Australian Government
Attorney-General's Department

Reforming Australia's anti-money laundering and counter-terrorism financing regime

Paper 4: Further information for digital currency exchange providers (DCEPs), remittance service providers and financial institutions

May 2024

Australian Government
Attorney-General's Department

Contents

Introduction

Each year billions of dollars of illicit funds are generated from illegal activities such as drug trafficking, tax evasion, people smuggling, cybercrime, arms trafficking and other illegal and corrupt practices. Money laundering is not a victimless crime. It is a critical facilitator of most serious crimes and undermines the rule of law globally.

Serious and organised criminal groups are driven by illicit profit. It sits at the centre of why they conduct their illegal activities. Laundering this illicit wealth allows them to enjoy the proceeds of crime and to reinvest in further criminal activities. Illicit financing facilitates serious crimes across Australia and the world, diverting government resources which could be used for social, health or education services, increasing the burden on law enforcement, and ultimately impacting the most vulnerable in our community. Money laundering and illicit financing also erodes trust in Australia's stable financial system, our government institutions and the equitable application of the rule of law across Australian society.

Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime establishes a regulatory framework for combatting money laundering, terrorism financing and other serious financial crimes. At its core, the AML/CTF regime is a partnership between the Australian Government and industry. No legitimate business wants to wittingly, or unwittingly, assist money laundering. Through the regulatory framework, businesses are asked to play a vital role in detecting and preventing the misuse of their sectors and products by criminals seeking to launder money and fund terrorism.

As the Attorney-General announced in April 2023, the Attorney-General's Department (the department) is consulting on reforms to the regime. The reforms aim to ensure it continues to effectively deter, detect and disrupt money laundering and terrorism financing, and meet international standards set by the Financial Action Task Force (FATF), the global financial crime watchdog.

Criminal groups are constantly finding new ways to obfuscate the origins of their illicit funds, and also finding new ways to exploit weaknesses in global financial systems. The reforms would protect Australia's economy and systems against exploitation, ensuring Australia does not become a haven for criminals seeking to launder their proceeds or finance their illicit activities, and cut off funding for terrorists and terrorist organisations.

Ensuring Australia is compliant with the international standards set by the FATF is a fundamental objective of the proposed reforms. Australia's AML/CTF regime will next be comprehensively assessed by the FATF over 2026-27 where Australia will be assessed against strengthened standards. A poor assessment risks Australia being 'grey listed' by the FATF, which could have serious consequences for Australia, including tangible economic and gross domestic product (GDP) impacts, and increased threats, risks and burdens for law enforcement.

The reforms also present an opportunity to improve the effectiveness of the regime and ease regulatory burden by simplifying and clarifying the regime to make it easier for businesses to meet their obligations, and modernising the regime to reflect changing business structures and technologies across the economy.

Ultimately, the reforms aim to significantly improve Australia's ability to target illicit financing. They will reduce the ability of criminal actors and autocratic regimes to invest their illicit funds into further criminal activities, and disrupt serious crime in the Australian community and in our region.

The department held a first round of consultation in 2023. Feedback was supportive of simplifying, clarifying and modernising the regime. Industry and stakeholders requested further detail on how the reforms would impact them and operate in practice.

This paper provides further detail on the changes relevant to the DCEPs, remittance service providers and financial institutions, including:

- the expanded list of services provided by DCEPs to be regulated under the AML/CTF regime,
- the new streamlined value transfer services, and
- travel rule and international funds transfer instruction (IFTI) reforms.

The proposals outlined in this paper have not been settled. The paper is designed to seek your feedback on the practical impact on you or your business to inform Australian Government decisions on the proposed reforms to the regime.

Expanding the range of regulated digital currency-related services

Why does the range of digital currency-related services need to be expanded?

Digital currencies are an increasingly popular conduit to represent, store and move value, and the digital currency sector and related technologies continue to evolve. The past decade has seen a rapid increase in the adoption of digital currencies in Australia, with the ATO advising that over 1 million Australians included them on their tax returns in 2022. The proposed regulatory changes to cover additional digital currency-related services would ensure that this rapidly growing sector is hardened against potential exploitation by criminals.

In October 2018, the FATF amended Recommendation 15 to require countries to apply AML/CTF regulation to the following digital asset-related services when done on behalf of another person:

1. exchanges between digital assets for fiat currency, and vice versa
2. exchanges between one or more forms of digital assets

3. transfers of digital assets[1]
4. safekeeping and administration of digital assets, and
5. participation in and provision of financial services related to an issuer's offer and/or sale of a digital asset.

Australia's AML/CTF regime currently only regulates exchanges between digital currency and fiat currency, and vice versa. The department is proposing to extend regulation to capture all five services required to be regulated by the FATF.

The services required to be regulated by the FATF have been identified as posing a high risk due to their vulnerability to misuse for money laundering and terrorism financing. In particular, these services can enable non-face-to-face business relationships, be utilised to move funds globally and instantaneously and facilitate pseudo-anonymous or anonymity-enhanced transactions.[2] Bringing these services within the scope of AML/CTF regulation would require businesses providing these services to identify, mitigate and manage their risks.

The department is separately proposing to adopt the terminology of '**digital asset**' to replace the current term 'digital currency' in the Act. The detailed proposals below will utilise the term 'digital asset' to reflect this. Further detail on the proposed terminology change be found on page 8 of this paper.

Detailed proposal

The proposals below are intended to regulate businesses when they meet the current geographical link requirement. If your provision of the proposed designated services has a geographical link to Australia, you will be a reporting entity and have AML/CTF obligations. Further, where Australian businesses provide services offshore in foreign branches or subsidiaries, they will be expected to comply with their AML/CTF program obligations. More detail on this can be found under the 'Broader reforms to simplify, clarify and modernise' heading.

The department proposes that the following designated services be amended or inserted into the Act. If you provide one or more of the digital asset-related designated services described in the Act, you must enrol and register with Australia's AML/CTF regulator and financial intelligence unit, AUSTRAC, as a digital asset service provider, unless your business is a financial institution.

[1] This service is proposed to be captured in the streamlined value transfer services and would also require registration as a digital asset business. This reform proposal is discussed in more detail under the 'streamlined value transfer services' heading.

[2] FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (Paper, October 2021).

Proposed amendment to Item 50A of Table 1 in section 6 of the Act

Exchanging or making arrangements for the exchange of digital asset for money (or vice versa) where the exchange is provided in the course of carrying on a digital asset business. The customer is the person whose digital asset or money is exchanged.

This designated service is currently regulated under item 50A of Table 1 in section 6. The proposed change to the designated service adopts minor additional wording to capture the FATF requirement to regulate the participation in, and provision of, financial services related to an issuer's offer and sale of a digital asset.

Proposed designated service 2

Exchanging, or making arrangements for the exchange of, one digital asset for another where the exchange is provided in the course of carrying on a digital asset business. The customer is the person whose digital asset is exchanged.

Consistent with FATF guidance, this proposed designated service would apply to any digital asset service provider regardless of the role they play in the process—whether they are a principal, a central counterparty for clearing or settling transactions, or another intermediary facilitating the transaction. A digital asset service provider would not have to provide every element of the exchange to be captured by the regime.

What would this look like?

Siobhan previously purchased $5,000 worth of Ethereum from DASPX and leaves it in a custodial wallet held by DASPX. DASPX is already registered with AUSTRAC, and undertook customer due diligence on Siobhan before it provided the designated service of exchanging money for digital assets.

Siobhan would now like to purchase an item using digital assets. The seller requests payment in bitcoin. Siobhan exchanges eth for bitcoin through DASPX, and instructs DASPX to transfer the bitcoin to the seller who provides a bitcoin wallet address at another digital asset service provider, DASPY. DASPX has therefore provided the designated services of exchanging digital assets for digital assets and transferring digital assets on behalf of a customer. All AML/CTF obligations including ongoing CDD, record keeping and reporting suspicious matters (if relevant) apply, although DASPX will not need to undertake initial CDD for Siobhan again given it has previously done so. DASPX will, however, also be required to comply with travel rule obligations (outlined below).

Proposed designated service 3

Providing custodial services of a digital asset or a private key on behalf of a person, where the services are provided in the course of carrying on a digital asset business. The customer is the person whose digital asset or private key is held in custody.

This proposed designated service is intended to apply to any entity that has custody over digital assets. For example, this would include having the ability to hold, trade, transfer or spend the digital asset on behalf of a customer. Custodial services could include persons who have custody of:

- a private key associated with another person's digital asset
- one of multiple private keys in a multi-signature arrangement, or
- smart contracts to which they are not a party.

The Act currently defines 'custodial services' by reference to the *Corporations Act 2001* (Cth), which may need to be adapted under the AML/CTF Act to cover similar services provided in relation to digital assets. The department will continue to work with Treasury to explore opportunities for alignment with proposed reforms related to digital asset platforms. In line with the FATF approach, the department does not propose to capture businesses that provide ancillary infrastructure, such as cloud data storage providers, which allow another entity to offer these services.

Proposed designated service 4

Providing a financial service (defined as a designated service in Table 1 of the Act) relating to an issuer's offer or sale of a digital asset, where the service is provided in the course of carrying on a digital asset business participating in the offer or sale. The customer is defined in the relevant item in Table 1 of section 6 of the Act.

This service refers to those providing financial services in the context of initial coin offerings and similar arrangements, and would be limited to businesses participating in the issuer's offer or sale of digital asset. Table 1 of section 6 of the Act lists traditional financial services such as making loans and acting as a guarantor. The requirement for 'participation' would exclude banks processing payments by their customers to purchase digital assets under an issuer's offer or sale if the bank is not otherwise involved in the offer or sale.

Consultation questions

a. Do you consider that the current term and associated definition of 'digital currency' is appropriate? What alternative terms outside of 'digital asset' might be considered, and why?
b. How should the scope of NFTs subject to AML/CTF regulation be clarified?
c. Are there any services that may be covered by the term 'making arrangements for the exchange…' that should not be regulated for AML/CTF purposes?
d. Is the proposed language around custody of digital assets or private keys clear?
e. Does limiting proposed designated service 4 to businesses 'participating' in an issuer's offer or sale of a digital asset clarify the scope of included services?

Amending the definition of 'digital currency'

Why does the definition of 'digital currency' need to be changed?

While the 'digital currency' definition in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act) generally works well, the evolving concept of digital currencies has resulted in regulatory gaps. For example:

- industry has raised concerns about the extent to which the definition applies to non-fungible tokens (NFTs), and
- the Act's requirement for digital currency to be 'generally available to members of the public without any restriction on its use'[3] has raised questions about the scope of coverage of stablecoins[4] minted on public blockchains which the issuer nevertheless intends only to be used by a subset of the public (e.g. their own customers).

FATF states that generally NFTs are not subject to the global FATF standards where they are in practice used as collectibles. However, FATF Guidance requires that regulators look beyond marketing terms to the underlying purpose. If a token functions as a means of payment or investment instrument it should be subject to AML/CTF regulation.

The FATF also recognises the type of stablecoins outlined above share many of the same ML/TF risks as other digital currencies because of their potential for anonymity and transferability outside of traditionally regulated sectors.[5] The increasing use of stablecoins as a means for the cross-border movement of value reinforces the argument that they should be subject to the same AML/CTF regulation in all cases as money and other means of transmitting value.

Detailed proposal

The department proposes adopting the terminology of '**digital asset**' to replace the current term 'digital currency' in the Act.

This would also align with other Australian Government developments.[6] Submissions to the first consultation paper commented on the need to take a whole-of-government approach to

[3] This element of the definition was originally intended to exclude 'closed loop' loyalty or rewards schemes, as well as credits issued by the operators of online role-playing games.
[4] Under the FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs), stablecoins are digital currencies that purport to maintain a stable value relative to a reference asset or assets such as fiat currency.
[5] FATF, 'FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins' (Paper, June 2020) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.
[6] Treasury, 'Regulating digital asset platforms' Department of the Treasury (Paper, 16 October 2023) https://treasury.gov.au/consultation/c2023-427004. Treasury has indicated a preference for the term 'digital asset' when referring to a digital token and its entitlements.

reforms, including reforms to Australia's payments systems led by Treasury. The department is also open to considering other terminology such as 'crypto asset' and 'virtual asset'.

The department proposes that Central Bank Digital Currencies (CBDCs) could be explicitly captured under the definition of 'money'.

Ensuring the integrity of remittance providers and digital asset service providers

Why do the current arrangements for remittance providers and digital asset service providers need to be amended?

Currently, AUSTRAC can refuse, cancel or suspend the registration of remittance service providers and digital asset service providers if they pose an unacceptable risk.

However, there is no power to restrict or ban individuals from key personnel roles with remittance providers or digital asset service providers. Unlike most other reporting entity sectors, these sectors are not subject to comprehensive fit-and-proper person regulation under a regulatory framework. For example, most entities providing financial services are required to obtain an Australian Financial Services License (AFSL), which includes fit-and-proper person checks. It is essential that the fit-and-proper person standard is upheld in relation to the digital asset service provider and remittance sectors, so that they are able to uphold the highest standards of integrity.

Detailed proposal

The proposed reforms would allow the AUSTRAC CEO to prohibit individuals from involvement in the management or business of a remittance service provider or a digital asset service provider based on a demonstrated lack of suitability, fitness or propriety. This would bring these sectors in line with the financial services sector, as similar powers allow ASIC to make such orders under the AFSL regime. The department proposes to give the AUSTRAC CEO the power to prohibit a person from:

- providing remittance services or digital asset services, or
- controlling, or performing functions involved in carrying on, a remittance or digital asset service business (including as an officer, manager, employee, contractor or in some other capacity).

The reforms could also empower the AUSTRAC CEO as part of registration, suspension and cancellation of registration decisions to consider:

- the capability of a remittance service provider or a digital asset service provider and its key personnel to comply with the AML/CTF Act and Rules, and

- whether key personnel connected with the applicant are fit and proper.

Any decision by the AUSTRAC CEO to prohibit or restrict an individual from involvement in a remittance service provider or digital asset service provider would be subject to procedural fairness and administrative review.

Streamlining value transfer service regulation

Why do remittance services need to be clarified and updated?

Clarifying the scope of remittance services subject to AML/CTF regulation

The current framework for transfers of value across borders is based on an outdated distinction between the transfers of value undertaken by financial institutions and those undertaken by remittance service providers. It has also not kept pace with the emergence of digital assets. This has led to significant challenges for payments service providers in interpreting their AML/CTF obligations.

The current definition of a 'designated remittance arrangement' in section 10 of the Act is extremely broad in its application to arrangements for transferring money on behalf of another person, except for those performed by financial institutions. It also raises questions about its application to arrangements for transferring money or property where the transfer of money is incidental to the provision of another service. For example, superannuation funds, car fleet managers and stockbrokers. Recommendation 11.2 of the 2016 *Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Statutory Review) noted that the definition is too broad and recommends that it be narrowed to exclude non-remittance businesses.

Streamlining 'value transfer' designated services and regulation of digital asset transfers

There are currently four separate value transfer services outlined in the Act, which is unnecessarily complex and fails to cover the transfer of digital assets on behalf of customers. This creates a gap in AUSTRAC's financial intelligence and can hinder law enforcement investigations. Streamlining the value transfer services provided by financial institutions, remittance service providers and digital asset service providers into a set of 'value transfer' designated services would simplify the regulation of payments.

Detailed proposals

Definitions

The department proposes to remove the definitions of '**electronic funds transfer instruction**' and '**designated remittance arrangement**' in sections 8, 9 and 10 of the Act, and replace those terms with a streamlined concept of a 'value transfer service'. This concept would apply to remittance providers, digital asset service providers and financial institutions that provide remittance-type services as part of their core business.

This change would also ensure that businesses that do not provide remittance services as part of their core business would not be incidentally captured by the AML/CTF regime.

Streamlined value transfer services

In order to create the streamlined value transfer services, the designated services in items 29, 30, 31 and 32 of Table 1 of the Act would be replaced with the following streamlined value transfer services:

Proposed designated service 5

In the capacity of an ordering institution, accepting an instruction to transfer value on behalf of a payer. The customer is the payer.

Proposed designated service 6

In the capacity of a beneficiary institution, making transferred value available to a payee. The customer is the payee.

These proposed designated services are intended to capture the transfer of money or other stores of value, including digital assets. Consistent with the existing funds transfer and remittance designated services, it would exclude the transfer of physical assets such as cash or bullion on behalf of a customer, or payments using cheques or other negotiable instruments drawn by the payer on the ordering institution.

Proposed designated service for intermediary institutions

Despite having a range of AML/CTF obligations, a business that only operates as an intermediary institution is unable to enrol with AUSTRAC or submit suspicious matter reports (SMRs) because it does not provide a designated service. The FATF standards require intermediary institutions to implement reasonable measures to identify value transfer messages that lack required payer and payee information, and to apply risk-based policies, systems and controls to determine whether to pass on, suspend or reject messages lacking this information. The department is considering whether this gap could be addressed by creating a limited designated service for those institutions, with obligations limited to those related to their role in the value transfer chain.

Proposed designated service 7

In the capacity of an intermediary institution, passing on a message in a value transfer chain to another intermediary institution or the beneficiary institution. The customer is the ordering institution or intermediary institution from which the message was received.

Given the nature of the services provided by intermediary institutions, i.e. as they do not have a direct business relationship with either the payer or payee in a value transfer, it may be appropriate to exempt them from a range of AML/CTF obligations when providing the designated service alone. This would include exemption from Customer Due Diligence (CDD) and ongoing CDD obligations (other than transaction monitoring). This would not, however, extend to exempting correspondent banks from CDD obligations where they provide an account service to another bank.

This will be supported by a definition of an intermediary institution, discussed below.

Proposed definition of 'value transfer chain'

The new designated services would be supported by an updated concept of a 'value transfer chain' which would define the terms 'ordering institution', 'intermediary institution' and 'beneficiary institution' by reference to their role in the value transfer chain. The inclusion of the terms 'ordering institution' and 'beneficiary institution' would exclude non-financial institutions that transfer value incidentally, such as entities that provide car fleet management services or other services in which value is passed on behalf of a customer incidentally to another service. An intermediary institution would be defined to mean a business which receives and passes on a message on behalf of the ordering or beneficiary institution. This would, however, exclude any business solely providing messaging infrastructure to allow the transmission of messages as part of a value transfer chain.

The ordering institution, any intermediary institutions and beneficiary institution would form a value transfer chain for the purposes of the travel rule and IFTI reporting reforms. Streamlining a value transfer chain would reduce undue regulatory burden on industry by clarifying obligations and concentrating these obligations on the transactions that are intended to be covered by each party.

Consultation questions

f. Are there any services currently provided by financial institutions that fall outside the definition of 'electronic funds transfer instruction', but would be captured by the 'value transfer' concept?
g. Is the terminology of ordering, intermediary and beneficiary institutions clear for businesses working in the remittance and digital asset service provider sectors?
h. Is the introduction of a limited designated service with appropriate exemptions the simplest way to clarify the transaction monitoring and risk mitigation and management expectations for intermediary institutions?

Updates to the travel rule

The travel rule is a FATF requirement for information about a payer and payee to 'travel' with a transfer of value. The travel rule is a record-keeping and data transmission requirement, not a reporting requirement. It serves two purposes:

- to allow law enforcement and regulatory agencies to obtain information on parties to value transfer transactions, and
- to support end-to-end transparency and risk management of transactions for businesses in a value transfer chain.

Why do the travel rule obligations need to be updated and extended to the remittance and digital asset sectors?

Under the current AML/CTF regime, only financial institutions are subject to the travel rule. Recommendations 15 and 16 of the FATF Standards require the travel rule to be applied to financial institutions, remittance providers and digital asset service providers. Under the proposed reforms, the streamlined value transfer services would trigger the travel rule for financial institutions, remittance providers and digital asset service providers for both domestic and cross-border transfers.

Further, the AML/CTF regime currently only requires information about the *payer* to be transmitted or received. However, FATF Recommendations 15 and 16 require information about both the payer and the *payee* to be transmitted or received. FATF Recommendation 15 also requires the payer information to be verified by the ordering institution. The proposed reforms would update Australia's implementation of the travel rule to align with FATF Recommendations 15 and 16.

Case study: Expanding the travel rule to cover digital currency

In August 2020, three individuals were sentenced for charges relating to purchasing stolen goods through their Melbourne-based gold buying business. In addition to knowingly buying proceeds of crime, it is suspected that they actively recruited criminals to carry out ram-raids of Melbourne-based jewellers in order to profit from the stolen takings.

Following Victoria Police interdiction, the syndicate expanded to Western Australia (WA) where they established a number of companies linked to a common business address. It is likely the relocation was an attempt to establish a presence in a new jurisdiction where they were not known to law enforcement. In January 2023, WA Police commenced Operation B to investigate the syndicate's suspected money laundering using several Perth-based businesses, including a registered DCE. The DCE was identified providing digital currency in exchange for cash received from persons involved in drug trafficking in WA. Furthermore, the investigation revealed the DCE traded a significant value of digital currency derived from one specific online casino. Although the DCE fulfilled AUSTRAC reporting requirements, it is likely this was done to a minimum standard. It is likely the DCE was willing to accept and process suspicious high value cash transactions where criminality was evident or inferred, given previous findings in Victoria.

The proposed 'travel rule' for digital currency transactions would have made it easier to trace the flow of funds observed during the investigation. The travel rule would have allowed investigators to access the identities of individuals purchasing digital currency from the DCE.

While investigators were able to determine the identities of some suspects who transacted beyond the $10,000 threshold, those that structured deposits in smaller amounts were able to maintain anonymity. Intelligence gathered during the operation identified many of the cash to digital currency customers were either likely to be involved in drug dealing activities, or were victims of scams and money was exchanged into digital currency wallets that could be accessed off shore. The travel rule would not only improve visibility of the beneficiaries of cash to digital currency transactions, but it would also cast a light on the identities of off-shore cyber-predators that target vulnerable Australians using various types of scams.

Detailed proposals

Travel rule trigger

The department proposes the new streamlined value transfer services would trigger the travel rule record-keeping and transmission obligations. This would result in responsibilities for all entities in the value transfer chain, including the:

- collection of travel rule information and verifying payer details for the **ordering institution**,
- keeping records of travel rule information, screening value transfer messages for missing travel rule information and taking appropriate action for **all institutions**, and
- transmitting travel rule information for **ordering and intermediary institutions**.

When the payer is an existing customer of the ordering institution, there would be no requirement for the ordering institution to collect or re-verify travel rule information if previously verified. It would simply need to be included in the value transfer message.

Travel rule information

Consistent with existing requirements, the department is proposing that full travel rule information would be required to be included with domestic and cross-border value transfers of money or property, except in the following circumstances:

- domestic value transfers where the ordering institution can provide full travel rule information to the beneficiary institution and authorities on request, or
- incoming cross-border value transfers where full travel rule information cannot be transmitted to the beneficiary institution due to technical limitations in existing Australian payment systems (for example the Bulk Electronic Clearing System).

In these circumstances, a subset of information sufficient to trace the transaction through the value transfer chain may be transmitted instead.

Travel rule and digital asset transfers

Consistent with the FATF standards, the department proposes that full travel rule obligations would apply to all digital asset transfers where digital assets are transferred from one financial institution or digital asset service provider to another. The exceptions outlined above for transfers of money or property would not apply.

Where there is a transfer of digital assets to a self-hosted wallet, limited travel rule obligations would apply. Under this approach, financial institutions and digital asset service providers involved in these transfers would be required to undertake counterparty due diligence to determine whether the destination of the transfer is a custodial wallet held with a regulated financial institution or digital asset service provider. For transfers to and from self-hosted wallets financial institutions and digital asset service providers would be required to:

- collect travel rule information from their own customer and, if the financial institution or digital asset service provider is the ordering institution, verify the payer information, and
- keep records of travel rule information,

but there would be no requirement to transmit, receive or screen for missing travel rule information.

Travel rule exemptions

The department is considering whether the current exemptions from the travel rule contained in section 67 of the Act remain appropriate or whether there are opportunities to clarify them in line with the FATF Standards. To streamline the legislation, exemptions from the travel rule reporting obligations and exemptions to the IFTI reporting obligations would be aligned where possible.

Travel rule thresholds and the 'sunrise issue'

Different countries have different applications of the travel rule, including different monetary thresholds at which the travel rule is triggered. Additionally, counterparty providers may be based in jurisdictions that have not yet implemented the travel rule and do not have a solution in place to send or receive travel rule information (referred to as the 'sunrise issue').

This means that sometimes travel rule information may be missing or incorrect when received from these countries. To address this, financial institutions, remittance providers and digital asset service providers would be required to take a risk-based approach to determining whether to make value available to the payee for incoming transfers lacking travel rule information. Additionally, the department proposes to maintain a zero threshold in Australia for all value transfers in line with existing requirements for financial institutions, rather than having the travel rule apply only above a certain monetary threshold. The department will consider how to manage travel rule information for transfers of digital assets if there are concerns about the data security and privacy protections implemented by a counterparty.

Consultation questions

i. What flexibility should be permitted to address the sunrise issue or where a financial institution or digital asset service provider has doubts about an overseas counterparty's implementation of adequate data security and privacy protections? What risk mitigation measures should be required?

j. Do you consider that the existing exemptions for the travel rule are appropriately balanced?
k. Are there challenges for financial institutions reporting cross-border transfers of digital assets, including stablecoins, on behalf of customers?
l. Should the travel rule apply when transferring value incidental to a foreign exchange or gambling service?

Reforms to IFTI reports

IFTI reports are a critical source of financial intelligence to combat and disrupt financial crime. In 2021-22 they comprised 98 per cent of AUSTRAC's financial intelligence. An IFTI involves either an instruction that is accepted in Australia for money or property to be made available in another country, or an instruction that is accepted in another country for money or property to be made available in Australia. IFTI reports are not contingent on the reported transaction being suspicious or unusual and therefore also provide a baseline measurement of 'normal' cross-border transactions.

IFTI reporting obligations do not apply to all regulated entities. The obligation falls on the sender of an instruction to transfer funds out of Australia, or the recipient of an instruction sent into Australia, whether or not the payer or payee is its customer. However, this 'first in, last out' approach has led to data quality problems in IFTI reports, as the first-in institution in Australia can only report information about the payee based on the information received from the overseas bank.

Why do IFTI reports need to be streamlined?

Financial institutions provided feedback throughout the first consultation process that simplification and modernisation of the IFTI reporting framework was a priority for reform. The current framework for submitting IFTI reports is outdated and is increasingly complex to apply to modern payment services. The proposed reforms would streamline obligations into a single IFTI report.

Some smaller businesses and sole traders indicated that they do not have the capacity to submit IFTI reports and that removing the current system of correspondent banks or remittance network providers submitting IFTI reports on their behalf would unduly increase the regulatory impact.

Detailed proposals

The reporting entity closest to the Australian customer should report IFTIs

The department proposes that the obligation to report IFTIs should rest with Australian institutions that initiate the outgoing transaction, or make the incoming payment available, for their customers. These institutions have a direct relationship with the payer and payee respectively.

Some businesses like correspondent banks or remittance network providers may still wish to offer to report IFTIs on behalf of smaller businesses. To mitigate regulatory burden on small businesses in particular, the reforms propose to allow correspondent banks or remittance network providers to report IFTIs on their behalf, subject to appropriate policies, systems and controls to the accuracy and completeness of IFTI reports. While the small business would remain responsible for any non-compliance with IFTI reporting obligations, defences would be available where the small business exercises due diligence.

What would this look like?

For example, a customer of a credit union wants to send funds overseas. The credit union has the relationship with the customer and thus has previously undertaken appropriate CDD with the customer. The credit union does not have the infrastructure to facilitate the funds transfer directly to the overseas institution, so they organise for the customer's money to be sent by Worldwide Capital Bank, a larger financial institution. The credit union and Worldwide Capital Bank agree to work together to ensure the accuracy of information in the IFTI report triggered by the funds transfer. As the credit union has delegated the obligation to report to Worldwide Capital Bank, they would not be liable for any non-compliance. However, they would be liable if the policies, systems, and controls they put in place were not reasonably sufficient to ensure the accuracy and completeness of the IFTI reporting.

IFTI reports should relate to the movement of value rather than movement of instructions

The department proposes to update the trigger for reporting IFTIs, so that IFTI reports would be triggered by the reporting entity sending value, or making it available to the customer, rather than it being triggered by the sending or receipt of an instruction which could subsequently not be given effect. This would minimise the possibility of cancelled and aborted IFTIs triggering the reporting requirement. IFTIs would still need to be reported within 10 days.

To achieve this, the department proposes IFTI reporting obligations be amended so that an IFTI report is triggered by a reporting entity acting on an instruction:

- for outgoing IFTIs, the ordering institution's reporting obligation would be triggered by initiating the transfer, or
- for incoming IFTIs, the beneficiary institution's reporting obligation would be triggered by making the transferred value available to the payee.

Streamline IFTI-E and IFTI-DRA reports in a single IFTI report

Under the current regime, there are two types of IFTIs. IFTI-Es (IFTI-electronic) relate to cross-border electronic funds transfer instructions that are sent or received between financial institutions on behalf of customers. IFTI-DRAs (IFTI-designated remittance arrangements) are instructions to transfer money or property under a designated remittance arrangement where one of the entities involved is not a financial institution.

IFTI-Es and IFTI-DRAs require reporting of different information and in a different format. The differences between these reports are unnecessarily complex, particularly for IFTIs that involve both financial institutions and remitters, and leads to inconsistency between sectors. These scenarios will likely increase as payment services continue to diversify and interoperability between payment systems becomes more common.

The department proposes to abolish the distinction between IFTI-Es and IFTI-DRAs and merge the two report types into a single IFTI report. This would allow IFTI reporting to adapt to current and emerging payment services and would reduce help reduce regulatory burden and complexity for businesses.

Extend IFTI reporting to digital asset transfers

The department proposes that IFTI reporting be extended to transfers of digital assets. This reporting would be limited to financial institutions or digital asset service providers transferring digital assets to, or receiving from, a counterparty based overseas on behalf of a customer. The geographic test for IFTIs related to digital asset transfers would therefore be tied to the overseas location of a counterparty's permanent establishment or an overseas jurisdiction in which the overseas counterparty is registered or licensed. The department is also considering whether IFTI reporting and other risk mitigation should be triggered by transfers of digital assets to or from self-hosted wallets whose ownership is unverified by the digital asset service provider or financial institution.

Apply IFTI reporting to certain incidental remittances

As noted above, the current definition of a 'designated remittance arrangement' is broad enough to capture arrangements for transferring money or property where the transfer of money is incidental to the provision of another service, which creates unintended regulatory burden. However, the department considers that the provision of some incidentally captured services should continue to carry an IFTI reporting requirement due to identified ML/TF risk.

The department proposes the Act be amended to expressly provide that IFTI obligations are triggered where a reporting entity, in providing a foreign currency conversion service contained in Item 50 of Table 1 of the Act, or a gambling service contained in Table 3 of the Act:

- transfers, or arranges to transfer value, out of Australia on behalf of the payer, or
- makes available, or arranges with the payee to make available, value transferred into or out of Australia to a payee.

Consultation questions

m. What is the anticipated regulatory impact for smaller financial institutions and remittance providers in giving them primary responsibility to report IFTIs sent or received by their customers?

  i. Could this impact be offset by continuing to allow intermediary institutions to submit IFTI reports on behalf of smaller reporting entities, but with requirements for appropriate safeguards to ensure the accuracy and completeness of reports?

n. What should be the 'trigger' for reporting IFTIs? At what point is a reporting entity reasonably certain that the value transfer message will not be cancelled or refused and the value transferred?
o. What information should be required to be reported in a unified IFTI reporting template, covering both IFTI-Es and IFTI-DRAs?
p. Are there challenges with digital asset service providers reporting IFTIs to AUSTRAC as proposed?

Cross-border movement of bearer negotiable instruments (BNIs)

The department is not proposing to change the current cross-border movement reporting framework, as it is compliant with Recommendation 32 of the FATF Standards and implements Recommendation 12.1 of the Statutory Review.

Industry stakeholders have expressed concern that the Act's current definition of a BNI is unclear, too broad and could make the cross-border movement reporting obligation for BNIs burdensome to comply with. This includes concerns that the definition creates uncertainty for reporting entities as to whether low risk instruments that are 'non-bearer' or 'non-negotiable' (i.e. named and crossed cheques) are captured under the framework.

In light of these concerns, the department proposes to reduce the impost associated with cross-border movement reporting of BNIs by clarifying the BNI definition in the Act.

The department proposes to amend the BNI definition in section 17 of the Act to clarify that it only covers instruments that are truly bearer negotiable in nature, that is instruments that are in bearer form, endorsed without restriction, made out to a fictitious payee or otherwise in such form that title to the instrument passes to the recipient upon delivery. This approach would also bring the BNI definition in the Act closer to the definition in the FATF Standards glossary.

Consultation questions

q. Would the proposed amendments to the BNI definition in the Act reduce the volume of reportable BNIs and regulatory impost on business?

Additional issues

Nested services relationship due diligence

Recommendations 13 and 15 of the FATF standards require due diligence to be conducted by remittance providers and digital asset service providers when involved in relationships similar to correspondent banking relationships. The department does not propose to create a bespoke correspondent due diligence obligation for these sectors. Instead, an Australian entity would be required to undertake enhanced due diligence where it provides services to a foreign counterparty remittance provider or digital asset service provider, which the counterparty would then use to provide services to its own customers. These are sometimes known as nested services. This enhanced due diligence would include understanding the nature of the counterparty's business, its reputation, regulatory status and AML/CTF controls.

Broader reforms to simplify, clarify and modernise the regime

In addition to the proposals outlined in this paper, the department proposes to simplify and clarify whole-of-regime obligations for AML/CTF programs, CDD and information sharing. This would remove prescriptive requirements, reduce administrative burden, and reinforce the risk-based approach of the regime.

Simplification reforms to AML/CTF programs and CDD requirements would facilitate an outcomes-based approach so that reporting entities can effectively identify, assess and understand the risks and to verify the identity of customers.

Please refer to Paper 5: Broader reforms to simplify, clarify and modernise the regime for further information.

When would the changes take effect?

If the proposed reforms become law, digital asset service providers, remittance service providers and financial institutions would be given time to make arrangements and prepare before being regulated under the AML/CTF regime. For example, when the Act was introduced in 2006, regulated businesses were given an extended period of time to allow them to meet their obligations.

To help businesses prepare, AUSTRAC would work closely with reporting entities to help you understand and meet your AML/CTF obligations. AUSTRAC's comprehensive guidance material, e-learning courses, and information sessions for the sector, can assist regulated entities to understand and implement their AML/CTF obligations, including identifying specific risks.

AUSTRAC also conducts information seminars for regulated sectors and operates a contact centre for businesses to assist with simple queries and accessibility to AUSTRAC systems. AUSTRAC would continue to deliver this support for the enhanced AML/CTF legislative regime as well as produce targeted and sector specific guidance to assist businesses providing certain high-risk services to understand and fulfil their obligations.

Consultation questions

a. Do you consider that the current term and associated definition of 'digital currency' is appropriate? What alternative terms outside of 'digital asset' might be considered, and why?
b. How should the scope of NFTs subject to AML/CTF regulation be clarified?
c. Are there any services that may be covered by the term 'making arrangements for the exchange…' that should not be regulated for AML/CTF purposes?
d. Is the proposed language around custody of digital assets or private keys clear?
e. Does limiting proposed designated service 4 to businesses 'participating' in an issuer's offer or sale of a digital asset clarify the scope of included services?
f. Are there any services currently provided by financial institutions that fall outside the definition of 'electronic funds transfer instruction', but would be captured by the 'value transfer' concept?
g. Is the terminology of ordering, intermediary and beneficiary institutions clear for businesses working in the remittance and digital asset service provider sectors?
h. Is the introduction of a limited designated service with appropriate exemptions the simplest way to clarify the transaction monitoring and risk mitigation and management expectations for intermediary institutions?
i. What flexibility should be permitted to address the sunrise issue or where a financial institution or digital asset service provider has doubts about an overseas counterparty's implementation of adequate data security and privacy protections? What risk mitigation measures should be required?
j. Do you consider that the existing exemptions for the travel rule are appropriately balanced?
k. Are there challenges for financial institutions reporting cross-border transfers of digital assets, including stablecoins, on behalf of customers?
l. Should the travel rule apply when transferring value incidental to a foreign exchange or gambling service?
m. What is the anticipated regulatory impact for smaller financial institutions and remittance providers in giving them primary responsibility to report IFTIs sent or received by their customers? Could this impact be offset by continuing to allow intermediary institutions to submit IFTI reports on behalf of smaller reporting entities, but with requirements for appropriate safeguards to ensure the accuracy and completeness of reports?
n. What should be the 'trigger' for reporting IFTIs? At what point is a reporting entity reasonably certain that the value transfer message will not be cancelled or refused and the value transferred?

o. What information should be required to be reported in a unified IFTI reporting template, covering both IFTI-Es and IFTI-DRAs?

p. Are there challenges with digital asset service providers reporting IFTIs to AUSTRAC as proposed?
q. Would the proposed amendments to the BNI definition in the Act reduce the volume of reportable BNIs and regulatory impost on business?