review the completed SRA Questionnaire and determine what documentation is required to undertake the SRA including, as appropriate, a letter of approval from other regions, scheme letter of approvals, scheme testing reports, other testing reports or any other document (**Documentation Pack**).

(ii) The Device Approval Applicant must submit:

(A) all documents identified in the Documentation Pack;

(B) the Vendor's Consent (in such form as required by the Company from time to time); and

(C) a Confidentiality Agreement (in such form as required by the Company from time to time).

(iii) These documents must be returned to the Company within four months from the date the Company issues them.

(iv) If the documents required are not received by the Company within that time, the Application for Registration will lapse unless the Company has granted an extension or a waiver (in its absolute discretion).

(v) Following any lapse in an Application for Registration, the Device Approval Applicant must submit a new Application for Registration under the Device Approval Process if it wishes to recommence the application process.

A.2. Structured Risk Assessment

A 2.1 Review Meeting

(a) The Company will analyse the SRA Questionnaire and Documentation Pack to determine the:

(i) system components;

(ii) vulnerabilities;

(iii) applied mitigants;

(iv) data asset flow; and

(v) any other information relevant to the assessment of the Device, Solution or Non-Standard Technology.

(b) The Company will schedule a Review Meeting with the Device Approval Applicant to discuss the SRA Questionnaire and the Documentation Pack.

(c) Following the Review Meeting, the Company may issue the Device Approval Applicant with a request for additional documentation. The Device Approval Applicant must respond to the Company's request within two months to enable the Application for Registration to proceed.

A.2.2 SRA

(a) The Company or a third party nominated by the Company will undertake the SRA using the Company's SRA Tool.

(b) The Company will apply the SRA Tool to calculate the exposure for each data asset flow element. The Company will provide information about the SRA methodology on request from the Device Approval Applicant.

A.2.3 SRA Assessment Report

(a) The Company will produce an Assessment Report identifying the exposure calculations for each data asset flow element and the SRA Risk Rating.

(b) The Company will determine the SRA Risk Rating based on an assessment of the totality of exposure calculations, considering the types of exposures disclosed and the scalability of risk, and a consideration of the risk rating principles in Table 1 below.

Table 1 Risk Rating Principles

Risk Ratings	Guiding Principles
Low	1. Data assets are not exposed to known vulnerabilities. 2. Mitigations for system components vulnerabilities are mitigated appropriately. 3. Mitigations are verified by third party testing.
Medium	1. Data assets are exposed to some vulnerabilities. 2. System component vulnerabilities are not adequately mitigated. 3. Data assets are exposed to non-scalable vulnerabilities. 4. System component vulnerabilities are subjected to complex attacks with limited data asset exposure.
High	1. System component vulnerabilities are subjected to non-complex attacks. 2. Data assets are exposed to scalable vulnerabilities. 3. Compromise of data assets will lead to a significant scale of fraud.

A.3. Decision

A.3.1 Low risk assessment

If the Company determines on the outcome of the SRA that the Device, Solution or Non-Standard Technology is low risk the Company will:

(a) accept the device for registration;

(b) send to the Device Approval Applicant a Letter of Approval in accordance with clause 5 of the Device Approval Process; and

(c) publish the Approved Device on the Approved Devices List.

A.3.2 Medium risk assessment

If the Company determines on the outcome of the SRA that the Device, Solution or Non-Standard Technology is medium risk:

(a) the Company may accept the device for registration with conditions and will:

(i) send to the Device Approval Applicant a Letter of Approval in accordance with clause 5 of the Device Approval Process detailing the applicable conditions; and

(ii) publish the Approved Device on the Approved Devices List; or

(b) where the SRA Assessment Report identifies security vulnerabilities the Company may accept the Device, Solution or Non-Standard Technology on a pilot basis and will:

(i) send the Device Approval Applicant a Pilot Letter detailing the pilot conditions as described in clause 5.1(b) below; and

(ii) publish details of the Pilot on the Extranet.

A.3.3 High risk assessment

If the Company determines, on the SRA Assessment Report, that the Device, Solution or Non-Standard Technology is high risk, the Company will decline the Application for Registration in accordance with clause 5.4 of the Device Approval Process.

A.4. Timing and costs

A.4.1 Timing

The Company will endeavour to complete the SRA Process within two months from receipt of all the documentation referred to in clause A.1.3 above. The actual timing will depend largely on the period of time the Device Approval Applicant takes to respond to requests for information from the Company, the complexity of the solution, and the quality of documentation received.

A.4.2 Costs

The Device Approval Applicant agrees to accept reasonable external costs associated with the device evaluation. The Company will determine what external costs are required. These costs may include technical security consulting and system testing by a specialised testing company. The Company will provide an estimate of any such costs and the Device Approval Applicant must accept the costs prior to the Company incurring them. If the Device Approval Applicant does not agree with the Company's decision on the external costs required or the estimate of external costs, the Device Approval Applicant can request a review under clause 7.1 above.

A.5. Pilot

A.5.1 Pilot Letter and Conditions for Pilot

(a) The Pilot Letter will:

(i) identify the security vulnerabilities disclosed in the SRA Assessment Report that are required to be mitigated before the technology could be considered for registration; and

(ii) detail the conditions of the Pilot in accordance with paragraph (b) below.

(b) The Pilot Letter will detail the conditions for the Pilot including:

(i) the liability shift to the Acquirer as set out in clause A.5.3 below;

(ii) the restrictions of the Pilot which may include without limitation the General Conditions referenced in Table 2, customised as appropriate, by the Company in its absolute discretion; and

(iii) the Company's right to terminate the Pilot at any time during the Pilot by notice in writing to the Device Approval Applicant if, in the Company's absolute discretion, the Company determines the technology is vulnerable to a significant security threat or other security issue.

Table 2 Pilot - General Conditions.

General Conditions	Restrictions
Deployment Restriction	10- xx 000 instances/ deployments
Reporting	Fraud, Chargebacks, Merchant Category Codes
Functionality	Contactless only, no PIN
In flight Remediation	After **xx** Months **xx** vulnerabilities must be remediated
Term	3 to 12 Months
Future Registration	After **xx** months, Vendor must start certification against **xx** standard
Deployment	Vendor can only deploy in **xx** Merchant Category Codes
Liability Shift	Acquirer accepts liability for any fraud incurred during the pilot

A.5.2 Repeat SRA

(a) Following completion of a Pilot, or in response to a request from the Device Approval Applicant at any stage during a Pilot if agreed to by the Company in its absolute discretion, the Company will repeat the SRA to determine if the security vulnerabilities identified in the Pilot Letter have been mitigated.

(b) Based on the outcome of the repeat SRA, the Company will determine whether to approve, accept for Pilot (as an extension of the current Pilot or as a Pilot under different conditions) or decline to approve registration of the

Device, Solution or Non-Standard Technology in accordance with clause 5.1 of the Device Approval Process.

A.5.3 Principles for Liability Shift

(a) The Device Approval Applicant is responsible for card losses incurred by an Issuer, where:

(i) such losses arise from the compromise of PIN and/or card data;

(ii) the relevant compromise was caused by the use of a Device, Solution or Non-Standard Technology in a Pilot; and

(iii) the relevant compromise occurred during the term of the Pilot.

(b) Any claim must be raised either during the Pilot or during the period ending 2 years after the conclusion of the Pilot.

(c) The definition of losses will be limited to chargebacks and chargeback fees associated with fraudulent use of PIN and/or card data, and costs associated with re-issuing Cards.

(d) Upon an Acquirer identifying that the PIN and/or card data associated with the cards of two or more Issuers have been compromised at device under Pilot (or group of devices under Pilot), the Acquirer must immediately advise AusPayNet in writing.