Response to Treasury on the Payments System Modernisation (Licensing: Defining Payment Functions) Consultation Paper

Table of contents

Group Country Manager Letter

19 July 2023

Director
Payments Licensing Unit
The Treasury
Langton Crescent
PARKES ACT 2600

Via email: paymentslicensingconsultation@treasury.gov.au

Dear Director of the Payments Licensing Unit,

Visa submission to Treasury on the Payments System Modernisation (Licensing: Defining Payment Functions)

Visa welcomes the opportunity to share its perspectives on the Payments System Modernisation (Licensing: Defining Payment Functions) Consultation Paper (consultation paper) and supports Treasury's commitment to ensuring that Australia's regulatory framework is fit for purpose.[1]

In responding to the consultation paper, Visa's submission focuses on several topics, including our principles for creating an effective and efficient licensing framework that facilitates and encourages continued innovation and investment in the payments system. In addition, we provide our perspectives on a number of specific questions in the consultation paper, such as the definitions, risk characteristics, exemptions, and regulatory obligations for various payment functions.

Visa also supports payments functions that are fully or predominantly non-customer facing not being required to hold a payments licence.

Visa is available to provide further details on our submission if helpful.

Yours sincerely,

Julian Potter
Group Country Manager, Australia, New Zealand, and South Pacific

[1] Treasury (2023), Payments System Modernisation (Licensing: Defining Payment Functions) - Consultation paper (treasury.gov.au), p5.

Executive summary

The following key points are addressed in Visa's submission to Treasury regarding the consultation paper on "Payments System Modernisation (Licensing: Defining Payment Functions)":

- **Visa commends Treasury for its intention to adopt "graduated regulatory obligations** based on the different types of risks associated with performing each payment function"[2].

- **Visa supports payments functions that are fully or predominantly non-customer facing not being required to hold a payments licence**.

- **Given the consultation paper includes Treasury's risk and consistency objectives**, we share Visa's key principles for Treasury's consideration, including:
  - Licensing frameworks should consider **the risk posed by individual participants** in the ecosystem.
  - **A licensing framework should be tiered, clear, and adaptable** to the roles of participants in the payments ecosystem.
  - **Outcome-based and technology-neutral regulation** helps ensure that countries can keep pace with fast-evolving market developments. It also fosters an environment that supports innovation.

- Although **the consultation paper helpfully describes some stablecoin types that are not included in the definition of a 'payment stablecoin'** – namely, stablecoins collateralised by other crypto assets and stabilised by algorithmically-driven processes, and those redeemable for commodities, such as gold – **more guidance is needed on the stablecoin types included in this category.**

- Although it may be reasonable to assume that a 'payment stablecoin' is one that is used primarily as a means of payment, **as currently defined in the payments industry there is little distinction between a 'payment stablecoin' and other commonly used terms for stablecoins**, such as 'fiat-backed stablecoin'.

- The **removal of unlicensed product issuers that use licensed intermediaries could impact fintech platforms** who embed financial products through the use of an enabler or BIN sponsor under the enabler's licence.

- In addition to the inclusion of the three broad risk categories (financial, operational and misconduct risks) in the consultation paper, Visa suggests **including data protection, cybersecurity and fraud risks as additional categories**.

[2] Ibid., p8.

- **Visa supports a risk-based approach as a preferable alternative to fixed thresholds**, while ensuring that licensed participants implement sufficient measures and risk controls to mitigate associated risks and meet high standards for data protection and cybersecurity.

- **We welcome the consultation paper's reference to payment system operators not being obligated to grant access to licensees that simply meet the common access requirements**, as they may have additional system-specific requirements.

Overview

Visa's core mission is to connect the world through the most reliable, secure and innovative payments network. In Australia, the ongoing development of a secure, efficient, competitive and innovative electronic payments system is essential to the growth, stability and resilience of the national economy.

As Treasury considers the introduction of a licensing framework, the payments ecosystem's success depends (among other things) on how straightforward it is for financial institutions, fintechs, payment facilitators and new entrants to be able to recognise obligations and be able to perform their activities accordingly. Furthermore, licensing frameworks should ensure a level playing field - if participants perform the same functions and bring the same level of risk to the ecosystem, they should be treated in the same manner.

Visa commends Treasury for its intention (as outlined in the consultation paper) to adopt "graduated regulatory obligations based on the different types of risks associated with performing each payment function"[3]. This is in line with our principles-based approach that includes the importance of licensing frameworks being proportional to the risk posed by individual participants in the ecosystem.

Risk management is a core aspect of Visa's business, from product and service design to security and operations. Our risk framework combines preventive, detective, and corrective controls, to ensure risks are properly managed. For further details on the robust mechanisms Visa has in place to manage and mitigate the risks Treasury outlines[4], see Attachment A.

Visa welcomes Treasury's acknowledgement that it is anticipated that its proposed reforms will mean "certain existing requirements in the corporations legislation, such as licensing, disclosure requirements, the design and distribution obligations, and the hawking prohibition, could extend to entities who may currently not be subject to these requirements". We strongly support Treasury's assessment that "it is unlikely to be appropriate for many of these requirements to apply to payment functions that are not consumer facing (such as payments clearing and settlement)"[5].

Visa provides transaction processing services (primarily authorisation, clearing and settlement)[6] to regulated financial institutions and our other clients through VisaNet, our global processing platform. We note that, through our core processing services, we enable the authorisation of transactions by providing the technology to relay authorisation messages, set standards for

[3] Ibid., p8.

[4] Treasury outlines three broad categories of risks (financial, operational and misconduct risks) to be addressed by the new licensing framework.

[5] Treasury (2023), Licensing of payment service providers – payment functions | Treasury.gov.au, p11.

such messaging and, if instructed by issuers, generate authorisation decisions for certain transactions on an issuer's behalf based on the parameters established by the issuer.

Visa is a payments processing technology company – not a financial institution - and it is our financial institution clients and partners that manage consumer, customer and merchant relationships. In addition, we do not issue cards, extend credit or set rates and fees for consumers.

As Treasury is aware, in Australia, the Visa debit and credit card system is currently designated as a critical payment system under the Security of Critical Infrastructure Act, and the Visa debit, credit and prepaid payment systems are designated by the Reserve Bank of Australia (RBA), which sets regulations and standards for the Australian payments industry. In addition, in February 2023, the RBA Payments System Board (PSB) agreed to extend its supervision to include payment systems where an outage could cause significant economic disruption and damage confidence in the financial system, including Visa.[7] Furthermore, Visa is a payment technology services provider to highly regulated Australian financial institutions, which are supervised by the Australian Prudential Regulation Authority.

Below, we explore some of the consultation questions in more detail.

[7] Reserve Bank of Australia (2023), Payments System Board Update: February 2023 Meeting | Media Releases | RBA

Response to Consultation Questions

List of payment functions

Principles underlying the list of payment functions

Consultation Question

1) Are there any other principles that should be considered in developing the list of payment functions?

Visa Response

As a global payments technology company, Visa supports strong and stable payment systems around the world, and the strength of our partnership with governments and regulators worldwide rests on the following principles, in line with Treasury's approach:

- Regulatory frameworks should encourage **continued investment in the payments system, thereby supporting an appropriate balance between improving security, efficiency, resilience and innovation**.
- Policy settings should be designed to take account of the **economic incentives necessary for key ecosystem participants** (issuers and acquirers, for example) to deliver new products and solutions, mitigate risk/fraud, and **not disproportionately benefit one party over another or impose unnecessary costs upon ecosystem participants**.
- Licensing frameworks should be **proportional to the risk posed by individual participants** in the ecosystem.
- **In line with this perspective, licensing requirements should be tiered, clear, and adaptable** to the roles of participants in the payments ecosystem. The ecosystem's success depends on how straightforward it is for financial institutions, fintechs, payment facilitators and new entrants to be able to recognise their duties and obligations and be able to perform their activities accordingly.
- **Duplicative and possibly conflicting regulation** should be avoided regarding other legal regimes in Australia, so that participants who are already subject to robust risk management compliance obligations under other existing laws in Australia are not subject to duplicative or burdensome regulatory requirements in new regulatory frameworks. This is because **overlapping regulatory frameworks cause confusion, diminish efficiencies, and can have the unintended effect of unlevelling the playing field** for entities that need to comply with multiple requirements.
- Placing **additional requirements may have a negative and disproportionate impact** on the ability of participants to continue investing in infrastructure and technology to safeguard security, data and privacy in the digital world.

- **Outcome-based and technology-neutral regulation** helps ensure that countries can keep pace with fast-evolving market developments and fosters an environment that supports innovation.
- **Licensing frameworks based on established international standards** form the backbone of the digital payments industry, ensuring ubiquity by maximising global interoperability and adoption in digital systems. Such standards also incentivise the creation of new and innovative products and services and, therefore, promote a vibrant payments ecosystem.
- Licensing frameworks should ensure a **level playing field, fair competition and avoid economic distortions**. If participants perform the same functions and bring the same level of risk to the ecosystem, they should be treated in the same manner. If participants benefit from other participants' infrastructure or investments via growth and economic benefit, these parties should be subject to requirements as appropriate.

<u>Consultation Question</u>

2) Is the list of payment functions comprehensive, or should other functions be included?

<u>Visa Response</u>

Visa does not have any recommendations on additional functions to be included. However, should Treasury decide to amend the proposed list of payments, we suggest Treasury consider the principles outlined in Visa's response to Question 1 above and continue to consult with industry participants to ensure consistency.

<u>Consultation Question</u>

3) Should all payment functions be treated as financial products under the corporations legislation or should some be treated as a financial service?

<u>Visa Response</u>

Currently, 'financial products' have their own regulatory regimes for the distributors of those products (for example, 'debit' can only be provided by authorised deposit-taking institutions (ADIs) and 'credit' by credit licensees). Applying this logic, it follows that all other payment functions should be default financial services unless they are, by definition, a payment service combined with a payment product. For example, a three-party model might fit this description, where it not only provides the payment process and settlement but also the issuance.

Description of each payment function

<u>Stored-value facilities (SVFs)</u>

Consultation Question

4) Does the term 'payment stablecoins' accurately describe the types of stablecoins this paper seeks to capture for regulation or are there other terms that may be more appropriate?

Visa Response

Although the consultation paper helpfully describes some stablecoin types that are not included in the definition of a 'payment stablecoin' – namely, stablecoins collateralised by other crypto assets and stabilised by algorithmically-driven processes and those redeemable for commodities, such as gold – more guidance is needed on the stablecoin types included in this category. As noted in response to Question 5 below, further clarity on how 'payment stablecoins' are clearly defined and distinguishable from other common terms defining stablecoins, like 'fiat-backed stablecoins' or 'trading stablecoins', would be beneficial. Furthermore, guidance on the potential role that blockchain or distributed ledger technology plays in reference to payment stablecoins could prove useful in differentiating these assets from other stored-value facilities.

Additionally, given the global nature of stablecoins, a more detailed description of what is meant by 'payment stablecoins' in the Australian context would help provide a basis of comparison for similar assets in other jurisdictions – including 'payment stablecoins' (in the United States), 'asset-referenced tokens' (in Europe) and 'digital payment tokens' (in Singapore).

Consultation Question

5) Does the proposed definition of 'payment stablecoins' adequately distinguish itself from other stablecoin arrangements?

Visa Response

Although it may be reasonable to assume that a 'payment stablecoin' is one that is used primarily as a means of payment, as currently defined in the payments industry there is little distinction between a 'payment stablecoin' and other commonly used terms for stablecoins, such as 'fiat-backed stablecoin'. Both could be viewed as "a digital representation of monetary value intended or purported to maintain a stable value relative to a fiat currency"[8] as well as being able to be redeemed for Australian dollars or another fiat currency actively marketed or sold in Australia.

Additionally, both payment and fiat-backed stablecoins are likely to be issued by entities that control the total supply, are responsible for the stability mechanism, and usually act as the counterparty for contractual arrangements. As such, it would be helpful if there was more detail in the consultation paper on how a 'payment stablecoin' is distinguished from a 'fiat-backed

[8] Treasury (2023), Payments System Modernisation (Licensing: Defining Payment Functions) – Consultation paper (treasury.gov.au), p13.

stablecoin' as well as other known terms for defining stablecoins, like 'trading stablecoin'. It would also be beneficial to understand if there are any restrictions planned on a 'payment stablecoin' where it concerns trading activities.

Furthermore, additional details on payment stablecoin issuers would be beneficial, including whether an issuer needs to be an insured depository institution (or subsidiary thereof) or if non-bank institutions are also eligible for approval as qualified issuers.

Consultation Question

9) Should any other payment functions be included?

Visa Response

Visa does not have any recommendations on additional functions to be included. However, should Treasury decide to amend the proposed list of payments, we suggest Treasury consider the principles outlined in Visa's response to Question 1 above and continue to consult with industry participants to ensure consistency.

Excluded and exempted activities

Consultation Question

10) Would the removal of the identified exclusions create unintended consequences?

Visa Response

Visa believes that the removal of unlicensed product issuers that use licensed intermediaries could impact fintech platforms who embed financial products through the use of an enabler or BIN sponsor under the enabler's licence. In this case, the unintended consequences may include the restriction of competition and reduction of innovation.

Consultation Question

11) Which existing exclusions and exemptions applicable to non-cash payment facilities should be amended or removed to support regulation of the proposed payment functions? Do any existing exclusions or exemptions require updating, such as the relief for low-value facilities?

Visa Response

Visa is not aware of any challenges arising from the existing exclusions and exemptions that would require updating.

Consultation Question

14) Should the exclusion for low value facilities apply to any PFS, such as money transfer services? If so, what thresholds should be considered a low value PFS?

Visa Response

Visa would be interested in exploring any exclusions based upon value thresholds or scale that Treasury may consider incorporating.

Characterising the risk of each payment function

Stakeholders impacted by risks

Consultation Question

16) Are there any other risk characteristics of a payment function that should be considered?

Visa Response

In addition to the three broad risk categories (financial, operational and misconduct risks) in the consultation paper, Visa suggests adding data protection, cybersecurity and fraud as further categories of risk that should be managed and mitigated to ensure licensed participants meet high standards regarding the safety and integrity of the payments ecosystem.

Consultation Question

17) What are the types of payment risks posed by the performance of each of the proposed payment functions?

Visa Response

See Visa's response to Question 16.

Consultation Question

18) While having regard to the obligations proposed to be imposed on the payment functions (outlined in Section 7), are the risks posed by the performance of each payment function appropriately mitigated by the payments licensing regime? Or are they more appropriately addressed by a framework outside of the payments licensing regime such as the PSRA or AML/CTF Act?

Visa Response

Payments licensing regimes typically cover a broader scope of topics and reflect the status of an entity at one point in time (e.g., financial standing of an entity at the point of licensing). The risks posed by each payment function would, therefore, be more appropriately addressed by frameworks outside of the payments licensing regime, such as the Payment Systems (Regulation) Act or AML/CTF Act, which are designed to address risks on an ongoing basis.

Overview of possible regulatory obligations

Consultation Question

19) Is the proposed risk-based approach to applying regulatory obligations appropriate?

Visa Response

Visa supports regulatory frameworks that ensure financial stability and risk management and encourage competition and innovation in the payments sector. These frameworks should align with the risks presented by individual organisations. A risk-based approach considers the varied risk profiles of different payment system participants to properly address risk attributes.

The drawbacks of non-risk-based approaches include potential limitations on the ecosystem's capacity to adapt to emerging global digital technologies and meet the changing consumer demand for versatile payment solutions due to fixed thresholds. A uniform set of thresholds for all participants imposes the same requirements intended for high-risk entities to those posing a minimal threat to the financial system. Complex licensing requirements for newcomers may also inadvertently restrict competition, stifle innovation and serve as a market entry barrier. Therefore, Visa supports a risk-based approach as a preferable alternative to fixed thresholds, while ensuring that licensed participants implement sufficient measures and risk controls to mitigate associated risks and meet high standards for data protection and cybersecurity.

Consultation Question

20) Should payment functions that are not customer facing be required to hold a payments licence? Should providers of these non-customer facing payment functions have different regulatory obligations, such as only having to comply with relevant industry standards?

Visa Response

Visa supports payments functions that are fully or predominantly non-customer facing not being required to hold a payments licence and, as a result, that they comply with requirements that are proportional to the risk that they present.

In this regard (and as outlined in Visa's Overview above), we provide transaction processing services (primarily authorisation, clearing and settlement) to highly regulated financial institutions and our other clients through VisaNet, our global processing platform. Visa is a payments processing technology company – not a financial institution - and it is our financial institution clients and partners that manage consumer, customer and merchant relationships. In addition, we do not issue cards, extend credit or set rates and fees for consumers.

We note that the consultation paper states that: "It is anticipated that the proposed reforms will mean certain existing requirements in the corporations legislation, such as licensing, disclosure requirements, the design and distribution obligations, and the hawking prohibition, could extend to entities who may currently not be subject to these requirements. … it is unlikely to be appropriate for many of these requirements to apply to payment functions that are not consumer facing (such as payments clearing and settlement)."[9] Visa agrees that it would not be appropriate for these requirements to apply to payments functions that are non-consumer facing, including payments clearing and settlement.[10]

Consultation Question

21) Should the common access requirements and industry standards be linked to the payments licence? For example, would it be appropriate for some entities to only be required to comply with mandatory industry standards but not be required to hold an AFSL or comply with the ePayments code?

Visa Response

In general, Visa supports the common access requirements and established international standards being linked to the payments licence, subject to Visa's response to Question 20 and the Overview we have provided.

We welcome the consultation paper's reference to payment system operators not being obligated to grant access to licensees that simply meet the common access requirements, as they may have additional system-specific requirements (for example, related to technical connectivity) and are best placed to manage the risks of accessing their system.[11]

Visa considers that it would be appropriate for some entities to comply with established international standards but not be required to hold an Australian Financial Services Licence or comply with the ePayments Code, which is the status quo for Visa at the current time. Among other things, this is because Visa is not customer facing and does not hold funds.

[9] Ibid., p11.
[10] Ibid., p28.
[11] Ibid., p31.

About Visa

Visa is one of the world's leaders in digital payments. Our mission is to connect the world through the most secure, reliable and innovative payment network – enabling individuals, businesses and economies to thrive. We facilitate global commerce and money movement across more than 200 countries and territories and among consumers, financial institutions, businesses, strategic partners and government entities through innovative technologies.

In Australia, Visa has offices in Sydney and Melbourne. Together with our Australian financial institutions, fintech and business clients and our technology partners, we are committed to building a future of commerce that fosters Australian economic growth, security and innovation. Since 2020, Visa has worked with Global Sisters to provide business mentoring and coaching to aspiring businesswomen who recently graduated from Global Sisters' small business education program. In the same year, we launched #WhereYouShopMatters, an initiative focused on supporting Australian small businesses through education and promotion. Prior to this, Visa partnered with Quest Payment Systems and The Big Issue, the independent magazine sold by homeless, marginalised and disadvantaged people, to enable Big Issue vendors to accept digital payments.

Visa continues to enable new payment flows and expand acceptance across the payments ecosystem, ensuring that every Australian can both pay and be paid in a secure and convenient way. We are realising this through Visa Fintech Partner Connect and the Visa Accelerator Program. The program provides Australian fintechs with access to Visa's technologies, networks and solutions, enabling businesses to scale for the benefit of consumers, businesses and the economy. Regarding security, over a five-year period, Visa invested nearly AU$14.5 billion in systems resilience, fraud management and cybersecurity, including tokenisation, Artificial Intelligence (AI) and blockchain-based solutions, to bring even more security to every transaction.[12] In 2021, Visa's AI-driven security helped financial institutions prevent more than AU$354 million in fraud from impacting Australian businesses.[13] As commerce moves rapidly online, the threat landscape is also changing and, in response, Visa released its updated Australian Security Roadmap 2021-23, given the increasing risk of cybercrime and scams facing Australian businesses and consumers. The roadmap highlights the steps that Visa is taking, together with industry, to continue securing digital payments in Australia.

---

[12] Visa data on global technology and operations investments, FY15-FY19. For further detail, see https://usa.visa.com/visa-everywhere/blog/bdp/2019/12/24/investing-in-the-1577207091483.html
[13] Visa (2021), "Visa's AI prevents more than $350 million in fraud from disrupting Australian businesses", https://www.visa.com.au/about-visa/newsroom/press-releases/visas-ai-prevents-more-than-350-million-in-fraud-from-disrupting-australian-businesses.html

Attachment A

Below are examples of how Visa manages the risks identified by Treasury in the consultation paper and other risks, such as cybersecurity and fraud:

- **Financial Risks:** Visa has a long track record of financial resilience with stable revenue and earnings growth. We have established an auditable control framework which consists of systems, policies, processes and procedures that comply with the applicable accounting and audit standards. Some of the tools that Visa employs to manage financial risk include our credit settlement risk policy (which incorporates liquidity guidelines set by the Bank for International Settlements for payment systems) and a collateral management program (designed to limit Visa's exposure to non-settlement in the event of a client's failure by requiring certain clients to post collateral).

- **Operational Risks:** An important component of Visa's operational risk management program is Visa's global business continuity policy. Across all areas of the business, Visa conducts analyses aimed at reducing the impact of potential key operational setbacks, while supporting the continuation and timely recovery of critical assets, systems, services and business functions. In addition, Visa's operational resilience program follows an established cycle of assessment, planning, exercising, and training that is defined in Visa's corporate policy, a multi-year strategy and execution plan, and procedural documents. Visa's business continuity plans are reviewed, updated, approved and exercised (where appropriate) at least once a year. Finally, our operational risk management program is supported by our corporate governance framework, which is guided by a fully independent board of directors, as well as fully independent board committees, including our Audit & Risk Committee.

- **Cyber Security Risks:** In Australia and globally, Visa takes seriously its shared responsibility to help secure the payments ecosystem against cyber threats. To manage the constantly changing threat environment and growing demands on our infrastructure, we devote significant resources to our talent and technology. Visa invested AU$14.5 billion in technology over the past five years, including to reduce fraud and improve security[14]. This extends to the implementation of zero trust architecture, adoption of a defence-in-depth approach, world-class technologies, best-in-class cyber security protocols and employment of over 1,000 world-class cyber security professionals.

- **Fraud Risks:** Visa uses Artificial Intelligence (AI) and machine learning to analyse approximately 500 unique risk attributes of any transaction, including critical information about the device, account holder spending profiles and global fraud trends. This fraud prevention system helps financial institutions identify and respond to emerging fraud

[14] Visa data on global technology and operations investments, FY15-FY19. For further detail, see https://usa.visa.com/visa-everywhere/blog/bdp/2019/12/24/investing-in-the-1577207091483.html

patterns and trends globally in real-time, making the global payment ecosystem safer for consumers and merchants. Visa relies on layers upon layers of security technologies to protect the valuable data flowing through our system. This multi-layered security approach has kept fraud rates low, despite significant growth in transaction volumes. We conduct regular exercises to ensure that in the event of an incident, we are fully prepared to respond effectively and expeditiously.