The Australian Debit Card Market: Default Settings and Tokenisation

Conclusions Paper

September 2023

Contents

1. Executive Summary

This paper sets out the conclusions of the Reserve Bank of Australia's recent public consultation on options for further enhancing the competitiveness, efficiency and safety of Australia's debit card market. In June 2023 the Bank published an [Issues Paper: 'The Australian Debit Card Market: Default Settings and Tokenisation'](#), which covered two sets of issues:

1. The practice of a default routing network being set for dual-network debit cards (DNDCs), particularly through 'priority' network settings on card chips.[1]

2. The tokenisation of debit cards for the purpose of conducting online transactions.

This paper provides a summary of the two issues, the options proposed by the Bank to address them, stakeholder feedback, and the Payments System Board's conclusions. The Board's key conclusions are outlined below.

Setting a default network on DNDCs

- **The Board decided that it will not continue to explore prohibiting the setting of a default routing network on DNDCs.** Stakeholders' feedback indicated that any benefits from such a prohibition would likely be outweighed by the costs and risks involved. Prohibiting the setting of a priority network would be costly as it would require all DNDCs to be reissued. There would also be the risk of failed transactions, particularly for overseas transactions and for certain types of transactions in Australia, including those made at legacy terminals.

- The Board, however, remains strongly supportive of merchants having the ability to choose their preferred debit card network through least-cost routing (LCR). The Board expects acquirers, payment facilitators, and gateways ('providers') to make faster progress on enabling LCR for merchants that could benefit from it. **If providers do not make substantial progress in enabling LCR for more merchants by June 2024, the Bank will explore imposing a formal regulatory requirement on providers to enable LCR for their merchants. Going forward, the Board also expects the industry to implement new form factors in a way that is compatible with LCR from the outset.**

Tokenisation of DNDCs and other cards

- There was broad support among stakeholders for the industry to explore introducing more standardisation for tokenisation. Accordingly, the Board decided that following further consultation with industry, the Bank will endeavour to publish high-level expectations on the tokenisation of payment cards by the end of 2023. The Bank has asked the Australian Payments Network (AusPayNet) to coordinate the industry's work to meet the Bank's expectations and to draft more specific tokenisation standards if required. The Bank will work with AusPayNet and

---

1   Default routing refers to the routing of a transaction to a particular network in the absence of a consumer or merchant choice of network. For card-present transactions, the default network is often determined by the 'priority' settings on the card chip set in line with EMVCo standards.

industry to put in place governance arrangements for this work so that all stakeholders' views are considered in formulating the industry response.

- **The Bank welcomes feedback on the draft expectations included in Appendix A**, and the extent to which prepaid and charge cards should be covered by the expectations.

2.   Setting a Default Network on Dual-network Debit Cards

2.1   Issues

The default routing of contactless DNDC transactions to the international debit networks, particularly due to 'first-priority' settings on card chips, has been of concern to the Bank for a number of years. Unless merchants can choose their preferred network for contactless transactions, this practice:

- can put upward pressure on merchants' debit card payment costs – for many merchants, payments via the international debit networks are significantly more expensive, on average, than payments via the eftpos network

- reduces competitive tension between the debit schemes, which reduces the incentive for the international schemes to lower their fees.[2]

The Bank has sought to address the competition and efficiency concerns relating to the default routing of debit transactions through its promotion of LCR. LCR functionality allows merchants (or their provider) to choose which debit network will process DNDC transactions, overriding any default setting. The Issues Paper noted that while LCR could be sufficient to address the Bank's concerns about default settings, it may not achieve the Bank's policy objectives in a timely manner due to delays in its implementation and barriers to merchant take-up. Data collected by the Bank show that since the Bank began advocating for LCR in 2017, LCR for in-person transactions has only been enabled for a little more than half of all merchants.

2.2   Policy options presented in the Issues Paper

The Issues Paper noted that while the Bank remains committed to the implementation of LCR, it had decided to explore additional regulatory options that could address the concerns raised by priority settings on DNDCs and improve competition and efficiency in the debit card market. The Bank noted that it was exploring the feasibility, and the associated costs and benefits, of preventing any one debit network from being given routing priority at issuance for domestic transactions. In effect, this would mandate that merchants be provided with at least a basic form of LCR, where the merchant chooses the routing network. In the Issues Paper the Bank sought feedback from stakeholders on whether there would be any technical or practical challenges to prohibiting the setting of a priority network, the benefits and costs of such a prohibition, and suggestions on alternative courses of action that could better address the Bank's concerns.

---

2   In this paper, 'scheme' refers to the entity operating the card system, whereas 'network' refers to the infrastructure of the scheme that allows for the processing of card payments.

2.3   Stakeholder views

Stakeholders provided consistent feedback that it was technically feasible to remove priority network settings on DNDCs. Some stakeholders agreed that removing priority settings would enhance competition and put downward pressure on merchant costs. However, most stakeholders believed that the policy would not provide any additional benefit beyond the current LCR initiatives and would add significant costs and risks to the payment system. A number of stakeholders highlighted the following:

- **The removal of priority settings *alone* would be practically ineffectual.** Under the EMVCo standards, if there was no priority network set at issuance, and merchant choice had not been programmed into the terminal, the transaction would be routed by default to the network whose application was listed first.[3] This would likely be the international network to ensure cards still work when used overseas. Accordingly, the status quo would likely be preserved.

    – In addition, stakeholders indicated that taking action to remove priority settings on the card chip would not affect the default settings for mobile wallet transactions, which account for a rapidly growing share of card payments. Consequently, any action to prohibit priority network settings for contactless (card-present) transactions is likely to have diminishing benefits over the next few years, and would not prevent the setting of a default network in new form factors.

- **Departing from global EMVCo standards would risk failed transactions and possibly unintended consequences.** The Bank could require a departure from EMVCo standards so that both networks on a DNDC truly had equal priority. However, feedback suggested that where merchant choice has not been programmed into the terminal – whether due to legacy terminals or other issues – the contactless transaction would fail or the cardholder would be required to enter their choice of network into the terminal, adding friction to the checkout process. The risk of failed transactions would be particularly high for overseas transactions. This would be disruptive for consumers, merchants and schemes. Some stakeholders also argued that deviating from EMVCo standards might result in other costly unintended consequences in the future, such as the delayed introduction of payments innovations into Australia.

- **Prohibiting a priority network would be costly** as it would require all DNDCs to be reissued with new EMV chips without a priority network selected. If the change were to be implemented as soon as possible, the cost to industry would be significant. Alternatively, if left to natural card reissuance cycles to reduce these costs, the implementation could take three years or more. On the acquiring side, stakeholders argued that it would require engagement with a large number of merchants to elicit and implement their routing choice potentially in a short period of time, which would involve significant effort. There would still be some residual risk of failed transactions for certain types of transactions and those made at legacy terminals.

- **Pursuing existing LCR initiatives was preferred to removing priority settings**. Taking into account the points above, the majority of stakeholders expressed a strong preference for the Bank to continue pursuing LCR initiatives to achieve its policy objectives rather than require the removal of priority settings.

---

3   EMVCo is a global technical body, owned by major international card schemes, which develops and manages technical standards, for example relating to contactless cards, aimed at providing globally interoperable and secure card payments.

2.4　The Board's assessment and conclusions

Stakeholder feedback indicated that prohibiting the setting of a default network on card chips would either be practically ineffectual or would risk failed transactions and additional frictions/poor customer experiences, and would either result in large costs for issuers or a lengthy implementation period. Further, such a prohibition would have diminishing benefits over the next few years given the rapid growth in mobile wallet transactions and would not prevent the setting of a default network in new form factors.[4] Accordingly, the Board judged that the benefits of such an action are unlikely to outweigh the costs and risks involved. The Board therefore **decided that it will not continue to explore prohibiting the setting of a default routing network on DNDCs.**

The Board, however, remains strongly supportive of merchants having the ability to choose their preferred debit card network through LCR. The majority of stakeholders supported the Bank continuing to pursue LCR initiatives to achieve its policy objectives. While LCR is now widely available to merchants for in-person transactions from a technical perspective, the functionality has only been enabled for 54 per cent of merchants as at the end of June 2023; this share has increased marginally over the past year. **The Board expects providers to make faster progress on enabling LCR for merchants that could benefit from it. Going forward, the Board also expects the industry to implement new form factors in a way that is compatible with LCR from the outset.**

Over coming months, the Bank will continue to actively engage with merchants' providers and gather more detailed information to understand providers' progress in enabling LCR. The focus of this effort will be to clarify the reasons why some merchants have not had LCR enabled and any barriers providers face in enabling LCR. **If providers do not make substantial progress in enabling LCR for merchants by June 2024, the Bank will explore imposing a formal regulatory requirement on providers to enable LCR for their merchants.**

4　Broader regulatory action could, in principle, target the setting of default networks for mobile wallet transactions and possibly future form factors. However, major mobile wallet providers plan to remove their default settings as part of facilitating LCR for mobile wallet transactions and there is currently some uncertainty about the extent to which the RBA's regulatory powers apply to new players in the payments system that may influence or control default settings for future form factors. The Bank is assisting the Australian Government with its plan to reform the regulatory architecture for payments, including modernising the *Payment Systems (Regulation) Act 1998* with updated definitions of a payment system and its participants.

3. Tokenisation of Card Payments

3.1 Issues

Tokenisation of card payments involves replacing sensitive information – the cardholder's primary account number (PAN) – with a unique token that contains less critical information than the PAN and can be restricted for use on a particular device and/or at a specific merchant. The Issues Paper noted that despite tokenisation becoming more widespread, many merchants and their providers continue to retain sensitive card details to facilitate repeated or recurring transactions, which undermines the security benefits of tokenisation. According to AusPayNet data, in 2022 fraudsters made more than $275 million in card-not-present transactions at Australian merchants using stolen Australian debit and credit card details. In addition to these losses (which are often borne by the merchant), cardholders, merchants and financial institutions incur significant costs investigating and resolving fraud cases.

The Issues Paper also noted that an AusPayNet working group had identified some areas where standardisation is necessary to ensure that the tokenisation of DNDCs for online transactions is implemented in a way that realises the benefits of tokenisation without undermining competition and efficiency. Some of the issues identified were also relevant to the tokenisation of payment cards more generally (not just DNDCs). The working group concluded that some standardisation would be required to enable:

1. *token portability* so that once customers' PANs have been tokenised and deleted, merchants will still be able to switch their provider while retaining their customers' current tokens. Without portability, if a merchant switched provider, they would need to ask their existing customer base to re-enter their debit or credit card details for future transactions. This would be highly unattractive to many merchants, as it would likely result in declined transactions and customer attrition, and could effectively lock affected merchants into staying with their current provider.

2. *token synchronisation* so that when issuers update details for a DNDC (such as a new expiry date), all network tokens are updated simultaneously to avoid the possibility that some online debit card transactions fail due to only one network token being updated.

3. *token visibility* so issuers can see which merchants have stored tokens for their debit and credit cards, and potentially provide their cardholders with value-added services to help them manage their recurring payments.

3.2 Policy options presented in the Issues Paper

The Issues Paper sought stakeholder views on expectations the Bank could set for the industry to address the issues identified by the AusPayNet working group, and to substantially reduce the amount of sensitive card details being held across the industry. In particular, views were sought on the relative importance of: addressing the token portability, token synchronisation and token visibility issues; potential solutions and their costs and benefits; and feasible implementation timelines. The paper also noted that the Bank had a strong desire to see a significant reduction in all types of card details being stored across the ecosystem (given the associated fraud risk) and sought views on the benefits and

costs of the Bank's expectations applying to all Australian-issued cards, including credit cards, single network debit cards and prepaid cards (as appropriate). The Issues Paper included an example of possible expectations the Bank could set.

3.3   Stakeholder views

Nearly all stakeholders expressed support for the Bank's consultation on tokenisation and agreed that it was a good time to consider whether some standardisation of tokenisation approaches was required. Most stakeholders considered token portability and synchronisation to be the most important issues to be addressed in a coordinated way. While a few stakeholders also considered token visibility to be important, others considered it to be less critical to address.

Many stakeholders noted that **token portability** was important because it will help to support competition between merchants' providers. Some stakeholders were of the view that significant investment in technical enhancements would be required to enable token portability. Most stakeholders were of the view that the card schemes were best placed to develop token portability solutions under an industry framework. Stakeholders suggested a few different models for how this could work including: (i) a network-agnostic token that is compatible across all networks; (ii) requiring schemes to offer token migration services (e.g. via an API); and/or (iii) requiring schemes to share data to support token migration.

Stakeholders noted that **token synchronisation** was important for the reliability of transactions and suggested that data sharing among payments system participants was needed. This would involve the development of real-time communication protocols between participants so that issuers and token-holding entities could notify other relevant parties of status changes related to a token.

Most stakeholders acknowledged the benefits of **token visibility** in providing greater transparency to issuers and cardholders, which could give customers greater control over their recurring card payments. However, token visibility was generally seen as functionality that was 'nice to have', and its absence did not have significant implications for security, competition or reliability. Further, some stakeholders raised concerns about token visibility; for example, these new services could, in principle, allow consumers to cancel a token at a merchant before providing the merchant with notice (despite notice being contractually required by some merchants).

Some stakeholders were not opposed to the industry continuing to shift towards network tokenisation – that is, tokenisation by the card scheme rather than a merchant or its provider. However, some stakeholders raised concerns about the impact on some providers and merchants should they no longer be able to store and use PANs, as well as possible adverse effects on competition and efficiency should the gatekeeper status of the card schemes be entrenched and enhanced.[5]

Most stakeholders were supportive of the Bank setting some high-level expectations for the industry, with AusPayNet playing a central role in coordinating the industry's work to meet the Bank's expectations. A few stakeholders saw less of a need for standardisation, and argued it was important that Australian practices continued to align closely to international standards. Stakeholder views were

---

5   *Network tokenisation* involves the card scheme tokenising the PAN and storing the PAN in a token vault. As such, both the merchant and the gateway do not store the PAN, instead using the token provided by the card scheme. In contrast, *merchant* (or *proprietary/gateway) tokenisation* is where a customer's PAN is typically tokenised by the merchant's payment gateway. When processing the tokenised payment, the merchant's gateway extracts the PAN from its own token vault before sending it to the card scheme. In some cases, tokenisation is performed by the (typically very large) merchant itself, rather than the gateway.

mixed around whether the end of 2024 was feasible for achieving token portability and making substantial progress in removing PANs. Some stakeholders were concerned about their systems' deep reliance on PANs and suggested that there could be a staged timeline for the reduction of PAN storage to provide a smooth transition towards full tokenisation. Considering these issues, some stakeholders viewed a mid-to-late 2025 timeline as more feasible.

3.4   The Board's assessment and conclusions

There was broad support among stakeholders for the industry to explore introducing more standardisation for tokenisation of DNDCs for online transactions. **Accordingly, the Board decided that following some further consultation, the Bank will endeavour to publish high-level expectations for the industry by the end of 2023. Given that some of the issues, particularly token portability, are relevant for payment cards more generally, the Bank's expectations should be met for debit and credit cards, as appropriate** (with the precise scope yet to be defined, as discussed below).

The Bank's draft expectations are set out in Appendix A. There are some key differences and additions to the example expectations published in the Issues Paper. In particular, the Bank is proposing that:

- the industry <u>not</u> be expected to move to network tokens

- merchants and their providers be allowed to retain PANs provided they meet minimum security standards, which may be more stringent than the Payment Card Industry Data Security Standard (PCI-DSS)[6]

- the card schemes build the necessary infrastructure to support network token portability, to the extent it doesn't already exist

- no expectations be set regarding token visibility

- the industry meet the expectations by mid-2025 (rather than the end of 2024).

The Bank has asked AusPayNet to coordinate the industry's work to meet the Bank's expectations and draft more specific tokenisation standards if required. The Bank will work with AusPayNet and industry to put in place governance arrangements for this work to ensure that all stakeholders' views are considered in formulating the industry response.

The Bank would welcome feedback on two matters:

1. **The draft expectations included in Appendix A.**

2. **The appropriate scope of cards to be covered by the expectations, particularly the extent to which they should apply to prepaid and charge cards.**

Stakeholders who wish to provide feedback should contact the Bank by email at pysubmissions@rba.gov.au by **13 October**. The Bank will then contact these stakeholders to discuss next steps.

---

6   The PCI-DSS is a set of minimum technical and operational requirements designed to protect cardholder data and is set by the PCI Security Standards Council. The PCI-DSS applies to all entities that store, process and/or transmit cardholder data, including issuers, merchants and merchants' providers.

Appendix A

Expectations for tokenisation of payment cards and storage of PANs

The Bank expects:

1. The rollout of the eftpos eCommerce tokenisation service to be completed by the end of March 2024. To facilitate planning, relevant industry participants should be provided with monthly updates on the service and its functionality ahead of the rollout.

2. When a DNDC is tokenised, tokens should be requested and stored for both the domestic and international networks, where supported by both networks.

3. Merchants and payment service providers that do not meet minimum security requirements – which should be at least compliance with PCI-DSS – must not store customers PANs after the end of June 2025.

Portability of debit and credit card tokens

4. All relevant industry participants – including schemes, gateways, and acquirers – should support portability for both scheme and proprietary tokens by the end of June 2025 to reduce the friction for merchants that wish to switch payment service providers.

   (i) The eftpos, Mastercard and Visa card schemes should each develop token migration services if a solution does not already exist, to enable portability for merchants from one gateway or payment service provider to another. These services should be standardised and aligned as much as possible across schemes to minimise the operational burden on gateways; the solutions should not require gateways to retain PANs.

   (ii) Gateways should ensure that their proprietary tokens do not impede merchants switching payment service providers.

   (iii) Token-holding entities should provide any reasonable data to any 'authorised' third-party required to support token migration, and token migration should be executed in a timely manner.

   (iv) Only the reasonable costs of processing a token migration should be passed on to merchants.

Synchronisation for DNDC tokens

5. Issuers and token-holding entities should ensure that any status change or life-cycle event related to one token is, where relevant, duplicated to all other relevant tokens in real time (or near real time), including notification to each relevant card scheme, to ensure that all such changes propagate through the full ecosystem. This applies regardless of where a status change or life-cycle event originates, be that merchant, scheme, issuer or cardholder.

6. To link multiple tokens and aid token synchronicity, a unique Payment Account Reference (PAR) for each account, or equivalent solution, should be widely shared and used throughout the Australian payments ecosystem.