Issuers and Acquirers Community Device Approval Process

Version No : 1.0

Effective: 16 December 2021

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.

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.

(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 standards:

(A) Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Version 6+;

(B) Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM), Version 3+;

(C) Payment Card Industry (PCI) Contactless Payments on COTS (CPoC);

(D) Payment Card Industry (PCI) Software-Based PIN Entry on COTS (SPoC).

(ii) **Application for Registration** means the application form published on the Company's website from time to time.

(iii) **Approved Standards Body** means PCISSC.

(iv) **Attestation of Compliance** means a digitally signed statement from an Approved Standards Body, confirming compliance to an Accepted Standard of the Device.

(v) **NST Process** means the process for Non-standard Technology approvals described in 'Process for Considering Non-Standard Technologies', which is Schedule 1 to this document.

(vi) **Registered Device** means a Device, Solution or other technology which is approved via the registration process set out in part 3 of this document.

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.

2. Approved Devices and Device Approval Applicants

2.1 The Company may approve a Device, Solution or other technology (including a delta application of an Approved Device) for the purpose of IAC Code Set and enter it on the Approved Devices List either:

(a) via the registration process described in Part 3 of this document; or

(b) via the NST Process.

2.2 The Device Approval Applicant:

(a) for applications via the registration process in Part 3 of this document, may be the, Acquirer, Third Party Provider, Device manufacturer or any third party; or

(b) for applications via the NST Process, must be an Acquirer.

2.2 Approved Devices (whether approved before or after December 2021):

(a) will remain approved for their Approval Period as stated on the Approved Devices List; and

(b) may be renewed as set out in clause 6 below.

3. Process for approval by registration with Attestation of Compliance

3.1 Operation of this clause 3

(a) 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.

(b) A Registered Device is an Approved Device for the purpose of the IAC Code Set from the date of the Letter of Approval, for the Approval Period.

3.2 Application for Registration.

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

3.3 Check validity of Attestation of Compliance against Accepted Standards.

The Company will examine the Attestation of Compliance for validity, including, by reviewing the Attestation of Compliance against the Accepted Standards.

3.4 Confirmation of registration and publication of registration on website.

If the Application for Registration is complete and the Attestation of Compliance is successfully validated in accordance with clause 3.3:

(a) within six weeks of receiving the Application for Registration the Company will:

(i) send to the Device Approval Applicant a Letter of Approval in a form to be determined by the Company from time to time, but such letter will contain at a minimum the name of the Device Approval Applicant, the Approved Device, the registration date and the Approval Period; and

(ii) publish the Approved Device on the Approved Devices List, which will set out the minimum details contained in the Letter of Approval.

3.5 Delta registration.

Where a Device Approval Applicant has completed a delta assessment for an Approved Device with an Approved Standards Body, the applicant must submit the delta Attestation of Compliance following the process specified in clause 3.2.

4. Process for Non-Standard Technology approvals

4.1 A Device Approval Applicant may seek approval of a Non-standard Technology via the NST Process.

4.2 Following the Decision Phase in the NST Process the Company will send to the Device Approval Applicant:

(a) a Letter of Approval in a form to be determined by the Company from time to time, but such letter will contain at a minimum the name of the Device Approval Applicant, the Approved Non-Standard Technology and the Approval Period and will publish the Non-Standard Technology on the Approved Devices List; or

(b) notification in writing of the decision to decline.

5. Decisions

5.1 Approval

If the Company approves a Device, Solution or Non-Standard Technology (including delta approval), the Company will issue a Letter of Approval to the Device Approval Applicant.

5.2 Decline

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

5.3 Revocation

Registration undertaken in accordance with clause 3 may only be revoked by the Company prior to the expiry of the Approval Period if approval of the Device, Solution or other technology has been withdrawn or revoked by an Approved Standards Body.

Non-Standard Technology approvals may be revoked by the Company prior to the expiry of the Approval Period if the Company determines that the Non-Standard Technology should no longer be approved because the Non-Standard Technology is vulnerable to a significant security threat which did not exist or was not apparent at the time the device approval was granted.

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

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

(b) remove the Approved Device from the Approved Devices List.

6. Renewal of Device Approval

6.1 Approval Period

Devices will be approved by the Company for the Approval Period as specified below.

(a) For Registered Devices, the Approval Period will align with the period of approval under the Attestation of Compliance.

(b) For Non-Standard Technologies the Approval Period will be determined by the Company in its absolute discretion up to a maximum of three years.

6.2 Renewal process

(a) Registered Devices

Registered Devices are required to be re-evaluated by the Approved Standards Body before the expiration date of the Attestation of Compliance and issued with a new Attestation of Compliance.

The Company will renew the approval for a Registered Device on expiry of the current Approval Period provided the Device Approval Applicant produces a new Attestation of Compliance for the Registered Device. Once the Company validates the new Attestation of Compliance:

(i) the renewed Approval Period will align with the period of approval under the current Attestation of Compliance;

(ii) the Company will send the Device Approval Applicant an updated Letter of Approval including the renewed Approval Period; and

(iii) the Company will update the Approved Devices List.

If the Attestation of Compliance for the 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.

(b) Approved Devices under the standard device approvals process in force prior to December 2021

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

(A) the Company will register the Approved Device as a Registered Device upon receipt of a valid Attestation of Compliance;

(B) any 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;

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

(D) 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

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

(ii) If the Approved Device is not covered by an Attestation of Compliance:

(A) The Company may, at its sole discretion, extend the Approval Period for a further period of three years or such other period as it (in its absolute discretion) deems appropriate having regard to changes in security technology, applicable standards, security threats and/or other knowledge of security issues; and

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

(C) the Company will update the Approved Devices List.

(c) Non-Standard Technologies approved under the NST Process:

At the conclusion of the Approval Period, the Company may, at its sole discretion, extend the Approval Period for a further period as it deems appropriate, having regard to changes in security technology, applicable standards, security threats and/or other knowledge of security issues. The Company will send the Device Approval Applicant an updated Letter of Approval including the new Approval Period and update the Approved Devices List.

7. Dispute resolution process

7.1 The Device Approval Applicant may request review of a Company decision.

7.2 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.

7.3 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.

Schedule 1

Process For Considering Non-Standard Technologies

PART 1 INTRODUCTION

1.1 Background

The card payment system is seeing a surge in new products and services due to the rapid changes in available technology and the growing number of organisations entering the payments market.
The process for considering non-standard technologies at Point of Interaction (POI) has been established in order to:

1. allow and encourage innovation;
2. quickly address emerging technologies while limiting the potential for fraud; and
3. act as an industry and avoid potential inconsistencies from card schemes acting individually.

The parties may follow the process set out in this Schedule or may agree an alternative process to register non-standard technologies at POI.

1.2 Purpose of this document

This document provides a description of the process for reviewing and approving non-standard technologies at POI.

1.3 Scope

This document supports the consideration of POI technologies that can be provided to a merchant to undertake card payments. POI technologies include attended and unattended Point of Sale (POS) devices and ATMs.

A proposed POI solution / technology will be considered under this process if it would normally be required to meet any of the following Australian or global payment standards but, by nature of its design, is unable to do so:

i) PCI PTS;

ii) PCI DSS;

iii) IAC requirements for PIN Entry Devices (IAC Code Volume 3 - Acquirers Code); and

iv) EMV.

Excluded from scope is any solution / technology that:

a) is not intended for use at POI;

b) is expected to be able to meet each of the standards listed above (where required) but has not yet completed the certification process; or

c) is a closed loop system.

1.4 Review of the process

The IAF will review the process for considering non-standard technologies at Point of Interaction from time to time and at least every two years.

PART 2 HIGH LEVEL PROCESS

2.1 Stages for assessing non-standard technologies at POI

The high level joint industry process for assessing non-standard technology at POI is made up of 6 stages as follows:

1. Request Phase

    a) Request for consideration of a non-standard technology by an acquirer or the IAF

2. Identification Phase

    a) Identification of existing applicable or partially applicable standards and academic research
    b) Identification of laboratories best matched for testing the non-standard technology

    c) Identification of subject matter experts

3. Technical Examination Phase

    a) Review of the device by selected laboratories

4. Assessment Phase

   a) Review of reports and assessment by AusPayNet

   b) Development of a high level risk assessment by AusPayNet

   c) Development of a pass/fail/pilot decision by AusPayNet

5. Pilot Phase

   a) A controlled pilot with strictly defined parameters including number of devices and merchant is permitted and subject to close monitoring by the Company.

6. Decision Phase

   a) Development of a pass/fail decision by AusPayNet.

2.2 Timing

The goal is to complete the Assessment within approximately 6 months from the time the Device Approval Applicant first approaches AusPayNet Management with a request for consideration. However, the actual timing will depend largely on the complexity of the solution, the quality of documentation received from the Device Approval Applicant, the workload of the selected laboratories and the level of support from card schemes.

2.3 Request for consideration

Figure 1 below highlights the steps of the request for consideration stage:

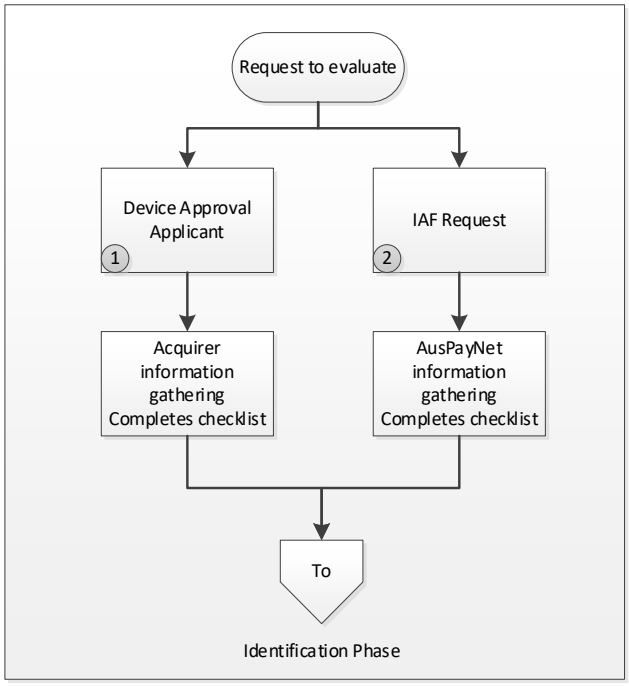

Figure 1 – Request Phase

1. A request for considering a non-standard technology evaluation is made to AusPayNet by the acquirer who wishes to use the device or technology (the Device Approval Applicant)[1].

[1]- A primary Device Approval Applicant should be nominated if a solution has more than one acquirer.

2. Alternatively, the IAF may request that a non-standard technology be considered for assessment if they believe it to be beneficial to the Australian Card Payments industry as a whole.

3. The standard checklist to be completed by the Device Approval Applicant (or AusPayNet if the IAF is the Device Approval Applicant) contains information about the proposed technology (Part 3 - Initial assessment checklist).

Note: As part of the initial request, the Device Approval Applicant agrees to accept the external costs associated with the device evaluation. These costs usually need to cover technical security consulting, system testing by a specialised testing company, plus travel costs for members to attend meetings.[2] If the IAF requests that a technology should be assessed, then the costs associated with the process will be covered through AusPayNet's normal budgetary process.

The Device Approval Applicant must ensure that the Device manufacturer or supplier (**Vendor**) is prepared to make the solution itself available to the lab for testing as part of the industry analysis.

2.4 Identification Phase

Figure 2 below highlights the steps of the identification phase

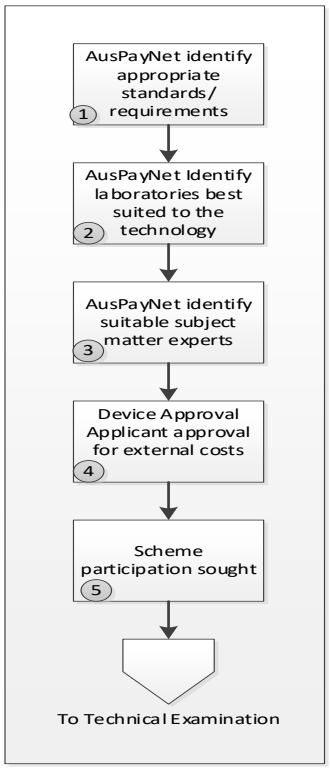

Figure 2 – Identification Phase

1. AusPayNet will initially review the Initial assessment checklist and obtain the views of the card schemes with regards to the technology under consideration. AusPayNet will then identify any possible existing standards including partial or draft standards or requirements applicable to the technology involved. This research must also examine the current state of academic research in the technology being considered.

[2]- An estimate of the expected costs will be advised to the Device Approval Applicant before any decision is made to spend the money.

2. AusPayNet will identify any laboratories with particular knowledge and/or skills in testing the technology involved.

3. AusPayNet will identify any subject matter experts willing to assist in the evaluation of the technology and estimate likely costs. Any consultants likely to be engaged must be willing to agree to AusPayNet's confidentiality requirements and any applicable terms of reference.

4. AusPayNet will advise the Device Approval Applicant of the selected laboratory (more than one laboratory is possible) and the likely estimate of external costs and obtain the Device Approval Applicant's agreement to bear those costs.

5. Having gained the Device Approval Applicant's approval for bearing the costs involved, AusPayNet may approach the card schemes requesting nominations for experts to attend and assist in the evaluation of the technology.

Prior to completing the Identification Phase, AusPayNet will ensure that appropriate contractual arrangements are in place, including:

a) Consent from the Vendor to authorise AusPayNet to access documents/personnel/premises as required by the scope of the assessment; and

b) A confidentiality undertaking between AusPayNet and the Device Approval Applicant/Vendor and any Subject Matter Experts.

2.5 Technical Examination Phase

Figure 3 below highlights the steps of the technical examination phase:

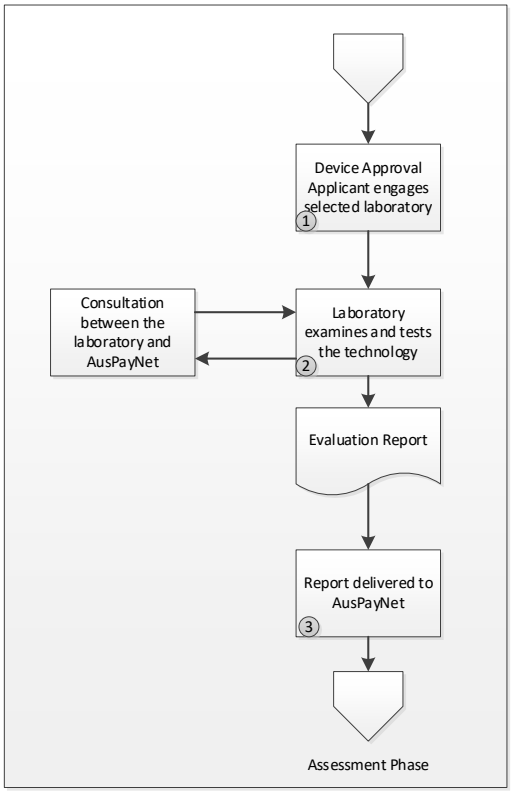

Figure 3 – Technical Examination

1. The Device Approval Applicant or Vendor will engage the identified laboratory or laboratories if so required by AusPayNet and arrange for a review with the output report to be provided to AusPayNet. This engagement should permit an ongoing dialogue between the laboratory and AusPayNet to ensure that desired outcomes are met.

2. The laboratory will examine and test the device against standards and requirements as advised by AusPayNet and its own knowledge and skill set.

    a) The lab carries out the technical review/penetration testing[3] for any identified risks and writes a draft report including:

        i) Highlighting the risks and the effectiveness of any relevant mitigation measures in place; and

        ii) Areas of uncertainty and why they are not able to provide a clear statement.

3. The laboratory will provide the report to AusPayNet and the Device Approval Applicant/Vendor if required by AusPayNet:

    a) Card schemes may carry out their own testing/analysis and provide AusPayNet with any additional risks that they consider as relevant for the device or technology under consideration.

2.6 Assessment Phase

Figure 4 below highlights the steps of the assessment phase:

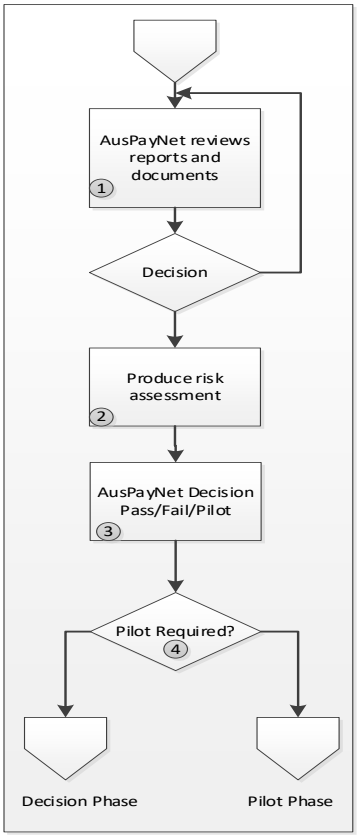

Figure 4 – Assessment phase

[3]- The card schemes may also choose to do their own testing in addition to the industry testing.

1. AusPayNet convenes a meeting, which includes nominated experts from the schemes and the attendance of any nominated subject matter experts to review the laboratory's findings and other relevant documentation. A maximum of three meetings may occur if more information is required.

2. AusPayNet produces a high level risk assessment of the device.

    a) In order to facilitate the risk assessment, the Device Approval Applicant/Vendor should provide to AusPayNet any available technical documentation and/or results from previous testing, including relevant testing carried out by the card schemes in Australia or internationally.

    b) In the risk assessment, AusPayNet will:

    - Assess the solution against the current standards to confirm and potentially identify which requirements of the current standards are not met;
    - Identify potential threats and risks to the payment system arising from the gaps to the current standards;
    - Assess the controls applied by the Vendor against these potential threats and risks to the payment system;
    - Assess the residual threats and risks to the payment system based on the combination of the potential threats and risks identified and the controls applied.

3. AusPayNet will determine whether:

    - to approve the device or decline to approve the device; or
    - a Pilot Phase is required and determined appropriate criteria.

2.7 Pilot Phase

If a pilot is recommended by AusPayNet, it can be run in line with pre-determined criteria[4] and the following assumptions:

1. All agreed criteria are applicable to the Device Approval Applicant, not the Vendor;

2. The Device Approval Applicant should report on performance against criteria at a pre-determined frequency;

3. Anything that AusPayNet considers as having an impact on the suitability of the new technology whilst the pilot is running will be part of the considerations when running and assessing a pilot;

4. The criteria may be amended by AusPayNet during the course of the pilot, although this should be a rare occurrence;

5. Card schemes may withdraw from a pilot at any time at their own discretion if it is deemed that the pilot will create a liability or risk to their issuers, their brands or network;

[4] Such criteria (including success criteria) would be agreed with the Device Approval Applicant and card schemes. Part 4 of this Schedule contains high level criteria for a pilot. The criteria for the pilot shall be strong enough to provide comfort to the industry that the technology is acceptable

6. By undertaking the Pilot Phase, the Device Approval Applicant accepts the liability shift stated in 'Principles for Liability Shift' in Part 4 to this Schedule; and

7. The Device Approval Applicant has the financial reserves to withstand the magnitude of liability described above.

Note: it is acknowledged that a pilot, in and of itself, cannot be used to test whether a solution is secure.

During the course of the pilot, the Device Approval Applicant collects the data and provides it to AusPayNet in line with the agreed criteria. Card schemes receive the data in relation to their pre-determined individual criteria from the Device Approval Applicant directly.

The data provided by the Device Approval Applicant is assessed by AusPayNet Management against the pre-defined criteria.

If significant issues are identified during the course of the pilot it can be shut down prior to completion by the Device Approval Applicant, the Vendor or AusPayNet.

2.8 Decision Phase

Following any Pilot Phase, AusPayNet will:

- review whether the criteria for the pilot have been met within the timeframe, and determine if the technology is suitable for broader rollout, and if a phased or full rollout is appropriate; and

- approve or decline to approve the device.

PART 3 INITIAL ASSESSMENT CHECKLIST

The initial assessment checklist should be completed by the Device Approval Applicant to request consideration for a non-standard technology at Point of Interaction and provided to AusPayNet in line with the process for consideration.

Australian Payments Network
Connect Inspire Thrive

1- Date of submission: ...../...../.....

2- Name of the Device Approval Applicant (acquirer):
.....
.....

3- Name of the Vendor (technology provider):
.....
.....

4- Name of the non-standard technology for consideration:
.....
.....

5- Software / hardware / firmware version numbers:
.....
.....

6- Provide details around the current and expected use of the technology:
.....
.....

7- Level of support from card schemes and names of contacts in Australia:
.....
.....

8- Information on markets where it is already running, for how long and the experience so far:
.....
.....

9- Incremental and economic benefits the solution delivers to stakeholders that existing solutions don't:
.....
.....

10- Description of the non-standard technology, including details around the equipment used, the security process and procedures used to manage the equipment and information about the system architecture where applicable:
.....
.....

11- What is required for merchants and/or other issuers and acquirer to adopt the solution?
.....
.....

12- Other technology that is relied upon to support the solution (e.g. mobile phone):
.....
.....

13- List (non-exhaustive) of standards that devices would be expected to be assessed against:
.....
.....

14- Details of the gap between the existing standard requirements and the new technology (why doesn't it comply with existing standard?)
.....
.....

15- Perceived risks of the non-standard technology and how can they be mitigated (impact on payment ecosystem):
.....
.....

16- How the Device Approval Applicant intends to mitigate the risks:
.....
.....

17- Evidence of any relevant certifications already obtained, failed or in progress:
.....
.....

18- Provide details of any previous independent testing that may have already been carried out:
.....
.....

19-Provide information (if available) on whether any process is already underway internationally or within Australia to establish new relevant standards:
.....
.....

20- If a pilot is proposed, details of any existing plans for pilot including merchant base, numbers and target date for initiating the pilot:
.....
.....

21- Any additional comments to be considered that the Device Approval Applicant deems relevant:
.....
.....

PART 4 HIGH LEVEL CRITERIA FOR PILOT

Once AusPayNet has agreed that the technology under consideration is appropriate for pilot, it will meet with the card schemes and agree on the industry criteria for pilot. It is important that the criteria for pilot are strong enough to provide comfort to the industry that the technology is acceptable for launch on the Australian market at the end of the pilot. This is because the expectation would be that if all the criteria for pilot are met within the timeframe, then the next step will be a phased or full rollout (depending on the size of the pilot).

Criteria for pilot include:

- Length of pilot (including tentative start and end dates)
- Pilot phases
- Frequency and content of reporting
- Restriction to specific states and/or concentration requirements
- Transaction types
- Eligible merchants (include anticipated number)
- Eligible devices
- Eligible cards
- Minimum number of transactions that need to be going through to consider that the technology was sufficiently tested
- % of active users that continue to use the solution throughout the pilot
- Industry mix of merchants
- Compliance and fraud limits
- Communication (or no communication) to merchants and card holders about the risks of the technology they are piloting
- Broader communication plan for before, during and after the pilot is being run.
- Merchant training
- Fraud rate
- Surveys to users (merchant and card holders) on how comfortable they are in using the solution

- Social media response
- Any additional security testing to be done whilst the pilot is running
- Progress through relevant standards bodies or similar
- The Device Approval Applicant has the financial reserves to withstand the magnitude of liability inherent to the risk of running the pilot

Each of the criteria will be assigned a success measure for the Device Approval Applicant and AusPayNet to track during the course and at the completion of the pilot.

Note: the card schemes may separately impose their own requirements to the Device Approval Applicant.

Principles for Liability Shift

- A Device Approval Applicant is responsible for card losses incurred by an Issuer, where such losses arise from the compromise of PIN and/or card data caused by the Device Approval Applicant's use of a non-standard POI technology in an approved IAC pilot during the pilot and for 2 years after the conclusion of the pilot.
- 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.
- Upon an Issuer identifying that the PIN and/or card data associated with the cards of two or more Issuers have been compromised at a pilot device (or group of pilot devices), the Issuer must immediately advise the Device Approval Applicant of the pilot and AusPayNet in writing.
- The standard of proof for all matters related to the pilot shall be on the balance of probabilities.
- Parties to any cost dispute shall attempt to resolve it by negotiating in good faith bilaterally prior to seeking to use AusPayNet's dispute resolution process (to be developed).

CHANGE HISTORY

Version	Approval date	Change
1.0	25/11//21	Approved by the IAF Effective 16/12/2021