KPMG Law

Level 38 Tower Three
300 Barangaroo Avenue
Sydney NSW 2000

P O Box H67 Australia Square
Sydney NSW 1213
Australia

ABN: 78 399 289 481

Telephone: +61 2 9335 7000
Facsimile: +61 2 9335 8968
DX: 1056 Sydney
www.kpmg.com.au

[redacted]

Australian Competition & Consumer Commission
GPO Box 3131
Canberra ACT 2601

Our ref

Contact Paula Gilardoni
Caroline Marshall

BY EMAIL: adjudication@accc.gov.au

6 April 2020

Dear Sir / Madam,

AUSTRALIAN PAYMENTS NETWORK LIMITED (ACN 055 136 519) APPLICATION FOR REVOCATION OF AN AUTHORISATION FOR PROPOSED CONDUCT AND SUBSTITUTION OF A REPLACEMENT

We are acting on behalf of Australian Payments Network Limited (ACN 055 136 519) (**AusPayNet**) to submit this application for revocation of an authorisation for proposed conduct and substitution of a replacement (**Application**) in respect of authorisations A91497 and A91498, which were granted by the Australian Competition & Consumer Commission (**ACCC**) on 31 August 2015 and are set to expire on 22 September 2020. Accordingly, please find enclosed the following documents for your consideration:

(a) the Application, which we confirm may be uploaded to ACCC's public register;

(b) a declaration we have completed on behalf of AusPayNet, as their legal counsel; and

(c) proof of payment of the $2,500 lodgement fee.

Please do not hesitate to contact us should you have any questions, or wish to discuss. Thank you for your assistance and we look forward to your adjudication.

Yours sincerely,

Paula Gilardoni
Partner

APPLICATION FOR REVOCATION OF AN AUTHORISATION AND SUBSTITUTION OF A REPLACEMENT

DATED 6 APRIL 2020

CONTENTS

1 Executive Summary

In 2015, Australian Payments Network Limited (**AusPayNet**) established the Issuers and Acquirers Community (**IAC**) framework (**IAC Framework**) to replace the Consumer Electronic Clearing System (**CECS**) framework.

The IAC Framework:

(a) manages ATM and EFTPOS payments;

(b) enables the multilateral settlement of amounts owing to or by financial institutions and issuer or acquirer participants (**IA Participants**) involved in ATM and EFTPOS transactions;

(c) engages in card payments industry policy development;

(d) admits a broad range of members (including entities that are not directly involved in the making of, or giving effect to, ATM and EFTPOS transactions, but are otherwise involved with the card payments industry); and

(e) seeks to actively monitor and manage IA Participant compliance with security standards and requirements.

The list of members of the IAC has been attached at Annexure A.

On 1 May 2015, Australian Payments Clearing Association Limited (**APCA**) (as AusPayNet was formerly known) sought authorisation from the Australian Competition and Consumer Commission (**ACCC**) in respect of the certification, suspension and termination provisions of the proposed IAC Regulations (**Regulations**) and IAC Code Set (**Code**).

The ACCC granted authorisations A91497 and A91498 for a period of five years (**Authorisations**). The Authorisations are set to expire on 22 September 2020.

With the Authorisations set to expire, AusPayNet wishes to apply for a revocation of the Authorisations and substitution of a replacement in respect of the relevant provisions of the Regulations and the Code, in accordance with section 91C of the *Competition and Consumer Act 2010* (Cth) (the **Act**).

AusPayNet submits that, like in 2015, the likely public benefits of the current application (**Application**) outweigh any possible detriments. The certification, suspension and termination provisions that are the subject of this Application have not changed substantially since 2015, although AusPayNet has made a number of changes to increase the transparency, security and the effectiveness of the broader IAC Framework. These changes have sought to ensure that the IAC Framework continues to provide material benefits to the public, while minimising any public detriments. It therefore continues to be the case that without the ability of IAC members to have some mechanism to enforce compliance with the standards established by the IAC (through the

ability to set minimum requirements for entry and issue fines to participants and/or suspend or terminate membership for non-compliance), the operational efficiency of the IAC could be undermined (and, at the extreme, may compromise the industry's ability to centrally coordinate the clearing and settlement of EFTPOS and ATM transactions).

Accordingly, AusPayNet submits that the likely benefit to the public of authorising these provisions would outweigh any detriment, including any lessening of competition that might result from the operation of the relevant provisions.

2 Applicant

2.1 The company and its business activities

AusPayNet, formerly named APCA, is a public company limited by guarantee, incorporated on 18 February 1992.

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. AusPayNet manages and develops regulations, procedures, policies and standards governing payments clearing and settlement in Australia. Individual institutions are responsible for their own clearing and settlement operations and are required to conduct their operations according to AusPayNet's rules as set out in the regulations and procedures for each of AusPayNet's frameworks.[1]

The board of directors of AusPayNet (**Board**) is comprised of three independent directors (including the Chair), one director appointed by the Reserve Bank of Australia (**RBA**), the CEO of AusPayNet (non-voting) and a number of directors appointed and an equal number of directors elected by AusPayNet members (currently eight directors are appointed or elected by AusPayNet members).

Through its network, AusPayNet brings together service providers, government, regulators and other stakeholders to administer and improve the Australian payments system.

AusPayNet has over 130 members, including financial institutions, card schemes, merchants such as Coles and Woolworths, new digital banks such as Volt, Xinja and Judo, and other payments industry stakeholders such as PayPal and Google.

2.2 Payment frameworks

AusPayNet is currently responsible for five payment frameworks. These are:

(a) the IAC, formerly CECS, which provides minimum standards to protect and enhance the security, integrity and efficiency of ATM and EFTPOS transactions;

(b) the Australian Paper Clearing System (APCS) relating to exchanges of paper-based payment instructions, primarily cheques;

[1] See section 2.2 below for more information.

(c) the Bulk Electronic Clearing System (BECS) relating to bulk direct entry low value transactions, allowing businesses (such as, for example, utility companies) to make arrangements to direct debit and/or credit large numbers of customers' accounts on a regular basis;

(d) the High Value Clearing System (HVCS) established as part of the development of real time gross settlement in Australia to provide an efficient and secure electronic payments mechanism for the finance industry; and

(e) the Australian Cash Distribution and Exchange System (ACDES) which governs the exchange and distribution of wholesale cash.

2.3 Name, address (registered office), telephone number and ACN

Australian Payments Network	
Name	Australian Payments Network Limited
Address	Level 23, International Tower Three 300 Barangaroo Avenue NSW 2000
Telephone	+61 2 9216 4888
ACN	055 136 519

2.4 Contact person's name and details (including email address for service of documents)

Australian Payments Network	
Name	Nancy Bryla
Position	General Counsel & Company Secretary
Telephone	[redacted]
Email	[redacted]

3 Details of authorisations to be revoked and substitution of a replacement

3.1 Authorisations previously granted

On 31 August 2015, the ACCC granted the Authorisations to APCA in respect of the certification, suspension and termination provisions in the Regulations and Code.[2] The following provisions were authorised:

(a) in the Regulations:

[2] See ACCC authorisation, available at https://www.accc.gov.au/public-registers/authorisations-and-notifications-registers/authorisations-register/australian-payments-clearing-association-limited-authorisations-a91497-a91498.

(i) section 4.1(c) – Eligibility for Membership – requirement to comply with Certification Requirements;

(ii) section 5.1(b) – Compliance with Certification Requirements;

(iii) section 6.3 – IAC Membership – Suspension;

(iv) section 6.4 – Effect of Suspension;

(v) section 6.5 – Termination; and

(vi) section 6.7 – Financial Claims Scheme – Suspension; and

(b) in the Code:

(i) Volume 1, clause 3.1 – Compliance with applicable requirements from Framework Participants;[3]

(ii) Volume 1, clause 3.4 – Certification of Prospective Framework Participant;

(iii) Volume 1, Annexure A – Annual Security Audit Checklist;

(iv) Volume 1, Annexure B – New Framework Participant Certification; and

(v) Volume 5, clause 3.5 – Suspension for Failure to Settle Event.

The Authorisations were granted for a period of five years and are set to expire on 22 September 2020.

3.2 Current Authorisations to be revoked and substitution of a replacement authorisation

AusPayNet is applying to the ACCC for the Authorisations to be revoked and substituted by a replacement, pursuant to section 91C of the Act (**Revocation and Substitute Authorisation**).

4 Industry background

4.1 Market growth

The way Australian consumers pay for goods and services has changed dramatically over recent years. In addition to the traditional payment methods of cash and cheque, which remain in use but are in long-term decline, and traditional debit and credit cards, Australian consumers are able to choose from a range of convenient and secure digital payment options, including contactless cards, mobile banking apps and wearable payment devices. This change has been enabled by technological innovation, both by financial technology companies (**Fintechs**) and incumbents in the payments sector.

The Australian card market has demonstrated continued and constant growth with debit and credit cards being the most common method of retail payment. Australia has the fourth highest number of non-cash payments per person, with non-cash payments growing at about 10% per year. Consumers and businesses executed more than 9.8 billion card transactions in 2019, an increase of 11.5% from FY2018 and 58% from 2015, with more than 27 million card

[3] As defined in section 5.2(a) below.

transactions every day. Australia has the highest level of contactless card use in the world with consumers making about 80% of point-of-sale (**POS**) transactions via 'tap-and-go.'[4] Debit card use increased by 9.3% from FY 2018 (and by over 29% from FY 2015) in value to $333.4 billion. Credit card use grew by 2.0% from FY 2018 (and 12% from FY 2015) in value to $336.1 billion.

The growth in card payments has been made possible by the roll-out of new payments technology, and Australian consumers' positive response and use of it. AusPayNet's role, promoting competition and innovation in payments as well as delivering efficiencies and controlling systemic risk, has enabled card payments' growth by ensuring Australians are able to enjoy these new technologies without having to question or be concerned about the safety and integrity of the system.

4.2 Innovation and Security

Innovation has underpinned significant benefits to end-users of the payments system, including consumers and merchants. In fact, changes in technology continue to accelerate and impact consumer behaviour. For example, new POS solutions enable smaller merchants to accept card payments using commercial off-the-shelf devices, such as a smartphone or tablet, rather than through traditional payment terminals.

With innovation, comes the potential for additional security risks that must be appropriately considered and managed. Accordingly, AusPayNet invests in the security of its frameworks and is a key participant in standards development through its involvement with global standards bodies including the International Standards Organisation (ISO), the Payment Card Industry (**PCI**), EMVCo,[5] the Fast IDentity Online Alliance (FIDO), the World Wide Web Consortium (W3C), and Standards Australia, to ensure the security standards for card payments keep pace with technology. In January 2019, AusPayNet was selected as one of 29 board members of the global Board of Advisors of the Payment Card Industry Security Standards Council (PCI SSC) where it contributes its expertise along with a range of vendors, merchants, institutions which issue cards used in card payment transactions pursuant to the rules of an Approved Card Payment System (**Issuers**) and institutions which acquire card payment transactions on behalf of Issuers (**Acquirers**). AusPayNet continually reviews its standards and specifications to ensure they are best practice and, where possible, future-proof for card security.

An example of AusPayNet's involvement in standards development concerns the development of PCI's Software-based PIN-entry on Commercial Off-the Shelf (**COTS**) (**SPoC**) standard and PCI's Contactless Payments on COTS (**CPoC**) standard. To ensure that the views of AusPayNet's members were fully represented, AusPayNet contributed to the development of

[4] See AusPayNet Annual Review 2019, available at https://www.auspaynet.com.au/sites/default/files/2019-10/AusPayNet_Annual_Review_2019.pdf; Philip Lowe speech (10 December 2019), available at https://rba.gov.au/speeches/2019/sp-gov-2019-12-10.html.

[5] EMVCo is the EMVCo, LLC representing Europay, Mastercard and Visa.

both PCI's SPoC standard (released January 2018) and CPoC standard (released December 2019). As a result, effective 1 January 2019, Acquirers are able to support SPoC solutions that accept chip and PIN payments via a commercial phone or tablet, approved by AusPayNet's standard device evaluation process.[6] AusPayNet is currently reviewing the applicability of the CPoC standard. AusPayNet expects that Acquirers will be able to support CPoC solutions that accept chip card payments by the end of 2020.

However, as the development of standards generally lags behind the technology, AusPayNet's non-standard technologies approval process, introduced in 2017, also enables AusPayNet to assess innovative technologies prior to the availability of finalised international standards. Through this process, AusPayNet is able to allow and encourage secure innovation by ensuring minimum security requirements are met. The recent approval by AusPayNet for the pilot of a mobile POS solution provides an example of how this process has enabled innovation in a secure manner.[7]

4.3 Regulatory reviews

In addition to the impact of technology and innovation (and, at least in part, because of it), there are a significant number of reviews and inquiries being conducted by various regulatory bodies that affect the payments industry and could impact aspects of the IAC Framework over time (**Regulatory Reviews**). A summary has been set out below.

(a) **Select Committee on Financial Technology and Regulatory Technology 2020.**

On 11 September 2019, the Senate established a Select Committee on Financial Technology and Regulatory Technology to inquire into and report on, amongst other matters, the size and scope of the opportunity for Australian consumers and businesses arising from FinTech and regulatory technology, the barriers to the uptake of new technologies in the financial sector, and the progress of FinTech facilitation reform. This inquiry is ongoing. An interim report was due to be published late March 2020 and the final report due October 2020. On 27 March 2020 the Committee announced that as the economic and financial environment has changed dramatically as a result of the unfolding COVID-19 pandemic, it has reopened its submissions process until 10 April 2020.

(b) **RBA Review of Retail Payments Regulation.**

On 29 November 2019, the RBA released an *Issues Paper: Review of Retail Payments Regulation* to review the regulatory framework for card payments in light of developments in technology, new entrants and innovation in the payments industry and how they have altered the retail payments landscape. This review was expected initially to conclude in

[6] There is a requirement on all IA Participants that all devices they employ in the IAC are to be approved by AusPayNet. The rationale for this IAC requirement is that, through compliance with minimum security standards and minimum technical standards, AusPayNet ensures confidence in the security, interoperability and resilience of the payments system.
[7] For further details, see https://www.auspaynet.com.au/insights/blog/Mobeewave.

Q2 2020 with a more detailed paper containing policy recommendations likely to be released later in 2020. The RBA announced on 26 March 2020 that the review was being put on hold although it was expected to be completed in 2021.

(c) **Australian Securities and Investments Commission (ASIC) ePayments Code Review.**

ASIC is currently undertaking a review of the ePayments Code to assess its fitness for purpose in light of innovation in financial technology. The ePayments Code is referenced in Volume 6 of the Code, primarily in relation to the disputed transactions process. The ePayments Code is also relevant to BECS procedures and the guidelines for Merit-based Incentive Payment System (MIPS), including the recovery of partial funds. This review is ongoing with ASIC aiming to release a second round of consultation around July 2020.

(d) **Consumer Data Right.**

On 23 January 2020, the Government announced a new inquiry into the Consumer Data Right (**CDR**) to examine how CDR can be, amongst other things, expanded beyond its current 'read' access to include 'write' access to enable customers to apply for and manage products (including, for Open Banking, by initiating payments and switching accounts). The report is due to be released by September 2020.

(e) **APRA's Priorities in relation to Cyber, Operational Resilience and Payments.**

On 30 January 2020, the Australian Prudential Regulation Authority (**APRA**) published its Policy Priorities and Supervision Priorities for the next 12 to 18 months (**APRA's Priorities**). In relation to the payments industry, APRA's Priorities included within an overall framework of emerging risk analysis, reviewing innovation and competition, including in the retail banking and payments sector the approach to regulating Purchased Payment Facilities (PPFs). On 23 March 2020, APRA announced that it was suspending all substantive public consultations and does not plan to recommence consultation on any non-essential matters before 30 September 2020.

4.4 AusPayNet Reviews

AusPayNet is currently undertaking its own reviews of the payments industry which will include an evaluation of the IAC Framework to ensure the Regulations and Code remain appropriate and effective over time (**AusPayNet Reviews**).

(a) **Payments Acceptance Governance Strategy**

Customer demand for convenience and speed is driving the rapid pace of innovation across card payments. To ensure AusPayNet appropriately responds to this pace of innovation, AusPayNet commenced a review in late 2019 of its strategy for payments acceptance governance. The review will include an assessment of existing approaches

under the Code for device approvals. The initial review is due to complete a forward-looking strategy for payments acceptance governance in Q2 2020 and approved changes could be implemented by 2022.

(b) **Future State for Australia's Payments Systems**

In November 2019, AusPayNet launched a consultation on the future of Australia's payment systems with a view to creating a plan for their sustainable evolution. The consultation process raises the possibility of consolidation and rationalisation of payment systems, an issue that has been recently flagged by the Governor of the RBA,[8] and the significance of technological innovation in the evolution of our payment systems, in such areas as CDR, digital identity and cloud technology. This review is expected to conclude in Q2 2020 with the publication of a set of conclusions that will create a plan for the evolution of Australia's payment systems.

Upon completion of the Regulatory Reviews and AusPayNet Reviews, AusPayNet expects it will conduct a further assessment of whether any proposed change(s) need to be implemented in the Regulations and Code. It was expected that such assessment would be completed between late 2020 to early 2021, but this timeframe will be impacted by delays in the completion of the Regulatory Reviews and AusPayNet Reviews that will follow as a consequence of the impact of COVID-19.

5 The IAC

5.1 IAC's framework

The IAC Framework's foundational documents are:

(a) the Regulations, which are binding on all Framework Participants.[9] The Regulations set out the governance structure and the rights and obligations of members of the IAC. The Regulations can only be amended on the recommendation of the management committee, the Issuer and Acquirer Forum (**IAF**), and with the approval of the IAC and the Board;[10] and

(b) the Code, which is binding upon IA Participants only. The Code details the minimum-security standards, interoperability standards, value added services and operational provisions that apply to all card payments (excluding closed loop cards and on-us

[8] Address to the 2019 Australian Payments Network Summit, Philip Lowe, Governor RBA, 10 December 2019, available at: https://www.rba.gov.au/speeches/2019/sp-gov-2019-12-10.html.
[9] As defined in section 5.2(a) below.
[10] See section 5.2(a) below.

transactions) within the IAC.[11]

The Code comprises seven volumes:

(a) **Volume 1 (Introduction and Member Obligations)** – establishes various binding obligations on IA Participants including compliance with certification requirements and annual audit requirements.

(b) **Volume 2 (Issuers Code)** – establishes Issuer obligations including mandatory requirements for PIN management and device security.

(c) **Volume 3 (Acquirers Code)** – establishes Acquirer obligations including mandatory obligations in relation to PIN management and transaction and device security.

(d) **Volume 4 (Device Requirements and Cryptographic Management)** – establishes the cryptographic standards and key management practices applicable to all devices and solutions and the device approval process (for both standard and non-standard technologies).

(e) **Volume 5 (Settlement Code)** – establishes procedures for settlement of obligations incurred by IA Participants arising from ATM and EFTPOS transactions.[12]

(f) **Volume 6 (ATM System Code)** – establishes the ATM system network and the operational and security requirements and procedures for IA Participants who participate in the ATM System including procedures for the security and integrity of ATM transactions and rules to promote the universal acceptance of cards at ATM terminals. Operator Members and Affiliate Members are encouraged to subscribe to the Code and participate in ATM Code Committee meetings to ensure ATM industry policy, standards and procedures represent the widest possible range of industry interests and perspectives.[13]

(g) **Volume 7 (Card Not Present Code)** – adopted in 2019, establishes an approach for mitigating the impact of card-not-present payments fraud for the benefit of all users of the payments ecosystem including merchants, consumers, Issuers, Acquirers and card schemes, through reporting and performance obligations imposed upon Issuers and Acquirers.

5.2 IAC's membership arrangements

The IAC was established principally for the benefit of Issuers and Acquirers involved in the processing of ATM and EFTPOS transactions (i.e., IA Participants). However, unlike the IAC Framework's predecessor, CECS, the IAC membership goes beyond IA Participants and also

[11] The scope of application of IAC requirements was extended effective 1 January 2019 to all card payments (excluding closed loop cards and on-us transactions). The intention to remove the exclusion from the IAC requirements of transactions switched across international card scheme networks, which was noted in AusPayNet's application for authorisation in 2015 and the 2015 ACCC Determination. AusPayNet informed the ACCC of the amendment to scope by email on 9 October 2018.

[12] The Volume 5 Settlement Code is currently under review following the adoption by eftpos Payments Australia Ltd of its own settlement rules which has impacted the way IAC members settle transactions.

[13] See section 5.2 below for more information on Operator Members and Affiliate Members and section 5.3 below for more information on Code committees.

admits Operator Members and Affiliate Members that have an involvement in the cards payment industry. The views of all members (i.e., Framework Participants, as defined in section 5.2(a) below) are considered important to ensure industry policy and the self-regulatory standards imposed upon the industry are developed in a fully informed and collaborative industry context.

More details on membership are provided below.

(a) *Types of membership*

Set out below are the four categories of membership within the IAC (collectively referred to as, **Framework Participants**).

(i) IA Participant

(A) Issuers;

(B) Acquirers; or

(C) an institution which represents one or more Issuer or Acquirer and settles directly the payment obligations of those Acquirers or Issuers,

is eligible to join the IAC as an 'IA Participant.'

An IA Participant has the right to attend and speak at IAC and IAF meetings, and has the right to nominate (or jointly nominate) a representative to the IAF. IA Participants may be appointed to a Code committee (which are responsible for the administration of the Code and referenced at section 5.3(c) below), where the IAF determines their representative has the expertise required, and the right to receive documents used in the deliberations before all IAC, IAF and Code committee meetings.

Upon becoming an IA Participant in the IAC, the IA Participant also becomes a voting member of AusPayNet, with the rights and obligations set out in AusPayNet's company constitution (**AusPayNet's Constitution**).

(ii) RBA

The RBA is eligible to be a Framework Participant in the IAC, and has the right to attend and speak at IAC and IAF meetings, to nominate a representative to the IAF, and to attend Code committee meetings, but it has no voting rights.

(iii) Operator Member

An institution which operates or administers a card payment system that has been recognised by AusPayNet and meets the approval criteria for operator members is eligible to join the IAC as an operator member (**Operator Member**).

Operator Members currently comprise American Express Australia Limited, eftpos Payments Australia Limited, Mastercard Asia/Pacific (Australia) Pty Ltd and Visa AP (Australia) Pty Ltd.

An Operator Member has no voting rights but it has the right to attend and speak at IAC and IAF meetings and, by invitation, Code committee meetings.

(iv) Affiliate Member

An institution which participates in the Australian card payments industry, although not in the capacity of an Issuer or Acquirer (**Affiliate Member**). Examples of Affiliate Members include technology providers, Fintechs, non-bank ATM providers, security laboratories, and payment gateways.

An Affiliate Member has no voting rights but it has the right to attend and speak at IAC meetings, and by invitation may attend IAF and Code committee meetings.

In addition to the specific requirements for each membership category there are several general requirements of membership, including that the Framework Participant must:

(i) be a constitutional corporation which carries on business at or through a permanent establishment in Australia;

(ii) be able to comply with AusPayNet's Constitution, the Regulations and, for IA Participants also the Code; and

(iii) agree to pay all applicable fees, costs, charges and expenses.

IA Participants are also required to settle any obligation they incur in accordance with the Code.

(b) *Membership fees*

The membership fees associated with each category of membership are set out below:

(i) IA Participant

(A) Entrance Fee: upon acceptance of each new IA Participant's application.

(B) Annual Corporate Fee: comprising an annual base fee and a periodic proportionate fee calculated by reference to members' payment system market share;

(C) Annual Framework Fee; and

(D) Ad hoc Special Project Funding Fee, as and when required.

(ii) RBA

There are no IAC membership fees for the RBA.

(iii) Operator Member

Annual Operator Member Fee (unless otherwise charged under AusPayNet's Constitution).

(iv) Affiliate Member

Annual Affiliate Fee.

The Entrance Fee is determined by the IAF. The Annual Corporate Fee, the Annual Framework Fee, Special Project Funding Fees and Operator Member and Affiliate Member Fees are determined by the Board.

Additional fees, payable by an IA Participant who proposes certain payment routing changes which require all IA Participants to make system changes, are set out in the Regulations and can only be amended with approval of the IAC and the Board.

A dispute resolution fee, currently $5,000, is payable by each IAC Framework Participant party to a dispute referred to AusPayNet under the IAC Resolution of Disputes process. The fee is also set out in the Regulations and can only be amended with approval of the IAC and the Board.

(c) *Current membership*

At the time of AusPayNet's application for authorisation of the IAC Framework, the IAC had 15 IA Participant members (then also members of CECS).

Operator Member and Affiliate Member categories did not exist prior to the IAC, however CECS did have an advisory council (**CECS Advisory Council**) which comprised interested stakeholders. Operator Members and Affiliate Members were included within the IAC Framework to ensure the development of IAC policy and standards be undertaken in a fully informed and collaborative industry context. Several members of the CECS Advisory Council became IAC Affiliate Members as operations transitioned from CECS to IAC.

In the years since authorisation of the IAC Framework, there have been the following changes to IAC membership:

	IA Participant	Operator Member	Affiliate Member
Dec 2015	15	3	9
2020	18	4	15[14]

[14] AusPayNet has added seven new affiliates to the initial stable of nine Affiliates Members from the CECS Advisory Council. One Affiliate Member joined in 2016 and resigned in 2018; another original member resigned in 2019. Two Affiliate members have recently merged into one organisation so one membership will lapse.

AusPayNet is also currently in discussions with 4 potential IA Participants, 1 potential Operator Member and 5 potential Affiliate Members.

5.3 IAC's governance structure

(a) *The IAC*

The IAC meets at least once every calendar year. The purpose of the annual meeting is to provide a forum for IAC Framework Participants to discuss any aspect of the operations of the IAC and any matters relevant to membership.

(b) *The IAF*

The IAF is responsible for the operation of the IAC (under a general delegation from the Board).

The IAF consists of:

(i) an independent director of AusPayNet nominated by the Board and who is the chair of the IAF;

(ii) a nominee of each IA Participant which has at least 2% of cards market share;

(iii) a person nominated by the RBA; and

(iv) three persons elected in a ballot by all other IA Participants.

Members of the IAF hold office for three years.

Operator Members generally attend all IAF meetings and their opinions are sought on matters that potentially or materially affect them as a group or the Card Payment System they operate. Affiliate Members may attend IAF meetings on invitation of the IAF Chair and are entitled to be notified of, and make submissions on, any matter before the IAF which potentially materially affects their business. Affiliate members are also invited to briefings following IAF meetings to ensure they are informed of relevant developments.

(c) *IAF Subcommittees*

The IAF has the power to delegate administration of the Code to one or more Code committees and to establish subcommittees. Code committees have the power to establish sub-committees to support them.

The following Code committees and subcommittees are currently in place:

(i) Security Code Committee (**SCC**)

The IAF has delegated to the SCC the administration of Volumes 1 to 4 of the Code. The scope of work and responsibilities of the SCC include:

(A) managing IA Participants' compliance with the IAC Code Volumes 1 to 4; and

(B) assessing device approval applications and SPoC solution approval applications on behalf of AusPayNet.

Membership of the SCC is restricted to twelve, excluding the Chair, and comprises representatives nominated by IA Participant members of the IAF. Membership can be extended to the other IA Participants should the maximum of twelve not be achieved.

(ii) ATM Code Committee (**ACC**)

The IAF has delegated to the ACC the management of Volume 6 of the Code.

Membership of the ACC is determined by the IAF and consists of a mix of business and technical experts comprising a non-voting Chair from the IAF and representatives nominated by IA Participants who participate in the ATM System. The Chair may invite Operator Members and Affiliate Members who subscribe to the ATM System Code to attend all or part of a meeting of the ACC as appropriate.

(iii) Technical Security Sub-committee (**TSSC**)

The SCC has delegated to the TSSC consideration of security in Volumes 1 to 4 and aspects of card payments security or other payments security as referred to it from time to time. The TSSC makes recommendations to the SCC.

Membership of the TSCC is determined by the SCC and requires an appropriate level of knowledge and expertise. The TSSC comprises representatives of IA Participants nominated by the SCC and ACC, other IA representatives considered appropriate by the SCC, and an independent payments security expert recommended by AusPayNet management. The non-voting Chair, appointed from the SCC, may invite other Framework Participants, including Operator Members and Affiliate Members, to attend all or part of a meeting.

(iv) Evaluation Review Sub-committee (**ERSC**)

The SCC has delegated to the ERSC consideration of device approval applications on behalf of AusPayNet including reviewing standard and non-standard device approval applications and recommending to AusPayNet whether to approve new devices.

The ERSC is convened as required and members with an appropriate level of expertise are drawn on as required from the SCC, TSSC and the ACC, together with experts from Operator Members or independent security experts where

required. The Chair is appointed by the SCC and may be a member of the SCC, the ACC, the TSSC or an independent payments expert.

(v) Sanctions Tribunal

The IAF has established the Sanctions Tribunal as a sub-committee and has delegated the compliance with the threshold requirements in the Code (**Threshold Requirements**) to it. Threshold Requirements are requirements under the Regulations or the Code which the IAF determines to be so fundamental to the integrity and safety of card payments that, under the Regulations, compliance is to be enforceable by imposition of a fine.

The Sanctions Tribunal has the power to impose monetary fines in cases of breach of the Threshold Requirements and determines the quantum of fines, up to the maximum permitted fine, guided by a set of criteria that includes consideration of the severity of the conduct. The maximum fine is ultimately determined by the IAF and has been set at a level that is commensurate with similar arrangements in other payment systems currently operating in the market.[15]

6 Proposed conduct

6.1 Details of the conduct

Details of the provisions subject to this application are set out below. All of these provisions have been subject to the Authorisations granted by the ACCC in 2015, except where minor changes were implemented to the provisions as noted in the table below.

Provision Subject matter	Operation of Provision
Regulations	
Clause 4.1(c) Eligibility for Membership	This clause incorporates a requirement to comply with certification requirements set out in the Code and Regulations. Certification includes the statement that all devices, solutions and Point of Interaction (**POI**) technologies (which include POS devices and solutions provided to a merchant to undertake card payments and ATMs) used by the IA Participant are approved by AusPayNet (**Certification Requirements**). It provides that in order to be an IAC Framework Participant, a person must be able to comply with any applicable laws, AusPayNet's Constitution, the Regulations and Code. Prospective IA Participants must be able to comply with the Certification Requirements (subject to clause 4.2 which gives the IAF the ability to allow a prospective IA Participant that is unable to

[15] The maximum fine was originally set in the Regulations at $25,000. The amendments to the Regulations introduced 1 January 2020 gave power to the IAF to determine the maximum fine. Effective 1 January 2020, the maximum fine was set by the IAF at $100,000.

Provision Subject matter	Operation of Provision
	comply with the Certification Requirements to become a member subject to certain conditions).
Clause 5.1(b) Obligations for Framework Participants - Compliance with Certification Requirements	This provision provides that IA Framework Participants must comply with the Code, including, without limitation, any Certification Requirements (if applicable). This provision was amended on 1 January 2020 limiting its application to IA Participants being the only Framework Participants who are required to comply with Certification Requirements.
Clause 6.3 IAC Membership - Suspension	This clause permits the IAF to suspend a member for a number of reasons, including: ▪ if requested by any relevant prudential supervisor; ▪ by agreement of the member; ▪ if the member no longer satisfies all applicable requirements for membership; ▪ for insolvency (other than insolvency events that result in automatic termination); ▪ for breaches of membership obligations (if the member fails to rectify or adequately explain the breach within 30 days of a request from the Secretary of IAF); ▪ if the member's membership of an approved card payment system is suspended or terminated; ▪ if the approved card payment system of which the Framework Participant is a member has its approval withdrawn and they are not a member of any other approved card payment system; or ▪ if the member acts in a manner contrary to the interests of the IAC.
Clause 6.4 Effect of Suspension	This clause provides for the consequences of a suspension of IAC membership. Suspended members that are IA Participants are not entitled to exchange ATM transactions with any other IA Participant. Suspended members are also not entitled to vote at any IAC meeting (unless approved by the IAF) or to have their nominee to the IAF vote at meetings of the IAF (but may continue to attend and participate in such meetings). The IAF can in its discretion remove any certification granted to the suspended member.
Clause 6.5 Termination	This provision establishes the circumstances and processes by which a member of the IAC may cease to be a member. In particular, the Board may terminate a

Provision Subject matter	Operation of Provision
	membership of the IAC if a suspension event has occurred and not been remedied, the IAF has recommended terminating the membership, the Board has consulted with any relevant prudential supervisor and the member has had an opportunity to make submissions to the Board regarding the termination. The Board is not required to give any reasons for such a decision.[16] Membership can also be terminated where a member resigns, becomes insolvent, is wound up, dissolved or otherwise ceases to exist.[17]
Clause 6.7 FSC Processing Requirements – Suspension	This clause provides for automatic suspension of IAC membership for any member which is subject to a declaration made by the Minister under section 16AD of the *Banking Act 1959* (Cth) (**Banking Act**). This provision relates to claims made under the Financial Claims Scheme, designed to protect depositors of authorised deposit-taking institutions (banks, building societies and credit unions) and policyholders of general insurance companies from some potential losses due to the failure of these institutions.
Code	
Volume 1: Clause 3.1 – Compliance with applicable requirements for Framework Participants	This clause provides that, by completing the relevant checklists, an applicant or IA Participant confirms, for the benefit of all IA Participants and AusPayNet, that when it operates in the IAC with other IA Participants it meets the applicable requirements in force at that time.[18] This provision was amended on 1 January 2020 to acknowledge that the IA Participant's declaration that the Secure Cryptographic Devices it employs will be approved by AusPayNet includes SPoC solutions and POI technologies.
Volume 1: Clause 3.4 – Certification of Prospective IA Participant	This clause provides that each applicant must arrange for certification as part of their membership application, including completing the relevant New IA Participant Certification Checklist (see Annexure B to this Application) and the relevant Annual Security Audit (see Annexure C to this Application).

[16] Note: AusPayNet provided a letter to the ACCC (6 July 2015) stating that it is AusPayNet's expectation and intention that any decision to terminate a member would detail the facts, circumstances and reasons.
[17] AusPayNet is in the process of considering amendments to the Regulations to provide for different termination arrangements for Operator Members and Affiliate Members. The current termination provisions were developed to specifically apply (and protect) IA Participants because they are involved in the processing of ATM and EFTPOS transactions. These provisions continue to be relevant to IA Participants (and will not change), but are less applicable to Operator Members and Affiliate Members that are not involved with the processing of transactions and have no operational rights or obligations under the IAC (as noted above, their role is mainly advisory and consultative).
[18] Note: Volume 5 is under review following the introduction of eftpos Payments Australia Limited's own settlement rules.

Provision Subject matter	Operation of Provision
Volume 1: Annexure A – Annual Security Audit Checklist	This provision presents mandatory requirements for Acquirers and Issuers relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. Numerous amendments were made to the Annual Security Audit since the ACCC made its determination in connection with the Authorisations in 2015 (**2015 ACCC Determination**) reflecting technical changes to the security requirements and standards.
Volume 1: Annexure B – New IA Participant Certification	This provision requires IA Participant applicants to warrant that they satisfy the relevant requirements.
Volume 5: Clause 3.5 – Suspension for Failure to Settle Event	This clause provides for the automatic suspension of IAC membership, and of further exchanges of settlement items between the defaulter and other IA Participants pursuant to the Regulations and/or Code, if a member fails to settle.

As noted in section 4.4 above, upon completion of the Regulatory Reviews and the AusPayNet Reviews, AusPayNet will assess whether any proposed change(s) need to be implemented in the Regulations and Code, and inform the ACCC of the further proposed changes or additional provisions it deems appropriate to seek authorisation (if any). It was expected that such assessment will be completed between late 2020 to early 2021, and that implementing the changes reflecting that assessment may take at least two years. This proposed timeframe will be impacted by delays in completion of the Regulatory Reviews and AusPayNet Reviews as a consequence of the impact of COVID-19.

6.2 Impact of proposed conduct

Application is hereby made under section 91(c) of the Act, for authorisation of the provisions listed in section 6.1 and a Revocation and Substitute Authorisation. The Application is made as the proposed provisions may contain a cartel provision (as defined in section 45AD of the Act),or may have the purpose or effect of substantially lessening competition within the meaning of section 45 of the Act.

The persons who may be impacted by the provisions of the Regulations and the Code, as well as the proposed conduct contained within them are:

(a) potential IA Participants who are unable to comply with the certification requirements (Regulations, clause 4.1(c));

(b) Framework Participants who:[19]

(i) may be suspended where they no longer satisfy requirements for membership (Regulations, clause 6.3);

(ii) may be terminated where they fail to rectify a suspension event or otherwise satisfy the grounds for termination (Regulations, clause 6.5);

(c) IA Participants who:

(i) are required to comply with certification requirements (Annual Security Audits) (Regulations, clause 5.1(b); Volume 1, clause 3.4; Volume 1, Annexure A);

(ii) may be suspended where they become subject to a declaration made by the Minister under section 16AD of the Banking Act related to the Financial Claims Scheme (Regulations, clause 6.7); and

(iii) may be suspended where they suffer a Fail to Settle (**FTS**) event (Regulations, Volume 5, clause 3.5).

For the reasons outlined in this Application, AusPayNet considers that in all the circumstances the proposed certification, suspension and termination provisions for which authorisation is sought are likely to result in a public benefit that would outweigh the detriment to the public constituted by any lessening of competition arising from the conduct.

7 Public benefits

7.1 Background

In 2015, the ACCC determined that the certification, suspension and termination provisions are likely to result in public benefits through the protection of the security, efficiency and integrity of the IAC. In particular, the ACCC accepted that without the ability of IAC members to self-enforce compliance with the standards established by the IAC (through the ability to set minimum requirements for entry and issue monetary fines to participants and/or suspend or terminate membership for non-compliance), the operational efficiency of the IAC could be undermined and, at the extreme, could compromise the industry's ability to centrally coordinate the clearing and settlement of card transactions.

These benefits continue to apply and it continues to be the case that the benefits of the IAC Framework cannot be realised unless members act in accordance with the Regulations and Code (and there is an appropriate mechanism to enforce such compliance).

Further, we note that the benefits associated with the IAF Framework are important not just to members of the IAC, but also to all end-users of the payments system – including consumers and

[19] Although in the future, these provisions may only apply to IA Participants. See footnote 17.

merchants – and the wider payments industry. Recent examples that illustrate how these benefits arise include the following:

(a) **Development of the Card-Not-Present (CNP) Fraud Mitigation Framework (CNP Framework).**

The CNP Framework, developed by AusPayNet following extensive collaboration with over 60 organisations including all key stakeholders and the RBA, is designed to reduce the levels of online card fraud (which represents almost 85% of all card fraud on Australian cards), to build consumer trust and to support continued growth in e-commerce. Volume 7 of the Code (Card Not Present Code) (**CNP Code**) (which incorporates the CNP Framework into the IAC Framework) was adopted in July 2019 and imposes reporting obligations upon Issuers and Acquirers against fraud thresholds and performance obligations upon Issuers, Acquirers and merchants when thresholds are breached.

In the nine months since the CNP Code came into force:

(i) the overall CNP merchant fraud rate has fallen from 12.3c per A$100.00 of commerce, to 9.9c per A$100.00 of commerce;

(ii) the average fraud rate across AusPayNet Issuers has fallen by 35%; and

(iii) of the 88 merchants in breach of the merchant fraud threshold at the start of the third reporting period, representing 33% of total fraud reported under the CNP Framework, 66 merchants have now reduced their fraud rate below the threshold.

(b) **Development of open-loop contactless payments for transit.**

AusPayNet, in collaboration with the payments industry and transport authorities, produced in 2017 an Open Loop Transport Payments Framework (**Open Loop Framework**) for use by transport authorities and/or local transport operators in Australia. The Open Loop Framework allows commuters to use their own payment card (or device, such as a smart phone or wearable) to tap on and off transport, instead of a closed-loop card (e.g. Opal, Myki etc). Version 4 of the Open Loop Framework was issued in December 2019, with additional elements including a scheme comparison table, mobility as a service, station parking and toll integration, discount/account management, and QR codes. A further review will be undertaken in mid-2020, addressing the evolving payments and transport landscapes. Transport operators expressed their appreciation for AusPayNet's ability to convene a working group with broad representation across the financial institutions and transport operators, under the auspices of the IAC.

(c) **Development of Guidelines for Accessible PIN Entry on Touchscreens.**

Innovation in payment technologies has provided many benefits for retailers, merchants and customers. However, with these new technologies comes the need to ensure inclusion and accessibility for all users. A working group comprising IAC members undertook an extensive consultation process with people living with vision and / or motor impairments, representative bodies for the disability community, their networks and their supporters. The community identified that the ability to enter PINs securely and independently on touchscreen POS devices, also referred to as "PIN on glass", is an area where accessibility and inclusiveness can be challenging in making independent financial transactions. AusPayNet's Guidelines for Accessible PIN Entry on Touchscreens were published on 3 December 2019. These guidelines, a world first, are designed to make it easier for IAC members designing and deploying new POS devices to do so in a way that helps people living with vision and/or motor impairments to make payments on POS touchscreens. Following the launch of the guidelines, the IAC is exploring opportunities to further develop its work in the accessibility domain.

7.2 Specific benefits of certification

All IA Participants are required to comply at all times with the requirements in the Code. The certification provisions in the Regulations (clauses 4.1(c) and 5.1(b)) and the Code (Volume 1 Part 3) require that an IA Participant comply with initial certification requirements, upon applying to become a member, and with annual re-certification requirements throughout membership.

The certification checklist for new IA Participants (a copy of which is attached at Annexure B) is a representation and warranty for the benefit of all other Framework Participants and AusPayNet that the applicant meets all the technical, operational and security requirements set out in the Regulations and the Code applicable to their role as an Issuer or as an Acquirer. The representation must be signed off by an auditor who is satisfied as to the accuracy of the applicant's statements of compliance with the Code obligations. Where an applicant is unable to comply with the certification requirements, the IAF may allow a prospective applicant to become a conditional member if the areas of non-compliance are not material to the security, integrity or efficiency of the IAC or the exchange of payment messages or transactions and the applicant will be able to comply with the certification requirements within 12 months.

An IA Participant's annual re-certification (a copy of which has been attached at Annexure C, Annual Security Audit) includes detailed statements from Acquirers regarding the management of cardholder PINs and associated cryptographic practices including details for all EFTPOS Terminals and ATMs deployed by the Acquirer. The annual certification for Issuers similarly requires detailed statements regarding the management of cardholder PINs and associated cryptographic practices including details for all deployed Security Control Modules (SCMs).

Issuer and Acquirer annual security audits must also be signed off by auditors. Where an IA Participant is unable to comply with certain requirements, the IA Participant may apply for exemption for a limited period of time. AusPayNet may grant the exemption if the remedial action/compensating controls are satisfactory having regard to the integrity and efficiency of the IAC. If granted, AusPayNet monitors the exemption and the IA Participant's path to compliance.

Both certification requirements remain fundamentally important in maintaining the integrity and efficacy of the IAC Framework and reducing risk in the payments system. These benefits can only be realised if members act in accordance with the Regulations and Code. Without the certification requirements and the associated sanction provisions for non-compliance, the efficacy and integrity of the IAC would be reduced, confidence of members would fall, and risk would be unnecessarily introduced to the payments system and its end users.

7.3 Specific benefits of suspension

Submissions received before the 2015 ACCC Determination contended that the IAC suspension and termination provisions promote the efficient operation of the relevant clearing systems and enhance their security and integrity, and that without these provisions the confidence of users of these systems would likely be diminished.[20] In 2015, the ACCC accepted that without the ability of IAC members to self-enforce compliance with the standards established by the IAC (through the ability to set minimum requirements for entry and fine participants and/or suspend or terminate membership for non-compliance) the operational efficiency of the IAC could be undermined.

Framework Participants may be suspended in circumstances including where:

(a) they are subject to prudential supervision and the relevant supervisor requests such suspension;
(b) an insolvency event occurs;
(c) they breach an obligation under the AusPayNet Constitution, Regulations or Code and fail to rectify or provide a satisfactory explanation within 30 days or if they engage in conduct reasonably regarded by the IAF as contrary to the interests of the IAC; or
(d) their membership of an Approved Card Payment System (**ACPS**) is suspended or terminated or the ACPS of which they are a member has its approval withdrawn.

The effect of suspension is that an IA Participant is not able to exchange ATM transactions with other IA Participants and is not entitled to vote at IAC and IAF meetings (if a member of the IAF) but is entitled to attend.

The significance of these provisions in protecting and enhancing the security, efficiency and integrity of card payments remains fundamental. The need to invoke the suspension provisions

[20] See Submissions of ASIC before draft ACCC decision, dated 29 May 2015 and submissions of CBA before draft ACCC decision, dated 21 May 2015.

is however tempered by the ability of IA Participants to apply for exemption from compliance with certain obligations for a limited period of time and by the ability to impose a fine on an IA Participant for non-compliance with the Code.

7.4 Specific benefits of termination

As stated in the 2015 application, without the ability of IAC members to self-enforce compliance with the standards established by the IAC (through the ability to set minimum requirements for entry and fine participants and/or suspend or terminate membership for non-compliance) the operational efficiency of the IAC could be undermined. In addition to the impact upon security in the payments system, at the extreme, this could compromise the industry's ability to centrally coordinate the clearing and settlement of EFTPOS and ATM transactions.

There are very limited circumstances where membership of an IA Participant, may (or would) be terminated and, in each instance, termination is subject to:

(a) the requirement that the IA Participant first be suspended and provided the opportunity to remedy the suspension event;

(b) the IAF's recommendation; and

(c) the Board providing the Framework Participant with the opportunity to make submissions.[21]

AusPayNet has never suspended or terminated an IA Participant, and the significance of such measure means that termination would only be used as an option of last resort.[22]

8 Public detriments

In its 2015 ACCC Determination, the ACCC stated that exclusion from the IAC would have an adverse effect on the financial institution concerned and potentially could make it very difficult for the institution to directly clear and settle consumer electronic payment instructions. Absent appropriate checks and balances on the use of the suspension and termination provisions has the potential to result in anti-competitive detriment.

The ACCC considered that the certification, suspension and termination provisions do not place unreasonable requirements on members and that there are adequate checks and balances on the manner in which they are employed including:

(a) if a member is subject to prudential supervision, the prudential supervisor must be consulted prior to termination of IAC membership;

[21] The limited circumstances currently equally apply to termination of an Operator Member and an Affiliate Member: see footnote 17 above.
[22] AusPayNet has also never terminated the membership of an Operator Member. However, for completeness, we note one recent instance where one Affiliate Member (i.e., a member who is not involved in the processing of transactions) ceased to engage with activities of IAC, ceased to attend meetings, respond to communications and stopped paying membership fees for a period of two years. Repeated attempts were made to contact the member without success, so it was not possible to secure a resignation. In these circumstances, a "termination" was formalised. IAC has not heard back from the Affiliate Member but notes membership would be reinstated if the member sought to engage with the IAC again.

(b) the representation of the RBA on the Board (responsible for membership termination decisions) and the right for the RBA to be represented on the IAF (responsible for certification of members and membership suspension decisions);

(c) the suspension and termination provisions can only be invoked in limited circumstances; and

(d) the ability of the IAF to impose fines for non-compliance with fundamental requirements under the Regulations or Code provides an alternative to suspension and termination of membership in appropriate cases.

The ACCC also considered that even if used, to the extent that suspension or termination may adversely affect the IAC member concerned, given the number of competing service providers this may not significantly affect competition for the clearing and settlement of consumer electronic payments more generally.

In addition, as stated in the 2015 application, any detriment from the certification, suspension and termination provisions and the IAC framework is mitigated in a context where:

(a) nothing in the Regulations or Code restricts IAC members in competing for the business of end users of card payment services; and

(b) the existence of the IAC does not preclude institutions from establishing other clearing arrangements outside the scope of the IAC regulatory infrastructure.

If set at an inappropriate level, minimum mandatory standards and procedures could potentially stifle innovation by network participants by potentially raising barriers to entry to the ATM and EFTPOS networks. However, AusPayNet submits that its minimum standards do not increase barriers to entry. As an example, the introduction of the non-standard device approval process in 2017 has enabled AusPayNet to promote and support secure innovation through a risk-based approach to the evaluation of devices and solutions that are outside the paradigm of current security standards.

The Regulations and Code also allow IA Participants to bilaterally agree to divergent standards from those established by the IAC, provided that the integrity, security and efficiency of the IAC overall is not diminished. AusPayNet submits that the remaining requirements applied to IAC members are a reflection of the practical requirements of providing value as an authorised deposit taking institution under the Banking Act (card issuers) or of clearing transactions (as acquirers and merchant principals).

It is also worth noting that the more proactive and transparent approach to compliance under the IAC relative to the CECS framework (i.e. the ability to fine participants through transparent and clear processes) has reduced the likelihood that the suspension and termination provisions would be triggered in the first place. The IAC spends time advocating for increased compliance, and invests time with IA Participants to ensure they achieve compliance with its requirements. Similar

to the provisions under the CECS rules, the Code provides that where an IA Participant is unable to comply with mandatory requirements, the Participant must apply for exemption and provide a compliance plan with a proposed date by which the Participant will achieve compliance. AusPayNet's compliance team actively monitors compliance plans and works with IA Participants to support their transition back to compliance. This is an ongoing process and is generally successful in ensuring IA Participants achieve compliance. Additionally, increased clarity and transparency around Threshold Requirements (ie, compliance requirements for which fines can be issued) has resulted in a substantial increase in compliance and therefore a reduced likelihood of the application of the suspension or termination provisions.

AusPayNet issued in late 2019 its first and to date only two fines for non-compliance with a Threshold Requirement – failure to provide an annual security audit. In accordance with the Regulations, all IA Participants were informed of the fine. It is anticipated that following the issuing of these fines, instances of non-compliance or continuing non-compliance with the Code (and potential risk for suspension and termination) will be even further lessened.

The recent increase in the maximum fine that may be awarded for non-compliance is designed to ensure that the possibility of fines remains a sufficient and appropriate inducement to compliance with the Regulations and Code.[23]

9 Balance of Public Benefit and Detriment

For the reasons outlined above, AusPayNet is satisfied that the likely benefit to the public would outweigh the detriment to the public including the detriment constituted by any lessening of competition that would be likely to result from the certification, suspension and termination provisions in the Regulations and Code. Accordingly, the relevant net public benefit tests are met.

10 Conclusion

For the reasons set out in this Application, the Applicant submits that the ACCC ought to grant authorisation of the above Code and Regulation provisions for a period of five years. The IAC Framework will create significant public benefits without material competitive detriments.

[23] Since the 2015 ACCC Determination, the IAF has increased the maximum fine previously prescribed in the Regulations to $100,000 commensurate with similar arrangements in other payment systems currently operating in the Australian market, and introduced a grading scheme for the imposition of fines referencing severity and impact of the breach relative to the integrity and safety of card payments.

ANNEXURE A – LIST OF MEMBERS OF THE IAC

Name of Institution	Address	Committee membership
IA Participant		
Adyen Australia Pty Limited	Level 6, 69 Reservoir Street, Surry Hills NSW 2165, Australia	IAF (via EMG)
Australia and New Zealand Banking Group Limited	Level 9, 833 Collins Street, Docklands VIC 3008, Australia	IAF, SCC, TSSC
Australian Settlements Limited	6C Geils Court, Deakin ACT 2600, Australia	IAF (via EMG), SCC
Bank of Queensland Limited	BOQ Centre, 259 Queen Street, Brisbane QLF 4000, Australia	IAF (via EMG), SCC, TSSC
Bendigo and Adelaide Bank Limited	Fountain Court, Bendigo VIC 3550, Australia	IAF (via EMG)
Citigroup Pty Limited	Level 15, 2 Park Street, 2 Park Street, Sydney NSW 2000, Australia	IAF (via EMG), ACC, SCC
Coles Group Limited	Level 1 Module 11, 800 Toorak Road, East Hawthorn VIC 3123, Australia	IAF, SCC, TSSC
Commonwealth Bank of Australia	Darling Park 1, Level 6 Tower 1, 201 Sussex Street, Sydney NSW 2000, Australia	IAF, ACC, SCC, TSSC

Cuscal Limited	Level 1, 1 Margaret Street, Sydney NSW 2154, Australia	IAF, ACC , SCC, TSSC
EFTEX Pty Limited	Level 5, 140 William Street, East Sydney NSW 2011, Australia	IAF (via EMG), ACC, SCC
Fiserv Solutions Limited	Level 13, 90 Arthur Street, North Sydney NSW 2060, Australia	IAF, ACC, SCC, TSSC
Indue Ltd	Level 3, 601 Coronation Drive, Toowong QLD 4066, Australia	IAF (via EMG), ACC, SCC
National Australia Bank Limited	800 Bourke Street, Docklands, Melbourne VIC 3008, Australia	IAF, ACC, SCC, TSSC
Suncorp-Metway Limited	RE061, GPO Box 1453, Brisbane QLD, 4001, Australia	IAF
Tyro Payments Limited	Level 1, 155 Clarence Street, Sydney NSW 2000, Australia	IAF (via EMG), TSSC
Westpac Banking Corporation	Level 1, 275 Kent Street, Sydney NSW 2000, Australia	IAF, ACC, SCC, TSSC
Windcave Pty Limited	33 Wilkinson Road, Auckland 1150, NZ	IAF (via EMG)
Woolworths Group Limited	1 Woolworths Way, Bella Vista NSW 2153, Australia	IAF, SCC
Operator Member		
American Express Australia Limited	GPO Box 1708, Sydney 2000, Australia	IAF (Observer)

eftpos Payments Australia Limited	GPO Box 126, Sydney NSW 2001, Australia	IAF (Observer), TSSC
Mastercard Asia/Pacific (Australia) Pty Ltd	Level 8, 100 Arthur Street, North Sydney NSW 2060, Australia	IAF (Observer)
Visa AP (Australia) Pty Ltd	Level 42, AMP Centre, 50 Bridge Street, Sydney NSW 2000, Australia	IAF (Observer)
Affiliate Member		
Advam Pty Ltd	Level 2, 26 Franklin Street, Adelaide SA 5000, Australia	
Cardtronics Australasia Pty Ltd	208/27 Mars Road, Lane Cove West, NSW 2066, Australia	ACC (Observer)
Diebold Nixdorf Australia Pty Limited	Suite 5, Ground Floor, Building C, 14 Rodborough Road, Frenchs Forest NSW 2086, Australia	ACC (Observer)
Gemalto	L14 Zenith Tower B, 821 Pacific Highway, Chatswood NSW 2067, Australia	
Giesecke & Devrient Australasia	94 Rushdale Street, Knoxfield VIC 3180, Australia	

Ingenico International (Pacific) Pty Ltd	Suite 1, 3 Minna Close, Belrose NSW 2085, Australia	
NCR Australia Pty Ltd	Level 9, 8-20 Napier Street, North Sydney NSW 2060, Australia	ACC (Observer)
Optus	Call Centre, Building A, Optus, 1 Lyonpark Rd, Macquarie Park NSW 2113, Australia	
Quest Payment Systems Pty Ltd	227 Burwood Road, Hawthorn VIC 3122, Australia	
Rambus Global Inc	Level 31, 120 Collins Street, Melbourne VIC 3000, Australia	
Southern Payment Systems Pty Ltd (trading as Pin Payments)	Level 1, 68 St Georges Terrace, Perth WA 6000, Australia	
Thales	World Trade Centre Northbank Wharf, Siddeley Street, Melbourne VIC 3005, Australia	
Threatmetrix Pty Ltd	Level 10, Tower 2/475 Victoria Road, Chatswood NSW 2067, Australia	
UL Transaction Security	709 Fiero Lane, Suite 25, San Luis Obispo 93420 CA, USA	
Verifone Pty Ltd	1/484 Graham Street, Port Melbourne VIC 3027, Australia	

LIST OF MEMERS OF IAC

Committee membership

IAF: Issuer and Acquirer Forum

IAF (via EMG): IAF via the Electing Member Group

SCC: Security Code Committee

ACC: ATM Code Committee

TSSC: Technical Security Sub Committee

ERSC: Evaluation Review Sub Committee

ANNEXURE B – COPY OF CERTIFICATION CHECKLIST FOR NEW FRAMEWORK PARTICIPANTS

ANNEXURE B NEW FRAMEWORK PARTICIPANT CERTIFICATION

Note: Annexure B.1 Acquirer Certification Checklist is ONLY to be completed by a new Framework Participant.

B.1 ACQUIRER CERTIFICATION CHECKLIST

To: The Secretary
Australian Payments Network Limited
Level 23
Tower 3, International Towers Sydney
300 Barangaroo Avenue
Sydney NSW 2000

Re: Issuers and Acquirers Community

From: Name of Applicant ("**Applicant**"): _____

Place of Incorporation: _____

ACN / ABN / ARBN: _____

Registered Office Address _____

_____

Name of Contact Person:: _____

Telephone Number: ( ) _____

Email Address: _____

CERTIFICATION OBJECTIVES

The objective of Certification is to ensure that each IAC Applicant that becomes an Acquirer confirms for the benefit of each other Framework Participant and the Company that it meets the technical, operational and security requirements applicable to Acquirers which are set out in IAC Code Set Volume 3 (Acquirers Code), IAC Code Set Volume 5 (Settlement Code) and IAC Code Set Volume 6 (ATM System Code) as applicable.

REPRESENTATIONS AND UNDERTAKINGS

By signing this Acquirer Certification Checklist, the Applicant:

(a) acknowledges that membership of IAC is conditional on the Applicant having obtained Certification in accordance with the IAC Regulations and Manual and that this Acquirer Certification Checklist is required to obtain that Certification;

(b) warrants that it satisfies the requirements applicable generally to Acquirers as set out in clause 2.1 of IAC Code Set Volume 3 (Acquirers Code), IAC Code Set Volume 5 (Settlement Code) and IAC Code Set Volume 6 (ATM System Code) as at the date of this Acquirer Certification Checklist, and that the information contained in this completed Acquirer Certification Checklist is correct and accurately reflects the results of system testing against current IAC requirements and including, if applicable, use of an appropriate test script supplied by the Company;

(c) if the Applicant is granted Certification, agrees to:

(i) immediately notify the Company if it becomes, or has become, aware that any information contained in this Acquirer Certification Checklist is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and

(ii) provide to the Company with full particulars of any such wrong or misleading information.

Terms used in this Acquirer Certification Checklist have the same meanings as in the IAC Code Set unless otherwise defined.

SIGNED for and behalf of **THE APPLICANT**

By signing this Acquirer Certification Checklist the signatory states that the signatory is duly authorised to sign this Acquirer Certification Checklist for and on behalf of the Applicant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Certification Checklist the signatory states that the signatory is duly authorised to sign this Acquirer Certification Checklist as auditor for and on behalf of the Applicant and that the signatory is satisfied with the accuracy of the responses contained within the certification checklist.

Name of Auditor	Signature of Auditor
Date	

Note: This Annexure B.2 Issuer Certification Checklist is ONLY to be completed by a new Framework Participant.

B.2 ISSUER CERTIFICATION CHECKLIST

To: The Secretary
Australian Payments Network Limited
Level 23
Tower 3, International Towers Sydney
300 Barangaroo Avenue
Sydney NSW 2000

Re: Issuers and Acquirers Community

From: Name of Applicant ("**Applicant**"): _____

Place of Incorporation: _____

ACN / ABN / ARBN: _____

Registered Office Address _____

_____

Name of Contact Person: _____

Telephone Number: ( ) _____

Email Address: _____

CERTIFICATION OBJECTIVES

The objective of Certification is to ensure that each IAC Applicant that becomes an Issuer confirms for the benefit of each other Framework Participant and the Company that it meets the technical, operational and security requirements applicable to Issuers which are set out in IAC Code Set Volume 2 (Issuers Code) and IAC Code Set Volume 5 (Settlement Code) as applicable.

REPRESENTATIONS AND UNDERTAKINGS

By signing this Issuer Certification Checklist, the Applicant:

(a) acknowledges that membership of IAC is conditional on the Applicant having obtained Certification in accordance with the IAC Regulations and Manual and that this Issuer Certification Checklist is required to obtain that Certification;

(b) warrants that it satisfies the requirements applicable generally to Issuers as set out in Part 5 of IAC Code Set Volume 2 (Issuers Code) and IAC Code Set Volume 5 (Settlement Code) as applicable, as at the date of this Issuer Certification Checklist, and that the information contained in this completed Issuer Certification Checklist is correct and accurately reflects the results of system testing against current IAC requirements and including, if applicable, use of an appropriate test script supplied by the Company;

(c) if the Applicant is granted Certification, agrees to:

(i) immediately notify the Company if it becomes, or has become, aware that any information contained in this Issuer Certification Checklist is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and

(ii) provide to the Company with full particulars of any such wrong or misleading information.

Terms used in this Issuer Certification Checklist have the same meanings as in the IAC Code Set unless otherwise defined.

SIGNED for and behalf of **THE APPLICANT**

By signing this Issuer Certification Checklist the signatory states that the signatory is duly authorised to sign this Issuer Certification Checklist for and on behalf of the Applicant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Issuer Certification Checklist the signatory states that the signatory is duly authorised to sign this Issuer Certification Checklist as auditor for and on behalf of the Applicant and that the signatory is satisfied with the accuracy of the responses contained within the Issuer Certification Checklist.

Name of Auditor	Signature of Auditor
Date	

Next page is C.1

ANNEXURE C – COPY OF ANNUAL SECURITY AUDIT

ANNEXURE A ANNUAL SECURITY AUDITS

Note: Annexure A.1 Acquirer Annual Security Audit (Part 1) must be completed annually by all Acquirer Framework Participants in combination with either Annexure A.2 Acquirer Annual Security Audit (Part 2) or a duly signed copy of a Visa PIN Security Requirements Self Audit

Note: Annexure A.3 Issuer Annual Security Audit must be completed annually by all Issuer Framework Participants.

A.1 ACQUIRER ANNUAL SECURITY AUDIT (PART 1)

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805.

The following documents are referenced in this checklist;

ISO 9564.1-2011	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems
AS 2805.6.1-2002/Amdt 3/2007	Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles
AS 2805.14.2-2009	Electronic funds transfer – Requirements for interfaces Part 14.2: Secure Cryptographic Devices (retail) – Security compliance checklists for devices used in magnetic stripe systems

Amended effective 21.11.16

A.1.1 General Security Controls

(a) Please provide the details for all EFTPOS Terminals and ATMs that you currently have deployed. Please use a separate sheet if necessary.

Amended effective 20.8.18

ATM	EFTPOS Terminal	Manufacturer	Model No.	Approx Quantity
☐	☐			
☐	☐			
☐	☐			
☐	☐			
☐	☐			
☐	☐			

(b) Please provide the details for all SCM devices that you currently have deployed. Please use a separate sheet if necessary. Inserted effective 1.1.16

Manufacturer	Model No.	Quantity

(c) Third Party Providers

Please provide details of all Third Party Providers used in providing acquiring services. Please use a separate sheet if necessary.

Third Party Providers	Type of service provided

(d) All parties to the Interchange, including merchants, Acquirers, Third Party Providers and any intermediate network entities maintain procedures and practices to prevent the unauthorised disclosure of Cardholder Data, which includes but is not necessarily limited to the Primary Account Number, Cardholder Name, Service Code, Expiration Date,

Reference IAC Code Set Volume 3, clause 2.5.

Yes	No	N/A

If N/A response: Reason

(e) Sensitive authentication data, including but not limited to, Full magnetic stripe (or equivalent), CVC2/CVV2/CID, PIN/PIN Block is not stored, outside of an SCD, subsequent to Authorisation.

Reference IAC Code Set Volume 3, clause 2.6.

Yes	No	N/A

If N/A response: Reason

(f) Message Authentication applies to all IAC Interchange Links. The MAC must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1. All interchange PIN and MAC cryptographic functions are performed within a Tamper responsive SCM. Amended effective 1.1.20

Reference AS 2805.4.1

Yes	No	N/A

If N/A response: Reason

(g) Message Authentication applies to all Terminal to Acquirer Links for all financial and key management messages

Reference AS 2805.4.1

Yes	No	N/A

If N/A response: Reason

(h) IAC Interchange Lines are subject to whole-of-message encryption in accordance with AS 2805.5.4 (IAC Code Set Volume 3, clause 2.4.4) Amended effective 1.1.20

Yes	No	N/A

If N/A response: Reason

(i) IAC Interchange Links comply with the key management practices of IAC Code Set Volume 4, clause 4.5.2. Amended effective 1.1.20

Yes	No	N/A

If N/A response: Reason

(j) IAC Interchange Lines comply with the key management practices of IAC Code Set Volume 4, clause 4.7.2 (if applicable). Amended effective 1.1.20

Yes	No	N/A

If N/A response: Reason

(k) Terminal key management practices comply with the requirements of IAC Code Set Volume 4, clause 4.8.2

Yes	No	N/A

If N/A response: Reason

(l) Host systems which support Terminals using the TCP/IP protocol for communications meet the requirements of IAC Code Set Volume 3, clause 3.5

Yes	No	N/A

If N/A response: Reason

(m) Privacy of communication complies with AS 2805.9 for all Terminal to Acquirer links, or any other privacy of communication standard approved by the committee of management (EFTPOS Terminals only) IAC Code Set Volume 3, clause 2.4.5

Yes	No	N/A

If N/A response: Reason

(n) Documented procedures exist, and are followed to ensure all PINs are encrypted using DEA 3 when transmitted outside a Secure Cryptographic Device. PINs are not stored in any form. If a transaction is logged, the encrypted PIN block is masked or deleted from the record before it is logged. Amended effective 29.4.16

Reference AS 2805.3.1 clauses 5.2 and 12.2.

Yes	No	N/A

If N/A response: Reason

(o) Each type of SCD used in Interchange and those devices providing a Remote Management Solution for Security Control Modules have been evaluated by a Company accredited Evaluation Facility using the method in and against the criteria in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management), and have been approved for use by the Company. Last amended effective 21.11.16

An SCD includes but is not limited to an ATM, PED, SCM or Key Loading and Transfer Device.

Reference ISO 9564.1, clause 5.1; AS 2805.14.2.

Yes	No	N/A

If N/A response: Reason

(p) Clear text PINs and Clear-text keys exist only in an SCD designed for use in its operational environment.

Yes	No	N/A

If N/A response: Reason

(q) All deployed ATM payment applications are either listed on the AusPayNet approved devices list or have been reviewed by the Acquirer or a trusted third party on behalf of the Acquirer and have been shown to contain no security vulnerabilities or other security weakness. Inserted effective 20.8.18

Yes	No	N/A

If N/A response: Reason

A.1.2 Device Management

(a) Documented procedures exist, and are followed, to determine that the SCD is managed in accordance with the privacy shielding requirements in clause 3.2.3 of IAC Code Set Volume 3 (Acquirers Code).

Yes	No	N/A

If N/A response: Reason

(b) For Terminals running multiple applications, documented, auditable, key management procedures exist and are followed for the secure management of any key used in the authentication processes associated with Terminal software authentication. Amended effective 20.8.18

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist, and are followed, to ensure that any Remote Management Solution for an SCM is managed in accordance with the requirements of clause 3.3.4 of IAC Code Set Volume 3 (Acquirers Code).

Yes	No	N/A

If N/A response: Reason

(d) From 1 January 2013, all symmetric encryption functionality weaker than DES-3 has been disabled within every deployed SCM.

Yes	No	N/A

If N/A response: Reason

(e) Acquirers shall maintain a register of all authorised non-payment applications per device. Inserted effective 1.1.15

Yes	No	N/A

If N/A response: Reason

(f) Operating procedures and the design of devices utilized require that the Cardholder can reasonably prevent others from observing the entered PIN. Amended effective 21.11.16

Reference AS 2805.14.2, clause B.2.1.B6.

Yes	No	N/A

If N/A response: Reason

A.1.3 General Key Management

Inserted effective 1.1.16

(a) Documented procedures exist and are followed to ensure if keys are loaded or transported using an electronic key loading device then:

(i) The key loading device has been evaluated and meets the applicable security requirements (see clause A.2.2);

(ii) The key loading device is under the supervision of a person authorised by management, or is stored in a secure manner (e.g. in a safe) such that no unauthorised person may have access to it; and

(iii) The key loading device is designed or controlled so that only authorised personnel under dual control can utilise and enable it to output a key into another SCD. Such personnel ensure that the transfer is not being monitored, e.g., that there is no key recording device inserted between the SCDs.

Yes	No	N/A

If N/A response: Reason

(b) If for archival purposes, reconstruction of a given key is required at a later date, procedures exist and are followed to ensure the key is retained in a form such as to preclude it being intentionally used again as active keying material.

Inserted effective 1.1.16

Yes	No	N/A

If N/A response: Reason

A.1.4 Supplementary Questions for Acquirers who are submitting Visa Audits

Note: The following requirements are only to be completed by Acquirers submitting a duly signed copy of a Visa PIN Security Requirements Self Audit to accompany this A.1 Acquirer Annual Security Audit (Part 1) submission (as described in clause 3.2.1).

(a) Compliance with the requirements of the Visa PIN Security Requirements Self Audit has been confirmed.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed for each of the individual requirements in the Visa PIN security Requirement Self Audit.

Yes	No	N/A

If N/A response: Reason

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Acquirer Annual Security Audit (Part 1) the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Annual Security Audit (Part 1) the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

A.2 ACQUIRER ANNUAL SECURITY AUDIT (PART 2)

Annexure A.2 Acquirer Annual Security Audit (Part 2) must be completed unless submitting a duly signed copy of a Visa PIN Security Requirements Self Audit.

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805 and ISO 9564. Amended effective 21.11.16

A.2.1 General Security Controls

Amended effective 21.11.16

(a) Any clear-text PIN block format combined with a PIN encryption process has the characteristics that, for different accounts, encryption of the same PIN value under a given encryption key does not predictably produce the same encrypted results. (Note the format 0 and format 3 PIN blocks specified in ISO 9564.1 meet this requirement.)

Reference ISO 9564.1, clause 9.3 and 9.4.

Yes	No	N/A

If N/A response: Reason

(b) No procedure requires or permits the Cardholder to disclose the PIN (verbally or in writing). Amended effective 21.11.16

Reference ISO 9564.1, clause 6.1.3.

Yes	No	N/A

If N/A response: Reason

A.2.2 Device Management

(a) Any SCD capable of encrypting a key and producing a cryptogram of that key is protected against unauthorised use to encrypt known keys or known key components. This protection takes the form of either or both of the following:

(i) Dual Access controls are required to enable the key encrypting functions; and/or

(ii) Physical protection of the equipment (e.g., locked access to it) under dual control.

Reference AS 2805.14.2, clauses E12 and E13.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist, and are followed, to determine that an SCD has not been subject to unauthorised modification or substitution prior to loading cryptographic keys. This assurance takes the form of one or more of the following procedures:

(i) Physical inspection and/or testing of the equipment immediately prior to key loading; and/or

(ii) Physical protection of the equipment.

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist, and are followed, to ensure that the SCD is physically protected (e.g., locked access) to protect against the possibility that the SCD may be stolen, modified in an unauthorised way, and then returned to storage without detection.

Yes	No	N/A

If N/A response: Reason

(a) Documented procedures exist to ensure that keys are not installed in any SCD where suspicious alteration of an SCD has been detected until the SCD has been inspected and a reasonable degree of assurance has been reached that the SCD has not been subject to any unauthorised physical or logical modifications.

Yes	No	N/A

If N/A response: Reason

(b) Documented, auditable, key management procedures exist and are followed for the secure management of any Acquirer controlled key used in the authentication processes associated with Terminal software authentication. Amended effective 20.8.18

Yes	No	N/A

If N/A response: Reason

(c) If the SCD can translate a PIN from one PIN block format to another or if the SCD verifies PINS, then procedures exist, and are followed, to prevent or detect, repeated unauthorised calls resulting in the exhaustive determination of PINS. Inserted effective 1.1.16

Yes	No	N/A

If N/A response: Reason

A.2.3 General Key Management

(a) Documented procedures exist, and are followed to control keys so that they exist in only one or more of the permissible forms:

(i) In a SCD;

(ii) Encrypted under a DEA 2 or DEA 3 key; or

(iii) Managed as two or more full length components using the principles of dual control and split knowledge.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure a person entrusted with a key component reasonably protects that component such that no person (not similarly entrusted with that component) can observe or otherwise obtain that component.

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist and are followed to ensure keys and key components are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist to ensure each of the following:

(i) A key is changed if its compromise is known or suspected;

(ii) Keys encrypted under or derived from a compromised key are changed;

(iii) Key is not changed to a variant or a transformation of the compromised key; and

(iv) The amount of time in which the compromised key remains active is consistent with the risk to all affected parties.

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure a key is used for only a single designated purpose.

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure that when a key is installed under dual control using key components that these key components are only combined within a SCD.

Yes	No	N/A

If N/A response: Reason

(g) Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. Key components are combined using one of the following functions:

(i) XOR; and/or

(ii) Encryption via DEA.

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure when in secure transit, cleartext key components are protected from compromise in one of the following manners: Amended effective 21.11.16

(i) Key components are transported in separate tamper-evident packaging; and/or

(ii) Key components are transported in a device meeting the requirements of a Physically Secure Device.

Reference ISO 9564.1 and AS 2805.14.1.

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure a cleartext key component is:

(i) Under the supervision of a person authorised by management with access to this component; or

(ii) Locked in a security container in such a way that can be obtained only by a person with authorized access; or

(iii) In secure transit; or

(iv) In a physically secure SCD.

Yes	No	N/A

If N/A response: Reason

(j) Documented procedures exist and are followed to protect the transfer of a key or key component into SCDs so as to prevent the disclosure of the key or key components. Examples of procedures include physical inspection of the SCD equipment to detect evidence of monitoring and dual custody of the loading process.

Yes	No	N/A

If N/A response: Reason

(k) Documented procedures exist and are followed to ensure that a key exists at only the minimal number of locations consistent with the operation of the system (e.g., including disaster recovery purposes, dual processing sites).

Yes	No	N/A

If N/A response: Reason

(l) Documented procedures exist and are followed, to prohibit, except by chance, the entry or use of the same key in more than one PIN entry device.

Yes	No	N/A

If N/A response: Reason

(m) Documented procedures exist and are followed to ensure a key shared between communicating parties is not shared, except by chance, between any other communicating parties.

Yes	No	N/A

If N/A response: Reason

(n) Procedures exist and are followed to ensure a key or key component that has been used for a cryptographic purpose is erased or destroyed when it is no longer required using approved destruction procedures.

Yes	No	N/A

If N/A response: Reason

(o) Documented procedures exist and are followed to ensure that when a key transport key (KTK) is changed because its compromise is known or suspected, an organisation which has previously shared the key is informed of the compromise even if the KTK is no longer in use.

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to monitor cryptographic synchronisation errors and to investigate multiple synchronisation errors to ensure the SCD is not being misused to determine keys or PINs.

Yes	No	N/A

If N/A response: Reason

(q) Documented procedures exist and are followed to ensure if two or more of a key's components are stored within the same security container (which is under dual control), then the components are secured in tamper evident packaging to preclude one component holder from gaining access to the other component.

Yes	No	N/A

If N/A response: Reason

(r) Documented procedures exist and are followed to ensure a key loading device does not retain a clear-text copy of any key it has successfully transferred.

Yes	No	N/A

If N/A response: Reason

(s) If personal computers are used to load encryption keys into a PIN entry device, procedures exist and are followed to ensure, at a minimum the following controls:

(i) The software loads the encryption key without recording the value in non-volatile storage;

(ii) Hardware used for the key loading function is maintained under dual control;

(iii) Hardware use is monitored and logs of key loading activity are maintained;

(iv) Cable attachments and hardware are examined before each use to ensure that the equipment is free from tampering;

(v) That the computer is started from power off position for each site's key loading activity; and

(vi) An SCD is used in conjunction with the personal computer to complete all cryptographic processing and for the storage of all encryption keys.

Yes	No	N/A

If N/A response: Reason

(t) Documented procedures exist and are followed to maintain a record of every instance when a container securing cryptographic materials is opened to record date, time, person(s) involved and the purpose of the access.

Yes	No	N/A

If N/A response: Reason

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Acquirer Annual Security Audit (Part 2) the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Annual Security Audit (Part 2) the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

A.3 ISSUER ANNUAL SECURITY AUDIT

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805 and IAC Code Set Volume 4. Amended effective 1.1.19

The following documents are referenced in this checklist;

AS 2805.6.1-2002/Amdt 3/2007	Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles
AS 2805.14.1-2011	Electronic funds transfer – Requirements for interfaces – Secure cryptographic devices (retail) – Concepts, requirements and evaluation methods. Inserted effective 21.11.16
AS 2805.14.2-2009	Electronic funds transfer – Requirements for interfaces Part 14.2: Secure Cryptographic Devices (retail) – Security compliance checklists for devices used in financial transactions. Amended effective 21.11.16
ISO 9564.1-2017	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems. Inserted effective 1.1.19
ISO 9564.2-2014	Financial services – Personal Identification Number (PIN) management and security – Part 2: Approved algorithms for PIN encipherment. Inserted effective 1.1.19
ISO 13491.1-2016	Financial Services – Secure cryptographic device (retail) – Part 1: Concepts, requirements and evaluation methods. Inserted effective 1.1.19
ISO.13491.2-2017	Financial Services – Secure cryptographic devices (retail) – Part 2: Security compliance checklists for devices sued in financial transactions. Inserted effective 1.1.19
Shamir, Adi (1979)	"How to share a secret", Communications of the ACM, 22 (11): 612-613, doi:10.1145/359168.359176. Inserted effective 1.1.19

A.3.1 General Security Controls

Inserted effective 1.1.19

These controls apply to all issuing services including issuing obligations in Interchange. Section 3.2 will address specific requirements and concerns where Issuers allow the transmission of cardholder PINs over open Networks in compliance with Part 3 of IAC Code Set Volume 2.

(a) Please provide the details for all SCM devices that you currently have deployed. Please use a separate sheet if necessary.

Manufacturer	Model No.	Quantity.

(b) Third Party Providers

Please provide details of all Third Party Providers associated with the management of PINs and the associated cryptographic practices used in providing issuing services. Please use a separate sheet if necessary.

Third Party Providers	**Type of service provided**

Last amended effective 1.1.19

(c) Any clear-text PIN block format combined with a PIN encryption process has the characteristics that, for different accounts, encryption of the same PIN value under a given encryption key does not predictably produce the same encrypted results. (Note the format 0, format 3 and format 4 PIN blocks specified in ISO 9564.1 meet this requirement.)

Reference ISO 9564.1, clauses 9.3.2, 9.3.5 and 9.4.2.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist and are followed to ensure all PIN blocks are encrypted using DEA 3 or AES when transmitted outside a Secure Cryptographic Device, except where Part 3 of IAC Code Set Volume 2 applies. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged. Last amended effective 1.1.19

Reference ISO 9564.1 clause 4.2 and ISO 9564.2.

Yes	No	N/A

If N/A response: Reason

(e) No procedure requires or permits the Cardholder to disclose the PIN verbally or in writing. Amended effective 21.11.16

Reference ISO 9564.1 clause 4.2(h).

Yes	No	N/A

If N/A response: Reason

(f) All parties to the Interchange, including Third Party Providers and any intermediate network entities maintain procedures and practices to prevent the unauthorised disclosure of Cardholder Data, which includes but is not necessarily limited to the Primary Account Number, Cardholder Name, Service Code, Expiration Date,

Yes	No	N/A

If N/A response: Reason

(g) Message Authentication applies to all IAC Interchange Links. The MAC must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1. All interchange PIN and MAC cryptographic functions are performed within a tamper responsive SCM. Amended effective 1.1.20

Reference AS 2805.4.1

Yes	No	N/A

If N/A response: Reason

(h) IAC Interchange Lines are subject to whole-of-message encryption in accordance with AS 2805.5.4 (IAC Code Set Volume 3, clause 2.4.4) Amended effective 1.1.20

Yes	No	N/A

If N/A response: Reason

(i) IAC Interchange Links comply with the key management practices of IAC Code Set Volume 4, clause 4.5.2 Amended effective 1.1.20

Yes	No	N/A

If N/A response: Reason

(j) IAC Interchange Lines comply with the key management practices of IAC Code Set Volume 4, clause 4.7.2 (if applicable). Amended effective 1.1.20

Yes	No	N/A

If N/A response: Reason

A.3.2 Device Management

(a) Each type of SCM used in Interchange, and those devices providing a Remote Management Solution for Security Control Modules have been evaluated by a Company accredited Evaluation Facility using the method and against the criteria given in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and have been approved for use by the Company. Last amended effective 1.1.19

Reference AS 2805.14.1, AS 2805.14.2 ISO 13491.1, ISO 13491.2, IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist, and are followed, to ensure that any Remote Management Solution for an SCM is managed in accordance with the requirements of IAC Code Set Volume 2, clause4.5.

Yes	No	N/A

If N/A response: Reason

A.3.3 Key Management

(a) Documented procedures exist, and are followed to control keys so that they exist in only one or more of the permissible forms: Amended effective 1.1.19

(i) In a SCD;

(ii) Encrypted under a DEA 2, DEA 3 or AES key;

(iii) Managed as two or more full length components using the principles of dual control and split knowledge; and/or

(iv) Managed as m of n key shares under a Shamir Secret Sharing Scheme.

Reference Shamir, Adi (1979).

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure a person entrusted with a key component or a key share, reasonably protects that component or share such that no person (not similarly entrusted with that component or share) can observe or otherwise obtain that component or share. Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist and are followed to ensure keys, key components and key shares are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys. Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist to ensure each of the following:

(i) A key is changed if its compromise is known or suspected;

(ii) Keys encrypted under or derived from a compromised key are changed;

(iii) A key is not changed to a variant or a transformation of the compromised key; and

(iv) The amount of time in which the compromised key remains active is consistent with the risk to all affected parties.

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure a key is used for only a single designated purpose.

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure that when a key is installed under dual control using key components that these key components or key shares are only combined within a SCD.

Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(g) Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. Key components are combined using one of the following functions: Amended effective 1.1.19

(i) XOR;

(ii) Encryption via DEA 2, - DEA 3 or AES; and/or.

(iii) Key shares are combined to form a key by a process using polynomial interpolation such that no active bit of the key could be determined without knowledge of m of n key shares.

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure when in secure transit, cleartext key components are protected from compromise in one of the following manners: Last amended effective 1.1.19

(i) Key components are transported in separate tamper-evident packaging; or

(ii) Key components are transported in a device meeting the requirements of a Secure Cryptographic Device.

Reference ISO 13491.1 (AS 2085.14.1).

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure a cleartext key component is: Amended effective 1.1.19

(i) Under the supervision of a person authorised by management with access to this component; or

(ii) Locked in a security container in such a way that can be obtained only by a person with authorized access; or

(iii) In secure transit; or

(iv) In a Secure Cryptographic Device.

Yes	No	N/A

If N/A response: Reason

(j) Documented procedures exist and are followed to ensure if keys are loaded or transported using an electronic key loading device then: Amended effective 1.1.19

(i) The key loading device has been evaluated and meets the applicable security requirements (see IAC Code Set Volume 4 clause2.4.12);

(ii) The key loading device is under the supervision of a person authorised by management, or is stored in a secure manner (e.g., in a safe) such that no unauthorised person may have access to it; and

(iii) The key loading device is designed or controlled so that only authorised personnel under dual control can utilise and enable it to output a key into another SCD. Such personnel ensure that the transfer is not being monitored, e.g., that there is no key recording device inserted between the SCDs.

Yes	No	N/A

If N/A response: Reason

(k) Documented procedures exist and are followed to protect the transfer of a key, key component or key share into SCMs so as to prevent the disclosure of the key, key components or key shares. Examples of procedures include physical inspection of the SCD equipment to detect evidence of monitoring and dual custody of the loading process. Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(l) Documented procedures exist and are followed to ensure that a key exists at only the minimal number of locations consistent with the operation of the system (e.g., including disaster recovery purposes, dual processing sites).

Yes	No	N/A

If N/A response: Reason

(m) If for archival purposes, reconstruction of a given key is required at a later date, procedures exist and are followed to ensure the key is retained in a manner such as to preclude it being intentionally used again as active keying material.

Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(n) Documented procedures exist and are followed to ensure a key shared between communicating parties is not shared between any other communicating parties.

Yes	No	N/A

If N/A response: Reason

(o) Procedures exist and are followed to ensure a key, key component or key share that has been used for a cryptographic purpose is erased or destroyed when it is no longer required using approved destruction procedures.

Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to ensure that when a key transport key (KTK) is changed because its compromise is known or suspected, an organisation which has previously shared the key is informed of the compromise even if the KTK is no longer in use.

Yes	No	N/A

If N/A response: Reason

(q) Documented procedures exist and are followed to ensure if two or more of a key's components or shares are stored within the same security container (which is under dual control), then the components and shares are secured in tamper evident packaging to preclude one component or share holder from gaining access to other components or in the case of key shares in an m of n key sharing scheme, m shares.

Amended effective 1.1.19

Yes	No	N/A

If N/A response: Reason

(r) Documented procedures exist and are followed to ensure a key loading device does not retain a clear-text copy of any key it has successfully transferred.

Yes	No	N/A

If N/A response: Reason

(s) Documented procedures exist and are followed to maintain a record of every instance when a container securing cryptographic materials is opened to record date, time, person(s) involved and the purpose of the access.

Yes	No	N/A

If N/A response: Reason

A.3.4 General Security Controls for PIN Usage over Open Networks

Inserted effective 1.1.19

This section addresses the minimum requirements for PIN usage in Issuer functionality offered over open networks which don't employ secure cryptographic devices for PIN entry. This includes, but is not limited to, PIN change and delivery mechanisms, internet banking registration systems, and other internet product offerings by an Issuer (Part 3 of IAC Code Set Volume 2).

(a) Documented procedures exist and are followed to ensure the Issuer complies with the current version of ISO 9546.1 to the maximum extent possible consistent with the Issuer's security policies and risk management requirements.

Reference IAC Code Set Volume 2 clause 2.1

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure the concurrent existence of clear text PIN and PAN is kept to the absolute minimum possible consistent with the functionality being implemented.

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist and are followed to ensure the Identification of the Cardholder uses additional identifying data other than that contained on or in the Card itself.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist and are followed to ensure Issuers provide Cardholders with a means to determine that the dialogue with the Issuer is genuine.

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure the Issuer uses calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and implements additional Cardholder authentication.

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure all systems transporting PIN data or PAN data, or both, over open networks provide mutual assurance to the Issuer and Cardholder that they are both genuine.

Yes	No	N/A

If N/A response: Reason

(g) Documented procedures exist and are followed to ensure all events involving the transmission of the PIN or PAN, or both, back to the Cardholder are acknowledged using an out-of-band mechanism.

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure Issuers provide Cardholders with the means to confirm the outcome of events involving a PIN or a PAN or both.

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure Issuers consider threats arsing through device convergence resulting from technological change in selecting acceptable out-of-band mechanisms.

Yes	No	N/A

If N/A response: Reason

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Issuer Annual Security Audit the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person

Signature of Authorised Person

Office Held

Date

AUDITOR SIGNOFF

By signing this Issuer Annual Security Audit the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor

Signature of Auditor

Date

Next page is B.1

END OF DOCUMENT