The Australian Debit Card Market: Default Settings and Tokenisation

Issues Paper

June 2023

Contents

ISBN 978-0-6456221-1-9 (Online)

1. Introduction

This paper outlines some options for further enhancing the competitiveness, efficiency and safety of Australia's debit card market. The key issues are:

1. **The practice of a default routing network being set at issuance on dual-network debit cards**. This practice can reduce competition between card schemes and puts upward pressure on merchants' debit card payment costs, which in turn feeds through into higher prices for consumers. The Reserve Bank of Australia (the Bank) seeks stakeholder views on the benefits and costs of actions to prohibit this practice, with merchants instead choosing the routing network.
2. **The tokenisation of debit cards for the purpose of conducting online transactions**. Tokenisation of card details in the online environment plays an important role in improving security. However, merchants and payment service providers continue to retain sensitive card details, which undermines the security benefits of tokenisation. There are also some areas where standardisation may be necessary to ensure that the full benefits of tokenisation are realised without impeding competition. The Bank seeks stakeholder views on expectations the Bank could set for the industry to address tokenisation issues and to substantially reduce the amount of sensitive card details being held across the industry by the end of 2024.

Debit card transactions account for around half of all consumer payments. The share of in-person debit card transactions that are contactless has risen from around 20 per cent in 2013 to around 95 per cent in 2022, as consumers have embraced the convenience of this technology (including mobile wallets). Over the same period, online card payments have also increased from 5 per cent to 10 per cent of all consumer payments, reflecting the long-term rise in e-commerce.

Around 85 per cent of debit cards issued in Australia are dual-network debit cards (DNDCs), which allow domestic payments to be processed via either eftpos or one of the other debit networks (typically either Debit Mastercard or Visa Debit). DNDCs facilitate competition between debit networks by allowing the choice of routing network to be made at the point of sale. Given the prevalence of debit card transactions, the Bank considers it important that the debit card market be safe, efficient and competitive.

This paper summarises relevant developments since the Bank released the Conclusions Paper to the Review of Retail Payments Regulation in October 2021, outlines some competition, efficiency and safety concerns related to the issues listed above, and identifies some potential courses of action for consideration. Key questions for stakeholders are included in sections 2.2 and 3.2 and collated in Appendix A.

The Bank will review written submissions received and will endeavour to meet with some stakeholders to discuss their submissions in more detail. The feedback received will be reviewed by the Payments System Board at its next meeting in August. The Board will consider:

1. Whether a consultation on policy actions to address the concerns raised by default settings on DNDCs is in the public interest. If so, the Bank will release a follow-up paper with more detailed proposals.

2. What expectations to set for industry regarding the tokenisation of DNDCs, including the steps that need to be taken and the deadlines for their completion.

2. Setting a default network on dual-network debit cards

2.1 Background

2.1.1 Payment costs on debit card transactions vary across debit card networks

When a merchant (such as a shop or business) accepts payments from a customer via a debit card, the merchant is charged a fee by their bank or payments provider. While this fee is often not easily observable or appreciated by consumers, higher payment costs for merchants feed through into higher consumer prices for goods and services.

Most debit cards in Australia are issued as DNDCs with functionality that enables a payment to be processed via either eftpos (the domestic debit network) or one of the international debit networks. These cards have an international scheme logo (Mastercard or Visa) on the front of the card and the eftpos logo on the back. Having Mastercard or Visa as one of the networks on the DNDC provides the cardholder with international transaction functionality, which eftpos does not provide.

The cost the merchant faces from their bank or payments provider for accepting a debit card transaction can vary depending on which debit network processes the transaction. For many merchants, payments via the eftpos network can be significantly less expensive – by around 20 bps on average for in-person transactions – than payments via the international Debit Mastercard or Visa Debit networks.

2.1.2 Contactless payments technology resulted in transactions being automatically routed to the international debit networks

When DNDCs were first introduced in Australia, the predominant method used to authenticate these debit transactions was by using 'CHIP/PIN' technology (see Box A). DNDC cardholders entered the card in the terminal and chose which network processed these transactions by pressing either the 'CHQ'/'SAV' button (eftpos) or the 'CR' button (international debit networks). While the CHIP/PIN functionality is still available in most cases, over recent years in-person card transactions have shifted to being mostly contactless, where the card is tapped on the terminal. DNDC transactions made using contactless technology typically do not provide the cardholder with a choice of routing network, with transactions instead usually routed to the international debit networks by default (unless the merchant is using least-cost routing).[1]

[1] The default can be overridden by the cardholder when using certain mobile wallets.

Box A: Debit card transaction authentication methods

'CHIP/PIN' technology

The use of CHIP/PIN technology as a transaction authentication method on a DNDC involves the cardholder inserting a DNDC (equipped with a security chip) into the merchant terminal and then selecting a routing network by pressing the 'CHQ', 'SAV' or 'CR' button. If a cardholder (or merchant) presses the 'CHQ' or 'SAV' button, the transaction will be routed to the domestic eftpos network. If the cardholder (or merchant) presses the 'CR' button (or more recently the 'Visa Debit' or 'Debit Mastercard' button), the transaction will be routed to the international network. The cardholder will then be required to authenticate the transaction by entering a PIN code.

Contactless payments using near-field communication technology

The use of contactless technology as a transaction authentication method involves a card being 'tapped' by a cardholder at the merchant terminal that can read the chip in the DNDC via near-field communication (NFC). The card can either be a physical card or a credential loaded onto a mobile wallet on a mobile device that is equipped with the relevant NFC technology. Contactless transactions provide convenience and speed at the checkout by not requiring further action by the cardholder to authenticate the transaction (up to a certain pre-set transaction value in the case of physical cards – typically $100 or $200 – with transactions over the threshold requiring a PIN code).

Contactless DNDC transactions currently route to the international networks by default (in the absence of least-cost routing, discussed further below).

The practice in Australia to date has been for card issuers to issue DNDCs with Bank Identification Numbers (BINs) allocated to the international debit schemes (Box B); these schemes' branding is on the front of the card with eftpos' branding on the back. Issuers of these DNDCs set the international debit network as the 'first-priority' network for transaction routing purposes so that contactless transactions, including in-person mobile wallet transactions, are routed to these networks by default. Issuers in Australia are currently unable to issue DNDCs carrying a BIN allocated to the international schemes with the 'first-priority' network being set to the alternative network on the DNDC. This is the practical effect of the limitations in the international networks' scheme rules and policies regarding the use of cards bearing BINs allocated to that scheme. Further, deeds made by Visa and Mastercard in favour of the Bank in 2013 relating to DNDCs include a clause that effectively provides that nothing in the deeds prevents the relevant scheme from requiring that it be the first-priority network on a card carrying a BIN allocated to that scheme.

Box B: Bank Identification Numbers

Bank Identification Numbers (BINs), also known as Issuer Identification Numbers (IINs), are the first (six to eight) digits that appear on a payment card. They are used for identification purposes and are allocated to schemes and/or issuers by the ISO Registration Authority pursuant to the international standard ISO 7812. The first digit(s) of the BIN identifies the major industry to which the card belongs. For example, the first digits of '4' and '5' have been allocated to 'Banking and financial'. The remaining digits of the BIN identify the location and identity of the issuer and other characteristics such as card type. The ISO standard allows for card schemes to be allocated blocks of BINs to hold on behalf of their member issuers (Visa cards typically begin with '4' and Mastercard cards typically begin with '5'). Alternatively, issuers can issue cards after applying for and being allocated a single BIN for a particular card type.

2.2 Policy issues

The default routing of contactless DNDC transactions to the international debit networks, as a result of them being set as the 'first-priority' network, has raised concerns for the Bank for a number of years. In particular:

- this results in upward pressure on merchants' debit card payment costs; for many merchants, payments via the international debit networks can be significantly more expensive, on average, than payments via the eftpos network
- there is reduced competitive tension between the debit schemes, due to the general inability of consumers or merchants to choose their preferred network for contactless transactions, which reduces the incentive for the international schemes to lower their fees.

2.2.1 The slow implementation of least-cost routing

The Bank has sought to address these competition and efficiency concerns relating to the default routing of debit transactions through its promotion of least-cost routing (LCR). LCR, also known as Merchant Choice Routing (or MCR), is functionality offered by payment service providers that allows merchants (or their payment service provider) to choose which debit network will process payments made by consumers using DNDCs. Merchant choice of network using LCR functionality overrides the priority, or default, network setting on DNDCs.

While LCR could be sufficient to address the Bank's concerns, 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. The Bank began advocating for LCR in 2017, and in 2021 the Bank set an explicit expectation for acquirers and payment facilitators to both offer LCR functionality for device-present transactions and promote the functionality to their merchant customers. The Bank recently published data on the availability and take-up of LCR by merchants.[2] The results show that after five years, LCR was still not available to all merchants, and only half of merchants had taken it up. The Bank also set an expectation

[2] See Connolly E (2023), 'The Shift to Electronic Payments – Some Policy Issues', Speech at AFR Banking Summit, Sydney, 28 March. See also RBA (2023), 'Update on Availability and Enablement of Least-cost Routing for Merchants', March.

in 2021 for the industry to make LCR functionality available for online transactions by the end of 2022. However, only a handful of industry participants met this expectation, though significant progress is expected to be made this year.

The Bank went further in 2022 by setting an expectation that LCR should be made available for mobile wallet transactions by the end of 2024. This highlights the fact that as new form factors are developed and adopted by the industry, the Bank will have to continue setting new expectations regarding LCR to avoid merchant choice being eroded by default routing to the international debit networks.

2.2.2 Policy options

The Bank remains committed to the implementation of LCR, which continues to be supported by the Government as outlined in its Strategic Plan for Australia's Payment System.[3] However, the Bank has decided to explore additional regulatory options, should they be necessary, that could address the concerns raised by the default network setting on DNDCs and improve competition and efficiency in debit card payments.

In particular, the Bank is 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. Instead, the merchant would choose the routing network, with the merchant's payments service provider responsible for identifying and implementing the merchant's routing network preference. Importantly, this would provide for competitive neutrality between the networks on DNDCs. In effect, the Bank would be mandating that merchants are provided with at least a basic form of LCR, where the merchant nominates the routing network. Merchant payment facilities with more sophisticated forms of LCR would also meet this requirement.[4]

The Bank understands that regulatory intervention resulting in DNDCs being issued without any network having priority has been undertaken successfully in some overseas jurisdictions, including in Europe and Malaysia.

2.2.3 Consultation questions

The specific questions for consultation are listed below.

The Bank would like to understand the practical implications of preventing any one network from being given priority at issuance, with merchants instead choosing the routing network. This includes considering the technical aspects of the current debit card transaction infrastructure, so that DNDC transactions continue to be processed if such a policy were to be implemented. Accordingly, the Bank is particularly interested in feedback regarding any technical challenges that may need to be overcome if issuers are no longer able to set a default routing network on DNDCs. The Bank is also seeking estimates of the costs of complying with such a policy.

[3] See Treasury (2023), 'A Strategic Plan for Australia's Payments System', June.

[4] LCR may be implemented in different forms. For example, it may take the form of: (a) a simple binary decision rule, whereby all relevant transactions are routed to the network that is cheaper on average; (b) a threshold-based decision rule, whereby transactions are routed to different networks depending on whether the transaction value is above or below a certain threshold (with the chosen network cheaper on average for the merchant for the given value range); or (c) a dynamic decision rule, whereby the routing decision for each individual transaction is based on an assessment of the relative cost of each network for that particular transaction.

Question 1

What would be the technical or practical challenges raised by prohibiting the setting of a default routing network on DNDCs at issuance? How could these challenges be overcome?

- **a.** By when would it be feasible for payment service providers to have identified and implemented a routing network preference for all of their merchant customers (such as by moving them to a merchant payment plan that provides LCR)?
- **b.** Will existing merchant terminals be able to accept contactless transactions conducted using a DNDC without a set default routing network, assuming that payment service providers have implemented a routing network preference for all of their merchant customers?

Question 2

What would be the benefits of such a prohibition? What would be the costs? Please provide estimates of the costs that would likely be incurred by your institution.

Question 3

What alternative courses of action could better address the Bank's concerns around default settings on DNDCs to improve efficiency and competition in the debit card market?

3. Tokenisation of dual-network debit cards

3.1 Background

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.[5] Tokenisation can help to reduce the amount of sensitive card details that can be stolen from merchants and payment service providers that store this information for subsequent transactions. Tokenisation technology is being increasingly adopted and plays an important role in securing payment cards.

Despite tokenisation becoming more widespread, there continues to be extensive retention of sensitive card details by merchants and payment service providers, which undermines the security benefits of tokenisation. There continue to be high-profile examples of databases that store customer card information being breached by cyber criminals. According to AusPayNet data, in 2021/22 fraudsters made more than $270 million in card-not-present purchases at Australian merchants using stolen Australian card details. In addition to the cost of goods and services fraudulently obtained – which is often borne by the merchant – cardholders, merchants and financial institutions incur significant costs in investigating and resolving fraud cases; these costs are, at least to some degree, inevitably passed on to consumers in the form of higher prices.

There are two main types of tokenisation for card payments:

- Merchant tokenisation is where a merchant requests a customer's PAN to be tokenised by their payment gateway. The merchant does not store the PAN and instead uses the token provided by the gateway, which in turn has stored the PAN in a token vault. When processing the tokenised payment, the merchant's gateway then extracts the PAN from the token vault and sends it to the card scheme.
- 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 need to store the PAN, instead using the token provided by the card scheme. Network tokenisation limits PAN exposure during the authorisation process, reducing the risk of a PAN being compromised when passed from a payment gateway to the card scheme.

In addition to its important role in combatting fraud, tokenisation can also provide broader benefits to consumers and merchants. In particular, network tokens remain valid after a card expires or is replaced, since the new card details are updated in the scheme's token vault. This means that consumers do not face the inconvenience of having to update their card details stored with merchants. Merchants also benefit from this feature as they avoid declined transactions where customers have not updated their

[5] The PAN on a credit or debit card is a 16 to 19 digit number, typically on the front of the card, which identifies the unique cardholder account and the issuer of the card. The first (six to eight) digits of the PAN is the Bank Identification Number (BIN), also known as the Issuer Identification Number (IIN); see Box B 'Bank Identification Numbers' for more details.

details, as well as the risk of losing some customers when card details need to be updated. Network tokenisation could also be leveraged to offer consumers innovative features to help manage their recurring payments if issuers have full visibility over the tokens associated with the cards they issue.

In the Conclusions Paper to the Review of Retail Payments Regulation in late 2021, the Bank set an expectation that as online eftpos functionality was being rolled out, all acquirers, payment facilitators and gateways would be expected to offer and promote the least-cost routing of transactions made using DNDCs in the online environment by the end of 2022. This expectation was the catalyst for the Bank having discussions with stakeholders in 2022 on how tokenisation could be implemented for online DNDC transactions in a way that facilitates LCR (e.g. through tokens being provided for each of the two networks on the card). As part of these discussions, some stakeholders raised issues regarding the tokenisation of DNDCs for online transactions. However, there was a lack of consensus across industry participants about the nature and severity of these issues and how to address them.

The Bank expects tokenisation to be implemented, since it can substantially reduce the amount of sensitive card details being stored – sometimes with minimal security – across the payments ecosystem. However, it needs to be implemented in a way that does not impede the adoption of LCR or competition in the acquiring market more generally. Consequently, in late 2022 the Payments System Board requested that AusPayNet establish an industry working group to investigate challenges the industry may face in implementing tokenisation for online DNDC transactions and possible solutions.

The AusPayNet working group did not consider network tokenisation of DNDCs to be a factor inhibiting LCR for online DNDC transactions, primarily due to most ecosystem participants still retaining customers' PANs. Retention of PANs means that online LCR is possible, even where card details have already been tokenised by the international card networks, since DNDCs will be able to be tokenised for a second network once eftpos' tokenisation service launches. However, PAN retention perpetuates the security risk that tokenisation is designed to address. To achieve the full security benefits of tokenisation, PANs will need to be deleted by ecosystem participants once both networks on DNDCs have been tokenised. A key dependency as to when this can occur is the timing of the launch of eftpos' eCommerce tokenisation service.

The AusPayNet report also identified three main areas (outlined in section 3.2) where industry standardisation is necessary to ensure that the benefits of tokenisation are fully realised. The Payments System Board discussed the AusPayNet working group's findings at its May 2023 meeting and announced in its post-meeting media release that it would set some expectations for the industry to address impediments to tokenisation, with the aim of substantially lessening the reliance of merchants and payment service providers on databases of card numbers by the end of 2024. The Bank seeks stakeholders' views on possible solutions to achieving industry standardisation, including what detailed expectations the Bank could set on the steps the industry should take and the timelines for their completion.

3.2 Issues

The AusPayNet working group identified three areas where industry standardisation (consistent minimum outcomes rather than prescribed arrangements) is necessary to ensure that the full security and efficiency benefits of tokenisation are realised:

1. **Token portability** to ensure that merchants are not impeded from switching between payment service providers once their customers' cards have been tokenised. In the absence of token

portability, if a merchant switched provider to get a better deal, they would need to ask their entire customer base to re-enter their card details. For most merchants this would be highly unattractive, as they would likely face declined transactions and customer attrition, and it would likely have the practical effect of 'locking in' a merchant to their current provider. To avoid this, a merchant or their provider might choose to retain customers' PANs, but as discussed above, widespread retention of PANs undermines the security benefits of tokenisation.

2. **Token synchronisation** where issuers ensure that any issuer-related token life-cycle events related to a tokenised DNDC are updated to both schemes simultaneously, to reduce the potential for failed transactions.
3. **Token visibility** so issuers, and potentially their customers, can see which merchants have stored tokens for their cards. As noted above, if issuers have full visibility over tokenisation of their cards, they could potentially offer customers features in the future to manage their stored card details and recurring payments (this is consistent with what issuers in jurisdictions such as India are expected to provide their customers).

While the AusPayNet working group was able to reach a consensus on the need for industry standardisation in the three areas above, it did not reach a consensus on how best to set or enforce these.

In addition to seeking stakeholder views on the issues above – including their relative importance, potential solutions and desirable/feasible timelines for implementation – the Bank welcomes input on the details of the expectations it could set for the payments industry to address these issues and to substantially reduce the amount of card details being stored across the industry. Examples of the expectations the Bank could set are listed in Box C.

Box C: Possible RBA expectations for the tokenisation of DNDCs in the online environment

1. The rollout of the eftpos eCommerce tokenisation service should be completed by March 2024; to facilitate planning, relevant industry participants should be provided with regular updates on the service and its functionality ahead of the rollout.
2. All relevant industry participants – including schemes, gateways, and acquirers – should support the portability of scheme tokens by the end of 2024 to reduce the friction for merchants that wish to switch payment service providers.
3. Merchants, gateways and acquirers should use tokens for both networks on DNDCs and delete DNDC PANs once complete. The Bank expects the industry to have made substantial progress by the end of 2024.
4. Issuers and schemes should support network token synchronisation by the end of 2024.
5. Schemes should provide issuers with full visibility of the tokens created for the cards they issue by the end of 2024.

While the focus of the Bank's discussions with stakeholders to date has been on the tokenisation of DNDCs in the online environment, the Bank has a strong desire to see a significant reduction in *all* types of card details being stored across the ecosystem, including for credit cards. Accordingly, the Bank also welcomes 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) – when used for online transactions. The Bank notes that there are precedents in some jurisdictions such as India for broader initiatives aimed at promoting tokenisation to improve the security of card payments.

The specific questions for consultation are listed below.

Question 4

What is the relative importance of addressing the issues regarding token portability, synchronisation and visibility?

Question 5

What are the potential solutions to these issues and their respective costs and benefits?

Question 6

What expectations could the Bank set for industry to address these issues, and the storage of PANs more generally, and what key details should be specified?

Question 7

Would the end of 2024 be a desirable and feasible timeline for the industry to support token portability, and to make substantial progress in removing PANs from the ecosystem?

Question 8

Should the Bank and the industry consider broader action to encourage the tokenisation of card payments and removing PANs, as seen in some other jurisdictions?

4. Next steps

The Payments System Board is seeking views from interested parties on the issues raised in this Issues Paper. Written submissions should be provided by no later than 12 July 2023, and should be sent to:

Head of Payments Policy Department
Reserve Bank of Australia
GPO Box 3947
Sydney NSW 2001

or

pysubmissions@rba.gov.au

Submissions provided by email should be in a separate document, in Word or equivalent format. Submissions in PDF format must be accompanied by a version in an accessible format such as .rtf or .doc.

The Bank may seek to meet with some stakeholders in July 2023 to discuss their submissions in more detail.

Please see the RBA Submission Guidelines in Appendix B for additional information.

Appendix A: Key questions for stakeholders

The Bank is seeking submissions on the issues discussed in this paper, including stakeholder views on some or all of the following specific questions.

Question 1

What would be the technical or practical challenges raised by prohibiting the setting of a default routing network on DNDCs at issuance? Could these challenges be overcome?

a. By when would it be feasible for payment service providers to have identified and implemented a routing network preference for all of their merchant customers (such as by moving them to an LCR plan)?

b. Will existing merchant terminals be able to accept transactions conducted using a DNDC without a set default routing network, assuming that payment service providers have implemented a routing network preference for all of their merchant customers?

Question 2

What would be the benefits of such a prohibition? What would be the costs? Please provide estimates of the costs that would likely be incurred by your institution.

Question 3

What alternative courses of action could better address the Bank's concerns around default settings on DNDCs to improve efficiency and competition in the debit card market?

Question 4

What is the relative importance of addressing the issues regarding token portability, synchronisation and visibility?

Question 5

What are the potential solutions to these issues and their respective costs and benefits?

Question 6

What expectations could the Bank set for industry to address these issues, and the storage of PANs more generally, and what key details should be specified?

Question 7

Would the end of 2024 be a desirable and feasible timeline for the industry to support token portability, and to make substantial progress in removing PANs from the ecosystem?

Question 8

Should the Bank and the industry consider broader action to encourage the tokenisation of card payments and removing PANs, as seen in some other jurisdictions?

Appendix B: RBA submission guidelines

RBA submission guidelines

In the course of undertaking public consultation on policy or regulatory matters, the Reserve Bank of Australia (RBA) may publish an issues or consultation paper (Consultation Paper) and invite interested parties to make a submission responding to issues raised in the Consultation Paper (a Submission).

These Guidelines set out general information about making a Submission and the RBA's processes for considering and publishing Submissions. The Guidelines apply to all Submissions, except to the extent that a particular Consultation Paper specifies any contrary information with respect to Submissions made in response to that Consultation Paper.

Making a Submission

A Submission should be made in writing and sent by post or by email to the addresses specified in the Consultation Paper. The RBA asks that, where it is practicable to do so, submissions are provided by email.

Submissions provided by email should be in a separate document, in Word or equivalent format. Submissions in PDF format must be accompanied by a version in an accessible format such as .rtf or .doc.

Submissions can be submitted to the RBA until 5pm AEST on the closing date specified in the Consultation Paper or such later date agreed by the RBA.

What happens to Submissions?

Your Submission will be read by RBA staff working on, or involved with, the relevant consultation process to which your Submission relates.

In the interests of informed public debate, the RBA is committed to transparency in its processes and open access to information. Accordingly, the RBA aims to publish Submissions on its website where it is appropriate to do so. However, the RBA reserves the right to edit (for example, remove defamatory material or, where appropriate, de-identify personal or sensitive information, publish or not publish Submissions on its website at its own discretion. The RBA's publication of a Submission is not an indication of the RBA's endorsement of any views or comments contained in that Submission.

Most Submissions that are published on the RBA's website will include the name of the submitter (unless requested otherwise – see the Privacy section below). If a Submission is published, the information in it, including the submitter's name and any contact details, can be searched for on the internet.

You cannot withdraw or alter your Submission once the RBA has published it.

Submissions may be kept confidential

If you do not want some or all of your Submission to be published by the RBA, you should clearly indicate this (for example, by including the word **confidential** prominently on the front of your Submission) and provide reasons for your request. Automatically generated confidentiality statements in emails are not sufficient for this purpose.

Where some parts of your Submission are considered to be confidential, the RBA requests that you provide two versions of the Submission at the same time prior to the closing date – one for consideration by the RBA and one, with confidential information removed, for publication (this latter version may also have contact details or other personal information removed – see the Privacy section below).

Please also note that any Submission provided to the RBA may be the subject of a request under the *Freedom of Information Act 1982* (Cth). Any request for access to a confidential Submission will be determined by the RBA in accordance with that Act, including any applicable exemptions (for example, those relating to material obtained in confidence or involving an unreasonable disclosure of personal information).

Privacy

Unless requested otherwise, published Submissions will usually include contact details and any other personal information contained in those documents.

Where you provide a separate version of your Submission for publication with contact details or other personal information redacted or removed, this will be taken as a request for the RBA not to publish such personal information.

For information about the Bank's collection of personal information and approach to privacy, please refer to the Personal Information Collection Notice for Website Visitors and the Bank's Privacy Policy, which are both available at http://www.rba.gov.au/privacy

Intellectual property rights

In making a Submission to the RBA, you grant a permanent, irrevocable, royalty-free licence to allow the RBA to use, reproduce, publish, adapt and communicate to the public your Submission on the RBA's website (except to the extent that you have specifically requested that all or part of your Submission is kept confidential), including converting your Submission into a different format to that submitted for the purposes of meeting relevant accessibility requirements.

To the extent that your Submission contains material that is owned by a third party, you warrant that you have obtained all necessary licences and consents required for the use of those materials (including for the RBA to use, reproduce, publish, adapt or communicate to the public such material), and have made arrangements for the payment of any royalties or other fees payable in respect of the use of such material.