

Australia

Peter Reeves

Gilbert + Tobin, Sydney

PR Reeves@gtlaw.com.au

Anthony Basa

Gilbert + Tobin, Sydney

ABasa@gtlaw.com.au

Maya Ruber

Gilbert + Tobin, Sydney

MRuber@gtlaw.com.au

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Australia, the regulatory regimes are technology agnostic, with the same regulatory concepts applying to fintech businesses and other types of financial service providers. The regulatory framework that applies to fintech businesses includes:

- financial services and consumer credit licensing;
- registration and disclosure obligations;
- consumer law requirements;
- privacy; and
- anti-money laundering and counter-terrorism financing (AML/CTF) requirements.

Financial services and consumer credit laws

The Corporations Act 2001 (Cth) ('Corporations Act') is the principal legislation that regulates the provision of financial services. Fintech businesses that carry on a financial services business in Australia must hold an Australian financial services licence (AFSL) or be exempt from the requirement to be licensed. Financial services are broadly defined under the Corporations Act to include the provision of financial product advice, dealing in financial products (as principal or agent), making a market for financial products, operating registered schemes and providing custodial or depository services. There are specific things that are listed as financial products (eg, securities, derivatives and managed investment schemes). Financial products are also defined generally as a facility through which, or through the acquisition of which, a person makes a financial investment, manages a financial risk or makes a non-cash payment (NCP). The definitions of financial service and financial product will generally capture any investment or wealth management business, payment service (ie, NCP), advisory business (including robo-advice), trading platform or crowdfunding platform.

Fintech businesses may also need to hold an Australian market licence where they operate a facility through which offers to buy and sell financial products are regularly made and accepted (eg, an exchange). In addition, if an entity operates a clearing and settlement (CS) mechanism which enables parties transacting in financial products to meet obligations to each other, the entity must hold a CS facility licence, or be exempt from the requirement to be licensed.

The National Consumer Credit Protection Act 2009 (Cth) ('Credit Act') imposes a licensing obligation on entities that engage in consumer credit activities. Fintech businesses that provide marketplace lending products and related services will generally constitute consumer credit activities that trigger the requirement to hold an Australian credit licence (ACL) or be exempt from the requirement to be licensed.

Adjacent to the Corporations Act and the Credit Act, the Australian Securities and Investments Commission Act 2001 (Cth) ('ASIC Act') contains prohibitions on misleading and deceptive conduct,

false or misleading representations, unconscionable conduct and unfair contract terms that will apply to fintech businesses that supply financial services or consumer credit.

The Australian Securities and Investments Commission (ASIC) is Australia's financial markets conduct regulator and is responsible for regulating the financial services and consumer credit regimes.

Australian consumer law

Fintech businesses may be subject to prohibitions in the Australian Consumer Law under the Competition and Consumer Act 2010 (Cth) ('Competition Act') which is enforced by the Australian Competition and Consumer Commission (ACCC).

The Australian Consumer Law applies to Australian businesses that engage or contract with consumers and small businesses. Broadly, these include prohibitions on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms. Notably, the unfair contract term regime captures standard form contracts with consumers and small businesses that employ fewer than 100 persons or generate less than AUD 10m (in the last income year).

While the Australian Consumer Law does not apply to the supply of financial services or consumer credit, many of these protections are enforced by ASIC either through mirrored provisions in the ASIC Act or through delegated powers.

Additionally, in 2018, ASIC received a delegation of power from the ACCC, enabling it to take action where there is potential misleading and deceptive conduct associated with crypto assets.

Anti-money laundering and counter-terrorism financing laws

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) ('AML/CTF Act') applies to entities that provide 'designated services' and have a geographical link to Australia. Generally, the AML/CTF Act applies to any entity that engages in financial services, credit (ie, consumer or business) and payment activities, and the operation of digital currency exchanges. Obligations include enrolment with the Australian Transaction Reports and Analysis Centre (AUSTRAC), reporting and customer due diligence.

Relevantly to fintech businesses, on 27 June 2023 AUSTRAC issued guidance to clarify the role of financial institutions and business sectors that are increasingly being 'debanked' because they are considered high risk. Debanking refers to financial institutions restricting, rejecting or terminating banking services to customers from certain industries. Sectors that have been affected by debanking include remitters, digital currency exchanges and payment service providers. AUSTRAC's guidance is not enforceable but provides a risk-based approach for financial institutions to follow when evaluating the legitimacy of customers from 'high risk' industries to minimise debanking.

Regulatory developments

On 10 December 2024, Parliament enacted the AML/CTF Amendment Bill 2024, which became the AML/CTF Amendment Act 2024 ('Amendment Act'). The Amendment Act implements significant reforms to Australia's AML/CTF framework to bring it in line with international standards. The majority of the reforms commenced on 31 March 2026 for existing reporting entities, including digital currency exchange services, with newly captured 'Tranche 2' entities required to comply by 1 July 2026. The AML/CTF regime now extends to lawyers, accountants, trust and company service providers, real estate agents, and dealers in precious metals and stones. Detailed requirements are set out in the AML/CTF Rules 2025, which came into force on 31 March 2026. See Section 7 for further details of the reforms.

The AML/CTF Transitional Rules have also commenced and will remain in effect from 31 March 2026 to 31 March 2029. During this transitional period, reporting entities may continue to use applicable customer identification procedures instead of the new initial customer due diligence (CDD) obligations, provided that certain criteria are met. This CDD arrangement applies only to initial CDD; ongoing CDD obligations must be complied with from 31 March 2026 onwards. The Transitional Rules also provide for an extended period for notification of appointment of an AML/CTF compliance officer, staggered timeframes for initial independent evaluations, and a delayed transition to international value transfer service (IVTS) reporting.

AUSTRAC has also issued core guidance on the reforms, in October 2025, and has finalised industry-specific guidance including AML/CTF programme starter kits for Tranche 2 entities.

Banking laws and prudential regulation

The Banking Act 1959 (Cth) requires those engaged in the business of banking to be authorised by the Australian Prudential Regulatory Authority (APRA) (ie, be an 'authorised deposit-taking institution' or ADI) before engaging in such business. APRA and ASIC jointly administer the Financial Accountability Regime (FAR) under the Financial Accountability Regime Act 2023 (Cth). The FAR establishes accountability obligations for ADIs, their senior executives and directors, deferred remuneration, key personnel, and notification obligations for ADIs (among other things).

Fintech businesses that operate as holders of stored value in connection with a purchased payment facility (PPF) may be required under the PSRA to be licensed as a special class of ADI authorised by APRA. A PPF is a facility (other than cash) where the customer can make payments up to the amount available under the facility and those payments are made by the provider of the facility (or another person acting in accordance with instructions), rather than the user of the facility. Regulatory oversight of PPF providers is split between APRA, ASIC and the Reserve Bank of Australia (RBA). APRA authorises large PPF providers that offer facilities which are widely available (ie, more than 50 users), have payment obligations over AUD 10m that are payable on demand, and are redeemable in Australian currency. This may be relevant for fintech businesses that offer digital wallets as a means of payment and storing value for customers.

Regulatory developments

On 30 July 2025, APRA released a discussion paper proposing changes to the ADI licensing framework to streamline the process and better support new entrants. The proposals include introducing formalised licensing criteria, clearer expectations, and a defined 12-month timeframe for applicants to demonstrate readiness. Following that consultation, on 13 May 2026, APRA published a formal consultation on draft ADI Licensing Criteria and ADI Licensing Guidelines. Consultation will close on 31 July 2026; APRA intends to publish the final ADI Licensing Criteria and Guidelines in late 2026.

The Financial Sector Collection of Data Act 2001 (Cth)

The Financial Sector Collection of Data Act 2001 (Cth) is designed to assist APRA in the collection of information relevant to financial sector entities. Entities that engage in the provision of finance in the course of carrying on business in Australia and have assets greater than AUD 50m must register with APRA and meet ongoing reporting obligations.

The Financial Sector (Shareholdings) Act 1998 (Cth)

The Financial Sector (Shareholdings) Act 1998 (Cth) imposes an ownership limit of 20 per cent in a financial sector company without approval from the Treasurer. A financial sector company includes ADIs, certain types of insurance companies and a holding company of either of those things.

Privacy laws

The Privacy Act 1988 (Cth) ('Privacy Act') regulates the handling of personal information by government agencies and private sector organisations that have an aggregate group revenue of at least AUD 3m. In some instances, the Privacy Act will apply to businesses (ie, credit providers and credit reporting bodies) regardless of turnover. The Privacy Act includes 13 Australian Privacy Principles which impose obligations on the collection, use, disclosure, retention and destruction of personal information.

In addition, the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) contains the Notifiable Data Breaches (NDB) scheme, which requires entities regulated under the Privacy Act to notify any affected individuals and the Office of the Australian Information Commissioner (OAIC) in the event of a data breach (ie, unauthorised access to, or disclosure of, information), which is likely to result in serious harm to those individuals.

The OAIC is Australia's privacy and freedom of information regulator and is responsible for administering the Privacy Act and the NDB scheme.

Regulatory developments

On 16 February 2023, the Attorney General released a report detailing 116 proposals at a principles level on how the Privacy Act can be uplifted to best fit consumer privacy needs

(‘Privacy Report’). The principles are aimed at strengthening the protection of individual personal information and enhancing individuals’ control over their data. The government published its response to the Privacy Report on 28 September 2023 and accepted (either in whole, or in principle) all but ten of the proposals.

Following the Privacy Report, on 10 December 2024 Parliament enacted the Privacy and Other Legislation Amendment Bill 2024. This legislation implemented numerous proposals in the Privacy Report. Key reforms include:

- enhanced regulatory powers for the OAIC;
- a three-tier civil penalty system providing the OAIC with greater flexibility in enforcement;
- new infringement notice powers allowing the OAIC to issue penalties without court proceedings;
- a statutory tort enabling individuals to sue for serious invasions of privacy;
- criminal offences for doxxing (releasing personal information in a menacing or harassing manner);
- requirements for the OAIC to develop a Children’s Online Privacy Code; and
- transparency obligations requiring entities to disclose when automated systems make decisions significantly affecting individuals.

Further reform is expected before the end of 2026.

Payment system laws

Fintech businesses that provide payment services must operate in accordance with various laws that regulate the infrastructure of Australia’s payments system and may be subject to direct regulation for certain activities. See Section 3 for further information about the regulation of payment service providers.

The RBA is Australia’s central bank and provides a range of banking services to the government and its agencies, overseas central banks and official institutions. It is also responsible for maintaining the stability of the financial system through monetary policy and regulating payment systems.

Regulatory developments

On 7 June 2023 the government released its Strategic Plan for Australia’s Payment System (‘Payments Strategic Plan’) outlining the policy objectives and priorities to reform Australia’s payments system. The Payments Strategic Plan was released alongside two consultations, the first on reforming the Payment Systems (Regulation) Act 1998 (Cth) (PSRA) and the second on modernising the licensing framework for payment services providers (PSPs). Subsequent consultations and draft exposure legislation have been also released.

On 19 September 2025 Parliament enacted the Treasury Laws Amendment (Payments System Modernisation) Bill 2025. This legislation expands the regulatory perimeter of the PSRA to include buy now, pay later (BNPL) providers, digital wallets, crypto asset payment facilitators, and cash distribution services. The reforms also introduce a ministerial designation power, enabling the Treasurer to direct nationally significant platforms into enhanced oversight, and broaden the RBA's powers to address emerging risks in the payments ecosystem.

In connection with this legislation, on 29 October 2025 the government invited public feedback on exposure draft regulations under the Payment Systems Legislation Amendment (2025 Measures No 1) Regulations 2025. The draft regulations support the legislation in Schedule 1 of the Treasury Laws Amendment (Payments System Modernisation) Act 2025 to clarify the scope of ministerial designation and directions powers, prescribe 'special regulators' and their functions, as well as persons authorised to use or disclose information relating to special payments systems. The draft regulations also propose to introduce protections from civil liability offences for special regulators and other prescribed persons. Comments on the draft regulations closed on 6 November 2025.

On 12 March 2026, Treasury released the full package of Tranche 1 exposure draft legislation under the Treasury Laws Amendment Bill 2026: Payments System Modernisation (PSP Bill). The PSP Bill forms part of the Payment System Modernisation reforms, aimed at modernising the regulatory framework for payment service providers, and introduces significant reforms to the regulation of stored value facilities (SVFs), including payment stablecoin issuers and digital wallet providers. The Tranche 1 package covers payment function definitions and core concepts, licensing obligations including safeguarding payment-related money, exemptions and exclusions, a framework for unclaimed monies, APRA powers for major SVF providers and designated PSPs, a rule-making power for a mandatory revised ePayments Code, and transitional arrangements.

The PSP framework proposed under the PSP Bill replaces the concept of PPFs regulated under the PSRA with a graduated regulatory regime for SVFs under the Corporations Act. An SVF is defined as a facility that allows a person to store value by transferring funds to another person without any onward payment instruction and subsequently redeem that value by making a non-cash funds transfer. This definition is designed to capture digital wallets that store value, payment stablecoins, prepaid accounts, and virtual and physical pre-paid cards. All SVF providers will be required to hold an AFSL and comply with the relevant obligations under the Corporations Act.

Stakeholder feedback on the Tranche 1 consultation will be considered in finalising the legislation for introduction to Parliament in 2026. Tranche 2 will progress in 2026 and will consider further reform elements, including common access requirements, the establishment of an industry standard-setting body and a review and update of the ePayments Code. See Section 3 for further information about the PSP Bill.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Australia regulates crypto assets through a combination of existing legislative regimes and, following recent reforms, dedicated digital asset legislation. As noted in Section 1, on 31 March 2026, the scope of the AML/CTF regime was expanded to require all providers of virtual asset services (including exchanges, transfers, safekeeping and administration of virtual assets) to register

with AUSTRAC and comply with AML/CTF obligations, including customer due diligence and record-keeping for up to seven years.

In addition, the Corporations Amendment (Digital Assets Framework) Act 2026 ('DAF Act'), which received Royal Assent on 8 April 2026 and will commence on 9 April 2027, represents Australia's first dedicated digital asset legislation. The DAF Act introduces digital asset platforms (DAPs) and tokenised custody platforms (TCPs) as new categories of financial products under the Corporations Act. DAPs capture platforms that hold digital tokens on behalf of clients, including centralised exchanges, brokerage platforms, custody and wallet providers, and staking platforms. TCPs capture platforms that tokenise real-world assets. Operators of both DAPs and TCPs will be required to hold an AFSL, and to comply with conduct, disclosure and asset-holding obligations tailored to digital asset activities.

From a regulatory guidance perspective, ASIC has released *Information Sheet 255: Digital assets: Financial products and services* (INFO 225) which informs businesses of ASIC's views on the legal status of digital assets. This turns on how digital assets are structured and the rights attached, which ultimately determines which regulations apply.

Notably, on 29 October 2025, ASIC reissued INFO 225 with substantial updates to clarify its regulatory approach to digital assets. In particular, the updates include detailed examples of common digital asset related business models (including token issuance, staking, custody and trading platforms) and explain how ASIC interprets each model's status under the Corporations Act. The updates also clarify licensing expectations for digital asset financial service providers and affirm ASIC's view that existing law is sufficiently flexible to capture digital assets, provided the activity falls within the financial product perimeter. The updates to INFO 225 follow key decisions of Australian courts in recent cases involving crypto assets and may serve to clarify ASIC's basis for intervention in future actions.

In parallel to re-issuing INFO 225, ASIC also granted an industry-wide no action position for digital asset financial service providers that provide financial services after 29 October 2025 who lodge an application for an AFSL on or before 30 June 2026. On 25 June 2026, ASIC extended the deadline of its no action letter to 30 September 2026 and expanded the scope of the position to cover authorised representative and authorised intermediary arrangements.

In addition, ASIC *Information Sheet 230: Exchange traded products: Admission guidelines* (INFO 230) outlines ASIC's expectations of market operators for admitting and monitoring exchange-traded products (ETPs) that hold or invest in crypto assets. The guidance outlines factors that market operators should consider when assessing whether a crypto asset is suitable as an underlying investment of an ETP. This broadly requires:

- institutional support of the crypto asset;
- service providers willing to support ETPs that invest in or provide exposure to the crypto asset;
- maturity of the spot market for the crypto asset;
- regulation of derivatives linked to the crypto asset; and
- the availability of robust and transparent pricing mechanisms for the crypto asset.

INFO 230 states that Bitcoin and Ether are likely to satisfy the criteria, but market operators are expected to make their own determination.

Regulatory developments

In recent years there have been a raft of government reviews into the regulation of crypto assets which have predominately focused on the transactional relationships (eg, the issuing and exchange process) and activities involving crypto assets, rather than the crypto assets themselves. A common theme of these reviews has been the inclusion of proposals to regulate crypto assets under the established financial services regulatory framework. An overview of some of the key regulatory developments on the regulation of crypto assets include:

- On 10 December 2024, ASIC reissued *Regulatory Guide 133: Funds management and custodial services: Holding assets* (RG 133), which sets out minimum standards for custody and management of client assets. The revisions expand the scope of RG 133 to expressly capture crypto assets and include good practice guidance for crypto asset holders (such as custodians of crypto assets that are financial products), including maintaining robust information security controls and risk management processes.
- On 21 March 2025, the government released a response to the Board of Taxation's review of the tax treatment of crypto assets and transactions in Australia, confirming that existing tax laws are applicable to crypto assets and transactions, while also recognising that the Australian Tax Office (ATO) can assist in improving certainty among the crypto asset industry by issuing targeted guidance.
- On 21 March 2025, the government released its *Statement on Developing an Innovative Australian Digital Asset Industry* (Statement) outlining the government's approach to transforming regulation of the digital asset industry. The Statement aims to position Australia as a global leader in the digital asset ecosystem and sets out strategic pillars including the introduction of a DAP regime, a modernised payment licensing framework to regulate payment stablecoins as SVFs, and a review of Australia's enhanced regulatory sandbox.
- On 19 September 2025, Parliament enacted the Treasury Laws Amendment (Payments System Modernisation) Bill 2025. This legislation expands the definitions of 'payment system' and 'participant' in the PSRA to capture a broader range of service providers, including crypto asset payment facilitators.
- On 18 September 2025, ASIC granted the first-of-its-kind relief through the ASIC Corporations (Stablecoin Distribution Exemption) Instrument 2025/631 ('Instrument 2025/631'), exempting intermediaries engaging in the secondary distribution of a 'named stablecoin' from holding separate Australian financial services, Australian market, or CS facility licences. Currently, the only 'named stablecoin' covered by the instrument is AUDM, issued by Catena Digital Pty Ltd.
- On 29 October 2025, ASIC invited public feedback on a draft legislative instrument, ASIC Corporations (Amendment) Instrument 2025/XX. The draft instrument proposes amendments to ASIC Corporations (Custody Standards for Providers of Custodial and

Depository Services) Instrument 2024/17 that would extend existing relief for omnibus account structures to digital assets in certain circumstances. Comments on the draft instrument closed on 12 November 2025.

- On 9 December 2025, ASIC released ASIC Corporations (Stablecoin and Wrapped Token) Instrument 2025/867, following its announcement of proposed relief for distributors of eligible stablecoins and wrapped tokens on 29 October 2025. This finalised instrument closely mirrors the draft instrument released for consultation and grants exemptions from AFSL, market licensing, clearing and settlement licensing and disclosure requirements for specific digital assets, being eligible stablecoins and wrapped tokens.
- On 20 April 2026, ASIC released its 18-month roadmap for licensing, supervising and enforcing the new regime governing DAPs and TCPs. The roadmap provides early visibility on the topics ASIC expects to consult on and the sequence in which new standards and guidance will be developed.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The provision of payment services is regulated by ASIC, APRA, the RBA and AUSTRAC under certain regulatory regimes is set out in Section 1.

Financial services

Under the financial services regulatory regime, a facility through which (or through the acquisition of which) a person makes an NCP (ie, other than through the delivery of physical currency) is a financial product (ie, NCP facility). When delivering payment services, the provider will generally be dealing in the NCP facility and providing advice in respect of the same. Both activities constitute the provision of financial services and require the provider to hold an AFSL or rely on an exemption.

ASIC has outlined numerous AFSL exemptions from this requirement, including NCP-specific exemptions related to gift vouchers and loyalty schemes. Payment services providers often provide these financial services under licensing exemptions which apply when the services are provided on behalf of an AFSL holder.

Whether a digital wallet comprises an NCP facility will largely depend on the functionality of the wallet. A digital wallet may be a part of an NCP facility if it allows users to make payments to a number of payees or enables a payment to be initiated in a digital asset which is converted into fiat to enable completion of the payment.

Notably, the reforms proposed under the PSP Bill (see Section 1) would retire the definition of an NCP facility and recast the perimeter around the following elements:

- *Products*: the single NCP facility is replaced by two categories of financial products: SVFs (including a tokenised subset with bespoke ongoing monthly and eventbased disclosure) and payment instruments.

- *Services*: a new regulated ‘payment service’ category would cover payment initiation, payment facilitation and payment technology/enablement.
- *Conduct*: a new ‘noncash funds transfer’ concept would become the foundational concept underpinning the definitions of the various payment services and products. A payer makes a noncash funds transfer where funds standing to the payer’s credit under a facility are transferred to a payee (or between the payer’s facilities) at the instruction of the payer or payee without physical cash.

Consumer credit

On 10 December 2024, Parliament enacted the Treasury Laws Amendment (Responsible Buy Now Pay Later and Other Measures) Act 2024 (Cth), bringing BNPL products within the scope of the Credit Act, commencing from 10 June 2025. BNPL providers must hold an ACL, comply with responsible lending and other credit obligations, and maintain membership of the Australian Financial Complaints Authority.

Under the Credit Act, BNPL arrangements are generally regulated as ‘low-cost credit contracts’ (LCCCs) which have statutory fee caps that limit the amount providers can charge in fees and default charges over the life of a contract. This category recognises the lower value and shorter-term nature of most BNPL products, and applies modified responsible lending obligations and fee caps that are proportionate to the risks involved. The responsible lending framework for BNPL providers under the Credit Act also allows providers to opt into a scaled version of the obligations, provided they maintain and regularly review a written policy for assessing whether a BNPL contract is unsuitable for a consumer. This aims to balance consumer protection with the need to support innovation and access to low-risk credit products.

In addition to statutory regulation, the Australian Finance Industry Association’s voluntary BNPL Code of Practice continues to operate as an industry standard, although it is not legally enforceable. The Code is currently being updated to align with the new legislative framework and to support best practice across the sector.

Banking laws and prudential regulation

Fintech businesses that operate as holders of stored value in relation to PPFs are required to be an ADI, unless an exemption applies. A digital wallet may constitute a purchased payment facility. This is possible where the digital wallet also allows deposits of fiat currency and the provider of the facility is the holder of stored value.

As noted in Section 1, under the PSP Bill, the existing PPF framework would be replaced by a new SVF framework in the Corporations Act, administered primarily by ASIC. ASIC would regulate conduct and AFSL requirements for SVF issuers (including tokenised SVFs) and other PSPs. APRA’s prudential remit would apply only to major SVF providers and certain PSPs designated by the Minister, in addition to their AFSL requirements, under a streamlined APRA registration model. The threshold for ‘major SVF provider’ is proposed to be AUD 200m in stored value calculated by reference to funds held in relevant SVFs on an aggregate group basis, with an opt-in pathway for

smaller SVF providers. Transitional arrangements, exemptions and safeguarding requirements will be addressed in subsequent tranches of legislation and regulations.

AML/CTF

Many PSPs also provide a designated service under the AML/CTF Act through a designated remittance arrangement. A designated remittance arrangement is where an instruction is accepted for the transfer of money or property, or where money or property is made available or arranged to be made available. Property includes digital assets (but not digital currency). Payment providers that provide designated services and have a geographical link to Australia must enrol and register with AUSTRAC before providing those services and comply with various AML/CTF obligations. AML/CTF obligations include adopting and implementing a risk-based AML/CTF programme, undertaking know your client (KYC) due diligence on their customers, and complying with various reporting requirements.

As noted in Section 1, from 31 March 2026 the AML/CTF Act will also cover the exchange and transfer of digital currency.

4. Special support for fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Regulators in Australia have been generally receptive to the entrance of fintechs and technology-focused businesses. The financial services regulatory regime adopts a technology-neutral approach, whereby services will be regulated equally, irrespective of the method of delivery. However, further concessions have been made by regulators to support technology-focused startups entering the market.

Innovation hubs

ASIC and AUSTRAC have established 'innovation hubs' designed to assist fintech businesses in understanding their obligations under Australian law.

The ASIC innovation hub is designed to foster innovation that could benefit consumers by helping Australian fintech startups navigate the Australian regulatory system. The innovation hub provides tailored information and access to informal assistance intended to streamline the AFSL application process for innovative fintech startups.

AUSTRAC's Fintel Alliance has an innovation hub targeted at combating money laundering and terrorism financing, and improving the fintech sector's relationship with the government and regulators. The innovation hub also assesses the impact of emerging technologies such as blockchain and crypto assets.

Regulatory sandbox

Since 2016, ASIC has made certain legislative instruments establishing a fintech licensing exemption which allows fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or ACL by relying on the legislative instrument (referred to as the regulatory sandbox). Since September 2020, this has been further developed into an enhanced regulatory sandbox, which allows testing for a broader range of financial services and credit activities for up to two years. There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. There are restrictions on how many people can be provided with a financial product or service, and caps on the value of the financial products or services which can be provided.

In October 2024, ASIC issued *Information Sheet 248: Enhanced Regulatory Sandbox* (INFO 248). Under INFO 248, the enhanced regulatory sandbox allows for testing of a broader range of financial services and credit activities for a longer duration. There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox, and the products and services that qualify for the licensing exemption. Once a fintech business accesses the regulatory sandbox, there are restrictions on how many persons can be provided with a financial product or service and caps on the value of the financial products or services that can be provided.

On 17 December 2025, the Treasury released a consultation paper in relation to the enhanced regulatory sandbox. The consultation closed on 6 February 2026, with the final report expected to be delivered later in 2026.

Broader fintech ecosystem initiatives

ASIC has also entered into a number of cooperation agreements with overseas regulators under which there is a cross-sharing of information on fintech market trends, encouraging referrals of fintech companies and sharing insights from proofs of concepts and innovation competitions. It is also the intention of a number of these agreements to further understand the approach to regulation of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions.

Additionally, in November 2024, the government launched Project Acacia, a major joint initiative between the RBA and the Digital Finance Cooperative Research Centre. The project involves various industry participants conducting 19 real-money pilot use cases and five proof-of-concept simulations across multiple asset classes, including fixed income, private markets, trade receivables and carbon credits. The project explores how different innovations in digital money and existing settlement infrastructure might support wholesale tokenised asset markets. ASIC has provided regulatory relief to facilitate this testing.

Commonwealth Bank, JP Morgan, ASX and HQLA X were selected to participate in Project Acacia's research into domestic wholesale tokenised asset markets, specifically targeting improvements to Australia's AUD 350bn repurchasing agreement market. Westpac has partnered with Chainlink and Imperium Markets to implement blockchain-based tokenised asset settlement capabilities, with the RBA estimating that tokenisation could save asset issuers up to AUD 12bn annually in Australian capital markets.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The Consumer Data Right (CDR) under the Competition and Consumer Act gives consumers a right to require banks and other data holders to share their data with accredited service providers (including banks, comparison services, fintechs or third parties). The CDR encourages the flow of information in the economy and competition within the market and allows consumers to authorise accredited persons to initiate actions on their behalf, such as making payments, opening or closing accounts, switching providers, and updating personal details.

The Data Standards Body is responsible for making data standards, including about the format and process for transferring data, while the Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) ('CDR Rules') provide the framework for how the CDR operates, defines elements for consent, outlines the accreditation framework and elaborates on privacy aspects of the scheme. The CDR framework applies to designated sectors determined by the Minister.

The banking sector was the first sector to be designated under the open banking regime. The CDR Rules for data sharing in the banking sector came into force on 6 February 2020, and consumers were able to consent to their bank sharing data with accredited data recipients from July 2020. The open banking regime has been implemented in a phased approach, having regard to both the types of banking entities and the products they offer. Since 1 July 2022, individual Australian bank customers have been able to authorise accredited third parties to access data across a full suite of banking products, with major ADIs facilitating data sharing for business consumers, partnerships, secondary users and joint accounts. These obligations were extended to non-major ADIs from 1 November 2022.

The non-bank lending sector was designated on 21 November 2022. On 4 March 2025, amendments to the CDR Rules took effect, extending CDR operation to the non-bank lending sector. Product data sharing obligations will commence 13 July 2026, with consumer data sharing obligations commencing in staged tranches from 9 November 2026 for initial providers (defined as having resident loans and finance leases exceeding AUD 10bn and more than 10,000 customers as of 4 March 2025) and 10 May 2027 for large providers (those with resident loans and finance leases exceeding AUD 1bn and more than 1,000 customers). BNPL products are included within the data sharing obligations.

Regulatory developments

On 9 August 2024, the government announced a 'CDR reset' to address concerns about high compliance costs and focus the regime on high-value use cases. This followed the release of the Heidi Richards compliance costs review, which found CDR implementation costs had substantially exceeded original regulatory estimates. As part of the reset, the government has:

- amended the CDR Rules to implement streamlined consent processes for consumers;
- signalled intention to ban screen scraping practices where the CDR provides a viable alternative; and
- directed the Data Standards Body to prioritise high-value use cases including consumer finance and lending, small business accounting services, and energy switching.

On 17 August 2025, the Treasury Laws Amendment (Consumer Data Right) Bill 2022 commenced, which implemented the action initiation framework. This enables consumers to use the CDR framework to direct accredited third parties to perform actions on their behalf, such as making payments, opening or closing accounts, and switching providers.

6. Regulation of virtual asset service providers.

At the time of writing, there is no standalone legislative regime that regulates virtual asset service providers (VASPs) but they are captured within the same legislative regimes as crypto assets (see Section 2).

7. AML and the Travel Rule in crypto asset transactions.

The reforms to the AML/CTF regime introduced under the Amendment Act on 10 December 2024 (see Section 1) include updated Travel Rule obligations. These obligations apply to all entities that provide value transfer designated services, including virtual asset transfers, replacing the existing Electronic Funds Transfer Instruction framework. Consistent with Financial Action Task Force (FATF) Recommendations 15 and 16, the reforms expand obligations beyond financial institutions to remittance providers and VASPs, covering both domestic and cross-border transfers. Entities involved in the value transfer chain, namely ordering, intermediary and beneficiary institutions, must collect and verify payer information. While the current focus remains on payer data, AUSTRAC has been granted rule-making powers to prescribe required information once FATF finalises its review of Recommendation 16. The reforms also recognise technical limitations in legacy systems and introduce limited obligations for transfers involving self-hosted wallets, where gathering travel rule information is not technically feasible due to the decentralised nature of such transfers.

In addition, the reforms also replace the current international funds transfer instruction reporting framework with a new IVTS regime, which applies to cross-border transfers of value, including virtual assets. The reporting obligation will now lie with the reporting entity closest to the Australian customer. The IVTS regime will also apply to unverified self-hosted wallet transfers. While the IVTS framework was legislated to commence on 31 March 2026, the AML/CTF Transitional Rules delay a reporting entity's IVTS reporting transition date to either 31 March 2029, or a substitute transition date nominated by the reporting entity of no later than 30 September 2029. In the interim, the existing framework will continue to operate.

The reforms also broaden the definition of 'virtual asset' to capture a wider range of tokenised assets (eg, non-fungible tokens (NFTs), stablecoins or governance tokens) and expand the AML/CTF regime to capture additional services, including previously unregulated VASPs that provide the following 'registrable virtual asset services':

- exchanges of a virtual asset for another virtual asset;
- transfers of virtual assets on behalf of a customer;
- safekeeping or administration of virtual assets; and
- participation in and the provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Existing 'remittance' designated services have also been expanded to 'value transfer' designated services, and this now includes transfers of virtual assets.

The reforms also broaden the definition of 'virtual asset' to capture a wider range of tokenised assets (eg, NFTs, stablecoins and governance tokens) and remove the prior limitation that the asset be 'generally available to the public without restriction'. This addresses a regulatory gap created by the emergence of stablecoins minted on public blockchains, where the issuer only intends for it to be used by a subset of the public.

From 31 March 2026, businesses providing virtual asset or value transfer designated services must register with AUSTRAC (where the geographical link is met) and implement an AML/CTF programme. This includes:

- a risk-based money laundering and terrorism financing (ML/TF) assessment;
- documented AML/CTF policies (replacing the former Part A and B structure);
- customer due diligence at onboarding and on an ongoing basis;
- periodic updates to AML/CTF policies; and
- compliance with reporting and record-keeping obligations (including suspicious matter reports, threshold transaction reports, and annual compliance reports).

Businesses will also need to engage an onshore AML/CTF Compliance Officer where they provide designated services through a permanent establishment in Australia.

8. Enforcement and cross-border recognition of tokenisation and structuring of secured transactions involving crypto assets.

How are financial instruments structured in relation to tokenised assets (eg, tokenised real estate, digital bonds, DeFi instruments)?

There are no typical financial instruments or structures that have been used in Australia in relation to tokenised assets. The type of financial instrument is determinable on how its structure and arrangement fits under the existing definitions of a financial product in the financial services regime (see Section 1).

What types of collateral are typically used to secure obligations arising in such digital asset transactions?

There are no typical types of collateral that have been used to secure obligations arising in digital asset transactions.

Describe the procedures to create and perfect a security interest in these types of collateral, including any requirements for notarisation, registration, stamp duty or other legal formalities.

At the time of writing, there is no established legal or commercial position on how to effectively take security over crypto assets or tokenised assets. The Australian market uses relatively standardised forms of security documents and perfection methods, such as registration on the Personal Property Securities Register in accordance with the Personal Property Securities Act 2009 (Cth) (PPSA). However, the effectiveness of these methods for crypto assets is yet to be tested by the courts.

In addition, there are no notarisation or stamp duty issues associated with taking or registering the security.

Will the courts in your jurisdiction recognise and enforce a foreign governing law clause in a crypto asset-related contract?

Parties to a contractual arrangement generally have discretion to choose the governing law, although the courts have in rare cases overturned the governing law chosen by the parties. A court may decline to give effect to a governing law clause, or read it down, in various circumstances including where:

- the governing law is not selected at the time of contracting but left to a party to nominate at a later date;
- Australian statute is taken to apply regardless of the parties' choice of law (for example, the unfair contract terms regime for standard form consumer or small business contracts);
- the clause is unfair or oppressive, particularly in standard form arrangements or where there is significant inequality of bargaining power. This risk can arise with crypto transactions executed via smart contracts, which are typically standard form;
- there are public policy grounds that warrant refusal of enforcement or the clause is included in bad faith: for example, for the purpose of avoiding Australian law.

In the case of a default, what enforcement procedures are available to secured lenders to realise their security interest and recover their claims?

The method of enforcement will depend on the type of security and collateral in question. Australian law provides robust enforcement rights for secured creditors, subject to compliance with statutory requirements and any applicable moratoria. For example:

- *Personal property*: enforcement is governed by the PPSA and the terms of the security document allowing secured parties to seize and sell collateral, or the appointment of a controller or receiver upon default, subject to notice and procedural requirements.
- *Real property*: enforcement is governed by state and territory legislation, typically involving the exercise of a power of sale or the appointment of a receiver or mortgagee in possession.

Enforcement does not routinely require court involvement, and lenders can generally enforce security upon the occurrence of an event of default as defined in the finance/security documents.

Is a public auction required for enforcement?

This response is focused on receivership as one of the most common types of enforcement.

A receiver appointed by a secured creditor has statutory duties in connection with the conduct of the receivership and sale of secured assets. This includes the duty to take all reasonable care to sell the secured property if it has a market value, at not less than market value, or otherwise for the best price reasonably obtainable. In determining whether the duty has been discharged, the courts have confirmed that it is the process followed by the receiver, rather than the ultimate price obtained, that is relevant.

There is no 'one size fits all' approach to discharging this duty – the nature of the property being sold and the relevant industry or sector in which it sits will be relevant in informing the receiver of the process to be adopted.

While not mandatory, a public auction is often determined by a receiver as necessary to satisfy the duty.

Can a secured lender appropriate the collateral directly in certain cases?

Generally, a secured lender cannot appropriate collateral directly because it would be inconsistent with statutory and general law duties imposed on secured lenders, mortgagees in possession and their enforcing parties (such as receivers or administrators) in connection with the exercise of a power of sale.

9. Litigation and jurisdiction on crypto assets: legal implications of disputes involving crypto assets.

Where the parties to a contractual agreement have agreed to submit to a particular court's jurisdiction (a submission-to-jurisdiction clause), the aggrieved party (the plaintiff) can usually commence proceedings in that court even if the defendant is not physically present in the jurisdiction. A submission-to-jurisdiction clause also permits jurisdiction in an international sense to be exercised over the parties, with the consequence that any judgment from a court in the nominated jurisdiction will typically be enforceable in other courts under common law principles, or the provisions of the Foreign Judgments Act 1991 (Cth) (where applicable).

Where parties to a contractual agreement have agreed to submit to an 'exclusive jurisdiction' clause, the courts will exercise a strong bias in favour of maintaining the agreement of the parties. If a party initiates legal action in the courts despite a foreign exclusive jurisdiction clause, the court will usually halt the proceedings through a 'stay of proceedings' unless the party resisting the stay demonstrates reasons to depart from the clause. These reasons may include an unforeseen and material change in the procedure of the nominated court or a real risk of fragmented or duplicative litigation because key parties are not bound by the clause. However, the inconvenience of the nominated forum is not a legitimate reason against staying the proceedings if this is a foreseeable outcome of the exclusive jurisdiction clause.

10. Intellectual property and crypto assets: legal protection, ownership, enforcement, and monetisation of IP rights related to digital and virtual assets.

Crypto assets are primarily protected by copyright, which arises automatically upon creation and grants the creator the exclusive rights to use and control how others use the copyrighted material. The initial owner of copyright materials normally lies with the creator, or if they were created by employees during the course of their employment, with the employer company.

Fintech businesses can also use trademarks to protect innovation in relation to crypto assets. For example, NFTs often feature a logo and present a way for fintech businesses to increase brand awareness and engage with their customer base. Australia recognises registered and unregistered trademark rights; however, registered trademarks are significantly simpler to enforce and commercialise. To ensure that these NFTs are also protected by trademarks, fintech businesses should ensure that:

- they have sought trademark registrations for any logos they want to utilise on a crypto asset; and
- these registrations specifically cover off the virtual goods which the crypto asset represents (eg, a logo which is to be used on virtual clothing should be registered in class 9 for 'virtual clothing').

Patent protection may also be sought for certain crypto asset and blockchain related innovations. However, the software patents are a complex area of law in Australia, and there are still many uncertainties on whether computer-implemented inventions are eligible for patent protections. While Australian law has generally been very reluctant to recognise computer-implemented inventions as patentable subject matter, the Full Federal Court decision in *Aristocrat Technologies Australia Pty Ltd v Commissioner of Patents* [2025] FCAFC 131 adopted a more 'permissive' approach which aligns more closely with other major jurisdictions like the United States and Europe. On 5 February 2026, the High Court of Australia denied the Commissioner of Patents' application for special leave to appeal, confirming that the Full Court 'applied established principles concerning the assessment of manner of manufacture and reached a unanimous and clear conclusion as to characterisation'.

As registered IP rights are jurisdiction-bound (eg, an Australian patent only confers exclusive protections in Australia), companies with an international customer base may want to seek IP registration in multiple different countries. However, it should be noted that applying for IP registration in other countries can be an administratively complex and expensive process. As a result, we recommend companies apply to have their patents registered only in the countries in which they intend to conduct business.

Companies looking to have multi-jurisdictional patent coverage for an invention but are unsure at the early stage which particular countries to target may find it helpful to file a patent under the Patent Cooperation Treaty (PCT), which is administered by the World Intellectual Property Organisation (WIPO). When an applicant files directly with a national office, they only have 12 months after the initial filing to choose which other countries to seek patent protections in. However, this limited timeframe is often not enough for companies to build up regional investor interest and identify their key markets. In contrast, the PCT system allows applicants to initially file a single 'global' patent application instead of having to file several applications in multiple

different countries (and incur all the associated filing costs), including ones where commercial potential is still uncertain. PCT applicants will receive a written opinion about their application, which can help companies decide whether it is worthwhile to financially commit to filing patents in multiple different countries. Applicants will only need to decide which countries to 'convert' their PCT applications into after two and a half years, by which time they will likely have a clearer understanding of both the patentability of their invention and also where their key markets are. As noted above, jurisdictions like the US and the European Union are more receptive to granting software patents than in Australia. This may also be a consideration when deciding which country to file a patent application in.

The transfer of crypto assets between parties on the market plays an important role in their monetisation and involves several IP considerations. It is important to understand what is actually being transferred when a crypto asset is bought and sold. In terms of IP, crypto assets such as NFTs comprise two layers of ownership which can be transferred. The first layer is the NFT itself, being the unique metadata about the underlying asset which is stored on a blockchain. This layer is normally transferred when an NFT is bought and sold. The second layer is the IP subsisting in the underlying asset (ie, the digital artwork) which is linked to or represented by the NFT. For the most part, acquiring an NFT does not assign to the buyer the copyright in the underlying asset. For example, purchasing an NFT for a digital artwork does not give the buyer the right to print the artwork on t-shirts and begin selling them. Even if a smart contract for an NFT purports to transfer the underlying IP, it is unlikely to comply with requirements applicable to an assignment under the Australian Copyright Act 1968 (Cth). Where the intent is to transfer or license the underlying IP represented by an NFT, the parties should enter an IP agreement that defines the usage rights granted to the buyer of the underlying asset.



the global voice of
the legal profession®

International Bar Association

Chancery House
53-64 Chancery Lane
London WC2A 1QS
United Kingdom
Tel: +44 (0)20 7842 0090
Fax: +44 (0)20 7842 0091
Email: editor@int-bar.org
www.ibanet.org