ABN 14 087 822 491
Level 3, 151 Castlereagh Street
Sydney NSW 2000
email: tgunthorpe@asl.com.au
Mobile: +61 407 605 708

Friday, 21 July 2023

Director
Payments Licensing Unit
Financial System Division
The Treasury
Langton Crescent
PARKES ACT 2600

Email: paymentslicensingconsultation@treasury.gov.au

Dear Director,

Payments System Modernisation (Licensing: Defining Payment Functions) (June 2023)

We welcome the opportunity to respond to Treasury's consultation on the Payment System Modernisation (Licensing: defining payment functions). The Australian payment ecosystem is at an important period of evolution to match the growing needs of its participants and end-users.

In response to the specific questions raised in the issues paper, please find our responses below:

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

Other principles to be considered are:

- The increasing compliment of digital and data with payments, especially with Open Data and Consumer Data Right (CDR) initiatives underway. It would be important to emphasize data privacy and security as paramount to protect consumers while fostering innovation.
- AI in payments - addressing AI's role will ensure responsible and fair practices, building trust in AI-driven payment solutions.

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

Yes , it is comprehensive, however, in the interest of fostering innovation and maintaining a competitive environment, the inclusion of emerging payment functions, such as decentralized finance (DeFi) solutions or tokenized payment services, should be considered.

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

We recommend adopting a nuanced approach:

- Payment functions that involve the issuance of payment accounts or facilities, such as stored-value facilities (SVFs), including traditional SVFs and payment stablecoin SVFs, should be considered as financial products. These functions directly offer customers a product (e.g., an account) that holds value and can be used for making payments. Treating these functions as financial products aligns with the traditional approach to regulation and provides clarity for entities offering such services.
- On the other hand, certain payment functions, like payment facilitation, authentication, authorization, and processing services, may not necessarily involve the direct issuance of payment accounts or facilities to end customers. These functions primarily facilitate the payment process or provide verification and authorization services. Considering them as financial services, rather than products, may be more appropriate. This approach

acknowledges the role of these services in supporting the overall payment ecosystem without subjecting them to the same level of regulatory requirements as financial products.

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?

Yes, it does, using the term "payment stablecoins" distinguishes these stablecoins from other types of stablecoins that may not be fully backed by cash or cash-equivalent reserves or are linked to distinct types of assets, such as other cryptocurrencies or commodities like gold. It also highlights the primary use case of these stablecoins, which is as a means of payment or a store of value.

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

Yes, it does, the proposed definition of payment stablecoins emphasizes the following distinguishing factors:

- Digital representation of monetary value
- Intended or purported stable value relative to a fiat currency.
- Issued by payment stablecoin issuers.
- Capable of being redeemed for fiat currency.

Question 6. Is regulation as an SVF an appropriate framework for the regulation of payment stablecoin issuers? If not, why? What would be an appropriate alternative?

Yes, it is, considering the shared characteristics and functions between payment stablecoins and traditional SVFs. The proposed regulation as an SVF recognizes the fundamental purpose of payment stablecoins, which is to serve as a means of payment and store of value, like traditional SVFs.

The key factors supporting the appropriateness of SVF regulation for payment stablecoin issuers are as follows:

- Functional Similarity: Payment stablecoins and traditional SVFs both involve the transfer of funds in return for stored value that can be used to settle transactions or transferred to others.
- Regulatory Consistency: Regulating payment stablecoin issuers as SVFs allows for a consistent regulatory approach with other similar payment functions.
- Two-Tier Regulatory Approach: The proposed two-tier approach for regulating SVFs, with standard SVFs overseen by ASIC and major SVFs regulated by both ASIC and APRA, ensures that the regulatory obligations align with the scale and risks associated with payment stablecoin issuers.

Question 7. Does the list of proposed payment functions adequately capture the range of payment services offered in Australia currently and into the future that should be regulated under a payments licensing regime?

Yes, it does, and the inclusion of payment initiation services reflects an awareness of emerging trends, such as Open Banking and the Consumer Data Right, and the potential for third-party payment initiation services.

Question 8. Does the list need to be broken down in more detail, for example, should facilitation, authentication, authorisation, and processing be separate functions?

While further breakdown of the list into more specific functions could offer a more granular approach, it may also introduce complexity and potential overlaps between the functions.

Currently, the proposed list of payment functions already encompasses various aspects of payment facilitation, authentication, authorization, and processing services. These services are interconnected and often provided by the same entities or as part of an integrated payment solution. Separating

them into distinct functions might result in regulatory redundancies, administrative burden, and challenges in defining clear boundaries for each function.

Question 9. Should any other payment functions be included?

Not currently.

Question 10. Would the removal of the identified exclusions create unintended consequences?

Potential unintended consequences may include:

- Regulatory Burden: Removing certain exclusions might subject previously exempt payment services to unnecessary or disproportionate regulatory burdens.
- Impact on Financial Inclusion: Excluding certain payment services from regulatory oversight might impact financial inclusion efforts, especially for low-value or limited-purpose facilities.
- Risk Misalignment: If exclusions are removed without considering the risks posed by the specific payment services, the regulatory framework might not adequately address the unique risks associated with those services.
- Inconsistency and Complexity: The removal of exclusions might introduce inconsistencies in the regulatory landscape and create complex compliance requirements for payment service providers.
- Competitiveness: If certain payment services are exempted or excluded from the regulatory framework while others are not, it may create an uneven playing field and impact the competitiveness of different market participants.

More specifically, are there implications regarding cheques that will not be out of the system?

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?

None at this time, however, existing relief for low-value facilities, such as the conditional relief for low-value non-cash payment facilities granted by ASIC should be moved into primary legislation or regulations to provide greater certainty to the industry. The terms of this relief, including monetary thresholds, may need to be reviewed and updated to ensure they remain appropriate given the evolving landscape of payment services.

Question 12. Should the incidental product exclusion apply to the proposed list of payment functions?

We believe this should be carefully considered. The inclusion of the incidental product exclusion can provide clarity and flexibility in certain circumstances, but it is essential to define its scope appropriately to avoid potential misuse or abuse. The incidental product exclusion typically allows for specific financial products or services that are ancillary to the main product or service to be exempt from certain regulatory requirements. It aims to prevent unnecessary regulatory burden on products or services that play a minor or secondary role in the overall offering. In the context of the proposed payment functions, applying the incidental product exclusion could be beneficial for payment services that are inherently supportive or complementary to the primary offering. For example, if a payment function is incidental to the core service provided by a regulated entity, it may not require separate licensing or extensive regulatory oversight. It is crucial to ensure that the exclusion is appropriately defined and does not create loopholes for entities to circumvent regulatory requirements.

Question 13. Should any exclusions or exemptions be revised to be more consistent with comparable jurisdictions? For example, should the 'single payee' exclusions and relief for loyalty schemes, electronic road toll devices, prepaid mobile phone account and gift cards be replaced by a general exclusion for payment instruments that can be used only in a limited way?

We believe that revising exclusions or exemptions to align with comparable jurisdictions can enhance consistency and regulatory harmonization. While considering revisions, it is essential to strike a balance between regulatory efficiency and consumer protection.

The 'single payee' exclusions and relief for loyalty schemes, electronic road toll devices, prepaid mobile phone accounts, and gift cards could be reviewed to determine whether a more generalized exclusion for payment instruments with limited functionality is more appropriate. Such an approach could streamline the regulatory framework and provide greater clarity for both industry participants and consumers. By introducing a general exclusion for payment instruments that can be used only in a limited way, the regulatory burden on specific payment services may be reduced, while still ensuring that adequate consumer protection measures are in place for services that may pose higher risks. This could be achieved by defining clear criteria for what constitutes 'limited use' and ensuring that the exclusion does not inadvertently exempt high-risk services from regulatory oversight.

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?

We believe that the exclusion for low-value facilities could be considered for certain payment facilitation services (PFS), such as money transfer services. However, the thresholds for what constitutes a low-value PFS should be carefully determined to strike the right balance between regulatory efficiency and consumer protection.

We do not propose an amount at this this time.

For money transfer services, considering an exclusion for low-value PFS may be appropriate for transactions that fall below a specific threshold. The thresholds could be based on factors such as the average transaction value, cumulative transaction volume within a defined period, or a combination of both.

Question 15. Should any other exclusions or exemptions be provided?

Potential areas where additional exclusions or exemptions could be considered include:

- Microtransactions: These transactions typically involve lesser amounts and are often used for digital content purchases, online gaming, or micropayments for digital services.
- Limited-use payment instruments: Exempting payment instruments that can only be used for specific purposes or within a closed-loop ecosystem, such as gift cards or loyalty program points, from certain regulatory obligations.
- Specific types of payment providers: Providing exemptions for certain types of payment providers that offer specialized or niche payment services with minimal risks to consumers. For example, certain community-based or non-profit payment providers that serve specific groups or local communities.
- Digital Wallets with Low Transaction Thresholds: Exempting digital wallets with low transaction thresholds from certain regulatory requirements, provided they meet specific criteria that demonstrate minimal risks to users and the financial system.
- Government-operated payment systems: Considering exemptions for payment services offered by government entities for specific purposes, such as government assistance programs or social benefits.

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

We would like to highlight the following risk characteristics of payment functions that should be considered:

- Interconnectivity: Payment functions that have extensive links to other financial institutions or systems may pose higher systemic risks in the event of operational or financial failures.
- Scalability: Payment functions that experience rapid growth without adequate risk management measures in place could lead to operational and liquidity challenges.

- Technology Dependency: Payment functions heavily reliant on technology may face increased operational risks related to cyber threats, system outages, and technological vulnerabilities.
- Innovation and Complexity: Understanding and managing these risks is essential to ensure consumer protection and financial stability.
- Cross-Border Transactions: Payment functions involving cross-border transactions may present additional risks due to regulatory variations, currency exchange rate fluctuations, and exposure to international compliance challenges.
- Consumer Trust: Any breach of trust or perceived lack of security could lead to reputational risks and reduced adoption by consumers.
- Operational Resilience: Assessing the resilience and contingency plans of payment functions can help mitigate risks.
- Fraud and Financial Crime: Ensuring adequate measures to detect and prevent such activities is essential.
- Market Concentration: Assessing the concentration of payment functions within the market can help identify potential risks related to monopolistic behaviour, market manipulation, and lack of competition.
- Regulatory Compliance: Non-compliance may lead to legal and regulatory risks, impacting both consumers and the financial system.
- Consumer Education and Awareness: Adequate disclosure and transparency in communication can help consumers make informed decisions.
- Cross-Platform Integration: Payment functions that integrate with other platforms or financial services should be evaluated for potential risks arising from data sharing, interoperability, and third-party dependencies.

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

Here are the types of payment risks associated with each function:

- Issuance of payment accounts, facilities, or instruments that allow value to be stored:
    - Financial Risk: The risk of insolvency or illiquidity of the PSP, leading to customers losing their stored funds or being unable to access their money when needed.
    - Operational Risk: Risks related to technical malfunctions, system outages, or errors that may result in customers' inability to access their accounts or complete transactions.
    - Misconduct Risk: The risk of mis-selling or misrepresentation of payment facilities, leading to customers being misled about the features or costs of the services.
- Issuance of payment instruments, payment initiation services, and money transfer services:
    - Operational Risk: The risk of technical failures, cyber-attacks, or system malfunctions that may lead to unauthorized transactions, payment delays, or data breaches.
    - Misconduct Risk: The risk of deceptive practices, such as misrepresenting costs or falsely presenting services, which can harm customers and their trust in the payment provider.
- Payment facilitation, authentication, authorization, and processing services:
    - Operational Risk: The risk of operational failures, technical glitches, or cyber incidents affecting the smooth processing and completion of payment transactions.
    - Systemic Risk: As these services facilitate a sizeable portion of payment transactions, operational failures may have ripple effects on other PSPs and the broader financial system.
- Payments clearing and settlement:
    - Financial Risk: The risk of participants in the payment system failing to settle their financial obligations, leading to liquidity problems and potential losses for other participants.
    - Operational Risk: The risk of operational disruptions in the clearing and settlement process, causing delays or failures in transaction processing.
    - Systemic Risk: A significant disruption or failure in the clearing and settlement process could have systemic implications, affecting the overall stability of the financial system.

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?

Yes, they do, however, it is essential to ensure that there is no unnecessary duplication of regulatory requirements, and that the most effective framework addresses the specific risks associated with each payment function.

The payments licensing regime should focus on mitigating risks related to the provision of payment services, such as insolvency risk, operational risk, and misconduct risk specific to the payment industry. It should set out clear and robust obligations that PSPs must adhere to, ensuring customer protection, security, and financial stability.

On the other hand, some risks may be more appropriately addressed by existing regulatory frameworks, such as the PSRA (Payment Systems Regulation Act) or the AML/CTF (Anti-Money Laundering and Counter-Terrorism Financing) Act. For instance:

- Systemic risks and stability of the payment system: System-wide risks and the stability of payment systems are best addressed under the PSRA. The PSRA focuses on the oversight and regulation of payment systems as a whole, ensuring their safety, efficiency, and reliability.
- Money laundering and terrorism financing risks: Risks related to money laundering and terrorism financing should be primarily addressed under the AML/CTF Act. This legislation is specifically designed to combat financial crime and enhance the detection and prevention of money laundering activities.
- Data security and privacy risks: Privacy laws and data security regulations are better suited to address risks associated with the protection of customer data and privacy.

The payments licensing regime should work in conjunction with these existing frameworks, ensuring proper coordination and cooperation among regulatory authorities to address various aspects of risk effectively.

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

Yes, it is appropriate and appears to consider the varying risks associated with different payment functions. However, it is essential to ensure that the regulatory obligations are proportionate, effective, and do not create unnecessary burdens for PSPs. The framework should strike a balance between consumer protection, financial stability, and fostering innovation in the payment industry.

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?

No, they should not. For non-customer facing payment functions that do not involve the storing of value or direct interactions with customers, such as certain payment facilitation, authentication, authorization, and processing services, a case could be made for different regulatory obligations. These functions primarily provide infrastructure and support services to facilitate payment transactions without directly impacting end customers. As a result, the risks they pose may be more related to operational aspects and cybersecurity rather than customer protection or financial stability. In such cases, considering compliance with relevant industry standards could be a reasonable approach, provided that these standards adequately address the specific risks associated with these payment functions.

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?

Linking the common access requirements and industry standards directly to the payments licence might not be the most appropriate approach in all cases. While it can simplify the regulatory process and provide a comprehensive framework, there are certain considerations that argue against such linkage.

- Firstly, different payment functions pose varying levels of risk to consumers and the financial system. Imposing common access requirements and industry standards uniformly on all payment service providers, irrespective of their functions and risk profiles, could lead to overregulation for some entities. For instance, non-customer facing payment functions, which may have minimal direct impact on end-users, might be subject to unnecessary compliance burdens if tied to the payments licence.
- Secondly, requiring all PSPs to obtain a payments licence, even if they do not interact with customers or store value, may create additional administrative hurdles and costs for these entities. It could discourage potential new entrants or innovative players in the payments industry who might not need direct access to payment systems and could operate efficiently under industry standards without obtaining a licence.
- Thirdly, the scope of common access requirements and industry standards should be carefully considered. If these requirements are designed primarily for PSPs seeking direct access to payment systems, then linking them to the payments licence might not align well with the broader regulatory objectives for non-customer facing functions.

Instead of making compliance with common access requirements and industry standards a mandatory part of the payments licence, a more flexible and risk-based approach could be adopted.

Question 22. What types of businesses should be subject to the common access requirements? There is limited information available on the number and size of non-bank PSPs interested in directly participating in Australian payment systems to clear and settle payments. If this is something that your business is interested in, please provide further information (including via a confidential submission).

Some types of businesses that could potentially be subject to the common access requirements include:

- Non-bank payment service providers (PSPs): Non-bank PSPs that offer payment initiation services, money transfer services, or other payment facilitation functions may seek direct access to payment systems to enhance efficiency and offer more seamless payment experiences for their customers.
- Payment processors and aggregators: Entities that act as intermediaries between merchants and payment networks may also be interested in obtaining direct access to payment systems to streamline payment processing and settlement for their clients.
- Fintech startups and innovative payment service providers: New and innovative players in the payments industry that aim to introduce novel payment solutions and technologies may find direct access to payment systems crucial for achieving their business objectives.
- Digital wallet providers: Providers of digital wallets or mobile payment applications may seek direct access to payment systems to facilitate fast and secure transactions for their users.
- Buy Now Pay Later (BNPL) providers: Companies offering BNPL services, which have gained popularity as an alternative payment method, may also have an interest in direct access to payment systems.
- Other emerging payment service providers: As the payments landscape evolves, new and specialized payment service providers may emerge, seeking direct access to payment systems for specific use cases or niche markets.

Question 23. Further information is sought to help identify the number and profile of participants that perform each payment function and therefore may potentially be affected by the new licensing framework.

Apologies, we were unclear on what the question being asking, or is it for additional information?

Question 24. How can the payments licensing processes across regulators be further streamlined?

Here are some strategies that can be considered to achieve this:

- Harmonization of Requirements: Collaborating among regulators to harmonize licensing requirements.
- Cross-Agency Coordination: Regular meetings and information sharing between regulators can lead to better understanding of each other's processes and requirements.
- Online Application Portal: Developing a user-friendly online application portal that can be accessed by PSPs.
- Pre-application Consultation: Offering pre-application consultation services to prospective PSPs can help them better understand the licensing requirements and tailor their applications accordingly.
- Regulatory Sandboxes: Implementing regulatory sandboxes or pilot programs can provide a controlled environment for PSPs to test innovative payment products or services without the burden of full compliance.
- Mutual Recognition: Exploring mutual recognition agreements with other jurisdictions can simplify the licensing process for PSPs with an existing license in one jurisdiction seeking authorization in another.
- Expedited Review Process: Introducing an expedited review process for certain categories of PSPs, such as startups or small businesses.
- Regulatory Guidance: Providing comprehensive and easily accessible guidance documents that outline the licensing requirements and procedures can help PSPs navigate the process more effectively.
- Regular Review and Improvement: Periodic reviews of the licensing process and feedback from PSPs can identify areas for improvement and lead to ongoing refinements to streamline the system.

Question 25. Is the proposal to provide central guidance and a website portal for PSP licensing processes a good alternative to the single point of contact proposal recommended by the Payments System Review?

Both approaches have their merits but would prefer central guidance and a website portal.

Pros	Cons
• Accessibility: A centralized website portal can provide easily accessible information to PSPs regarding licensing requirements, application procedures, and relevant regulatory guidance. This can help PSPs navigate the licensing process more efficiently and reduce confusion. • Transparency: Clear and comprehensive guidance available on the website can enhance transparency in the licensing process, allowing PSPs to understand the regulatory expectations and compliance standards. • Cost-Effective: Developing a website portal is likely to be a cost-effective option compared to establishing a dedicated single point of contact team, especially for smaller regulatory authorities with limited resources. • Scalability: A website portal can be scalable and accommodate many	• Limited Interaction: While a website portal can provide information, it may lack the personalized interaction and support that PSPs may need during the application process. • Coordination Challenges: Without a designated single point of contact, PSPs may need to interact with multiple regulators separately, which could lead to coordination challenges and potential delays. • Tailored Support: Some PSPs, particularly those with complex business models or novel products, may benefit from more tailored and hands-on support during the licensing process, which a website portal may not provide.

applicants simultaneously without significant operational constraints.	

We thank you for the opportunity to review and respond to the Payments System Modernisation (Licensing: Defining Payment Functions) Consultation Paper (June 2023) and are happy to provide further information as needed as Treasury develops policy on this important issue.

Yours sincerely,

Trent Gunthorpe
Chief Product Officer
Australian Settlements Limited