

New Zealand

Zac Kedgley-Foot*

Bell Gully, Wellington

zac.kedgley-foot@bellgully.com

Campbell Pentney[†]

Bell Gully, Auckland

campbell.pentney@bellgully.com

Richard Massey[‡]

Bell Gully, Auckland

richard.massey@bellgully.com

Alix Boberg[§]

Bell Gully, Wellington

alix.boberg@bellgully.com

Emma Fountaine**

Bell Gully, Wellington

emma.fountaine@bellgully.com

Isobel Ryan^{††}

Bell Gully, Wellington

isobel.ryan@bellgully.com

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

In New Zealand, the regulatory regime that applies to financial services generally does not distinguish between fintech and other financial services, with the same regulatory concepts applying across the board. In addition to registration and licensing requirements for certain financial service providers, the regulatory regime includes securities, consumer credit and responsible lending laws, market conduct, privacy and data protection, anti-money laundering rules, and other prudential regulations for banks, non-bank deposit takers and insurers.

Financial services and products regulation

The Financial Markets Conduct Act 2013 (FMC Act) is the principal legislation in New Zealand that regulates the provision of financial services and products (defined at the end of this section). It contains various regimes that apply to offers of financial products, and the provision of financial services, in New Zealand. The most relevant regimes for fintech are as follows.

Fair dealing in relation to financial products and financial services

The 'fair dealing' provisions set out in Part 2 of the FMC Act prescribe standards for dealing in financial products and the supply (or possible supply) of financial services, and impose civil liability on anyone who engages in misleading or deceptive conduct in relation to financial products and financial services, which would include a person making misleading or deceptive statements in any offering or marketing material.

Sections 19 to 23 of the FMC Act provide for fair dealing in relation to financial products and financial services (including financial advice, client money or property services and discretionary investment management services (see below)) by prohibiting misleading or deceptive conduct, and false, misleading or unsubstantiated representations.

The fair dealing provisions in the FMC Act apply to conduct outside New Zealand by a person carrying on business in New Zealand to the extent that conduct relates to the supply of a financial service that occurs in New Zealand.

-
- * Zac is a partner and specialist banking and finance lawyer, who is experienced in advising on a broad range of banking, debt capital markets and derivatives transactions and financial services regulation.
 - † Campbell is a special counsel who specialises in indirect taxes such as GST and custom duties as well as emerging technologies, including blockchain and cryptocurrency.
 - ‡ Richard is a partner who delivers strategic advice across a range of sectors, with a focus on consumer law, e-commerce, and emerging legal and regulatory requirements.
 - § Alix is a partner specialising in regulatory investigations and commercial litigation, particularly focussing on financial regulation, corporate crime, contract and consumer law and class actions.
 - ** Emma is a lawyer who specialises in banking and finance law and financial services regulation. She advises on domestic and international banking and capital markets transactions and the regulation of financial products, services and markets in New Zealand.
 - †† Isobel is a lawyer who specialises in corporate and commercial litigation, with a particular focus on company, shareholder and cross-border disputes.

Regulated offers of financial products

Regulated offers of financial products to persons in New Zealand must comply with certain disclosure, registration and other requirements set out in the FMC Act. A regulated offer means an offer of financial products to one or more investors where at least one of those investors requires disclosure under the FMC Act (ie, at least one investor is not a wholesale investor, and the offer does not fall within an exemption that applies to the offer as a whole due to its nature or the nature of the issuer).

The principal disclosure obligations that apply to regulated offers of financial products are to:

- prepare a product disclosure statement (PDS) for the offer;
- lodge the PDS with the Registrar of Financial Service Providers; and
- supply to the Registrar of Financial Service Providers all the information that the register entry (if any) is required to contain.

The PDS and the register entry must include all material information about the offer of a financial product and be up-to-date, accurate and understandable. The FMC Act also contains restrictions on advertising a regulated offer (including an intended offer) of financial products.

In addition to the disclosure requirements, a person making a regulated offer of debt securities or managed investment product must comply with various governance and registration requirements (including a requirement to have a trust deed/governing document that complies with the FMC Act and to appoint a licensed supervisor).

Licensing of market services and financial product markets

The FMC Act imposes specific registration, licensing, disclosure and conduct obligations on providers of the certain financial services, which include the following:

FINANCIAL ADVICE

In order to give regulated financial advice (ie, financial advice that is given in the ordinary course of a business and does not fall within a number of specific exceptions) to clients, a person must obtain a financial advice provider (FAP) licence or operate under another FAP's licence. FAP licences are subject to specific conditions. In addition, the financial advice regime imposes certain conduct and disclosure obligations on FAPs, which include duties relating to prioritising clients' interests, exercising care, diligence and skill, complying with the applicable code of conduct, and not recommending the acquisition of financial products that contravene the financial advice regime. The financial advice regime in New Zealand extends to robo-advice.

FINANCIAL PRODUCT MARKETS

The FMC Act requires that, subject to certain exemptions, a person must not operate a financial product market in New Zealand unless the person has a licence to do so. A financial product market is a facility where financial products are bought or sold, or where offers or invitations to buy or sell financial products are made, and a financial product market is taken to be operated in New Zealand in a number of circumstances including if it is promoted to investors in New Zealand by or on behalf of the operator.

Obtaining a financial product market licence is time-consuming and expensive as the licence can only be issued by the responsible minister on advice of the regulator. Among other conditions and obligations, a licensed financial product market must be operated under market rules that are approved under, and comply with, the FMC Act.

P2P LENDING OR CROWDFUNDING INTERMEDIARIES

There is no requirement for a peer-to-peer (P2P) lending or crowdfunding service to be licensed; however, providers may choose to apply for a licence because there are less onerous disclosure requirements for borrowers that offer debt securities through a licensed P2P lending service or companies who want to offer shares through a licensed crowdfunding service (in particular, not being required to supply a PDS).

In order to obtain a licence, the applicant must demonstrate that it meets certain eligibility criteria set out in the FMC Act and the corresponding regulations, including that it has fair, orderly, and transparent systems and procedures for providing the service; it has an adequate fair dealing policy; and it has adequate systems and procedures for ensuring that each issuer does not raise more than NZD 2m in any 12-month period under the service. A licensed P2P lending or crowdfunding service must comply with certain disclosure and conduct obligations (eg, supply a disclosure statement (different to a PDS), provide prescribed transaction information to the investor and enter into a client agreement with the investor before the investor applies for or acquires any financial products under the service), with the standard conditions (eg, in relation to outsourcing and governance arrangements) and any specific conditions imposed by the regulator when issuing the licence.

DERIVATIVES ISSUER

Under the FMC Act, a person acting as a derivatives issuer (ie, a person that is in the business of entering into derivatives) in respect of a regulated offer of derivatives (see the paragraph titled 'Regulated offers of financial products' above) that is made by the derivatives issuer must be licensed. Licensed derivatives issuers have a variety of compliance obligations, including complying with various client fund and client agreement rules, record-keeping requirements and reporting obligations. In addition, a licensed derivatives issuer must ensure compliance with the conditions attached to its derivatives issuer licence, which include restrictions on outsourcing arrangements, financial resource requirements and minimum standards on governance arrangements.

DISCRETIONARY INVESTMENT MANAGEMENT SERVICE

Licensing obligations apply to persons who are in the business of providing a 'discretionary investment management service' (DIMS) to retail clients. This includes arrangements where the provider decides which financial products to acquire, or dispose of, on behalf of an investor and in doing so, is acting under an authority to manage some or all of the investor's holdings of financial products (ie, a separately managed account).

Licensed DIMS providers must comply with certain conduct and DIMS-specific disclosure obligations, including to ensure that a disclosure statement is provided to each investor before an investment authority is granted, enter into a written client agreement for the DIMS, ensure clients' money and property is held by an independent custodian, and comply with certain record-keeping and reporting obligations.

In the case of some of the above market services, a licence will not be required to offer that service to wholesale investors only. For example, to provide financial advice to wholesale clients only, a licence is not required but certain duties will still apply. These include the duty to give priority to your client's interests when there is a conflict, and the duty to exercise care, diligence and skill when giving advice.

Client money or property services

A provider of a client money or property service is subject to disclosure and conduct obligations under the FMC Act and the corresponding regulations (ie, regulated), unless a limited set of exclusions applies, such as in relation to a provider that is the operator of a designated settlement system or a derivatives issuer. A client money or property service is the receipt of client money or client property by a person and the holding, payment, or transfer of that client money or client property and includes a custodial service.

A regulated client money or property service provider is, among other requirements, subject to the following disclosure, conduct and handling obligations:

- to hold or ensure that client money or client property is held on trust for the client; and
- to ensure that the client money and client property are held separate from money or property held by or for the provider on its own account.

A provider who provides a custodial service that is a regulated client money or property service, and that relates to a financial product (subject to a number of exemptions) (ie, a custodian), has additional obligations imposed by regulations. Under these regulations, custodians have reporting, reconciliations, assurance engagement and general conduct obligations among others.

If a provider of regulated client money or property services only deals with certain categories of wholesale clients, it will not be subject to the disclosure and handling obligations that apply to providers under the FMC Act and the corresponding regulations but will be required to comply with certain high-level conduct obligations in the FMC Act.

Relevant definitions

The following definitions are relevant to the above summary of regulatory regimes under the FMC Act.

FINANCIAL SERVICES

The definition of financial services is broad, and several of the services that are captured under the definition will be relevant for fintech, including:

- providing market services (see the paragraph titled 'Licensing of market services and financial product markets' above);
- providing a regulated client money or property service (including a custodial service);
- keeping, investing, administering, or managing money, securities or investment portfolios on behalf of other persons;
- being a creditor under a credit contract;
- acting as an offeror of financial products offered in certain circumstances;
- operating a money or value transfer service;
- issuing or managing the means of payment (including electronic money);
- changing foreign currency; and
- trading financial products or foreign exchange on behalf of other persons.

FINANCIAL PRODUCTS

Financial products under the FMC Act are of four types (with each type, in turn, having its own definition): debt securities, equity securities, managed investment products and derivatives. In addition, the regulator has a 'call-in' power under the FMC Act. The regulator may declare that a security (the definition of which is wider than the definition of financial product and which could, for example, include a fintech product that would not otherwise be a financial product) is a financial product of a particular kind. Before making such a declaration, the regulator is required to consult with those who would be substantially affected, and a declaration cannot be retrospective.

Registration of financial service providers

The Financial Service Providers (Registration and Dispute Resolution) Act 2008 (FSP Act) applies to persons who are in the business of providing a financial service (see the definition titled 'Financial services' above) in New Zealand. The FSP Act requires financial service providers to register on an online register for each financial service they provide. In addition, if a person provides a financial

service to a client that is not a wholesale client under the FSP Act, they may also be required to become a member of an approved dispute resolution scheme.

However, a financial service provider will not be required to comply with the FSP Act if it meets certain requirements, including that it does not have a place of business in New Zealand and does not provide the relevant financial service to clients that are not wholesale clients under the FSP Act in New Zealand.

Privacy and data protection

The Privacy Act 2020 (Privacy Act) is New Zealand's primary privacy and data protection legislation. The Privacy Act does not distinguish between fintech businesses or other agencies, but rather applies to any business in New Zealand, and overseas business carrying on business in New Zealand, in relation to the collection, storage, use and disclosure of personal information relating to an identifiable individual.

The Act sets out 13 'information privacy principles' (IPPs). These include, for example, that an agency should take reasonable steps to inform the individual of various specified matters (including that personal information is being collected and the purposes for which the information will be used) before the information is collected or as soon as practicable thereafter (IPP3). In practice, this requirement is usually met by covering these items in a privacy policy. The principles also restrict disclosure of personal information and include specific restrictions for cross-border disclosure (although that is permissible in limited circumstances including where the disclosing agency believes on reasonable grounds that the recipient is: 'subject to privacy laws that, overall, provide comparable safeguards' to those under the Privacy Act or is required to protect the information in a way that, overall, provides comparable safeguards to those under the Privacy Act, such as under a data processing agreement).

The Privacy Act repealed and replaced its predecessor (the Privacy Act 1993) on 1 December 2020. The new Privacy Act is intended to reflect changes in technology and the ways in which personal information is collected, stored and shared. One of the key changes was the introduction of mandatory reporting of 'notifiable privacy breaches' to the Officer of the Privacy Commissioner and affected individuals. For that purpose, a 'privacy breach' is defined broadly and can comprise:

- unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of personal information; or
- an action that prevents an agency from accessing personal information on either a temporary or permanent basis.

A privacy breach is 'notifiable' if it is reasonable to believe it has caused serious harm to an affected individual or is likely to do so. Whether harm is 'serious harm' depends on the circumstances of the privacy breach and requires an assessment on a breach-by-breach basis, taking into account specific factors set out in the Privacy Act.

A new IPP (IPP 3A) came into force from 1 May 2026, imposing new notification obligations for organisations who collect personal information indirectly (ie, other than from the relevant individual). The disclosure is similar to IPP3, noted above, but applies specifically for indirect collection. Certain

exceptions apply, including where the individual concerned has previously been made aware of the relevant information by a third party (eg, an intermediary agency).

On 21 July 2025, the Office of the Privacy Commissioner issued the Biometric Processing Privacy Code 2025, which came into effect from 3 November 2025 for any biometric processing activities that commence after that date. The Code specifically regulates comparison, analysis or other types of processing of 'biometric information' (including for example, facial scans or fingerprints) by a technological system.

Consumer credit and responsible lending laws

The Credit Contracts and Consumer Finance Act 2003 (CCCFA) contains New Zealand's credit contracts legislation.

It imposes a range of obligations on lenders in respect of consumer credit contracts (ie, loans provided to individuals for personal, domestic or household purposes). Those obligations include requirements to comply with responsible lending conduct obligations and specific disclosure requirements. Certain provisions of the CCCFA, which address oppressive credit contracts and repossession rights, also apply to all credit contracts (ie, both business and consumer loans).

In December 2019, the CCCFA was amended to address a number of perceived issues in the credit market, with a particular focus on addressing harm to vulnerable consumers. The amendments included expanded requirements to carry out 'responsible lending', including:

- more prescriptive requirements regarding how and when affordability and suitability tests must be conducted; and
- introduction of a new certification, and fit and proper person requirement for lenders, their directors and senior managers.

The amendments were implemented in stages, with the final amendments taking effect from December 2021. Following criticism of the extensive reach of the new obligations, a series of targeted amendments were implemented to partially reduce the compliance burden on lenders.

Further changes have been introduced under the current coalition government (including the repeal of the affordability regulations). In addition, the government has confirmed changes to the treatment of buy now, pay later (BNPL). BNPL products were previously not treated as consumer credit contracts for the purposes of the CCCFA (because they do not charge interest or credit fees, nor take security). From 2 September 2024, new regulations took effect to make BNPL products subject to certain targeted aspects of the CCCFA. As a result, BNPL providers must comply with various CCCFA obligations, including:

- ensuring that default fees are 'reasonable' (ie, that they are calculated based on the actual cost of defaults);
- assisting borrowers to make informed decisions and treating them reasonably and ethically; and
- providing relief to borrowers who face 'unforeseen hardship'.

Some of the CCCFA obligations were modified under the regulations to suit the BNPL context. In particular, BNPL providers do not have to carry out any affordability assessments (provided they comply with certain credit reporting and disclosure requirements).

The government has recently announced further reforms to the CCCFA intended to further streamline compliance for consumer credit providers. The amendment bill proposes various amendments, including making retrospective changes to deal more leniently with disclosure breaches, transitioning lenders from certification to the broader financial services licensing regime, and removing the due diligence duty for directors and senior managers. The bill will also transfer regulatory responsibility for credit contracts and consumer finance from the Commerce Commission to the Financial Markets Authority.

Anti-money laundering and countering financing of terrorism

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) imposes obligations on reporting entities. A reporting entity includes a financial institution. The term 'financial institution' is broadly defined in the AML/CFT Act and captures several of the services covered by the definition of financial services (see the definition titled 'Financial services' above).

The AML/CFT Act is silent on whether it applies to reporting entities constituted (or otherwise located) outside New Zealand. However, the AML/CFT supervisors have issued a guidance note (Guidance Note) on the territorial scope. The Guidance Note states that the definition of reporting entity in the AML/CFT Act implies a place of business in New Zealand from where the activity is directed which is likely to include New Zealand staff and infrastructure. Activities may also be carried on in New Zealand where there is active, direct marketing to New Zealand customers. Therefore, an overseas person carrying on business in New Zealand and engaged in one or more of the activities listed in the AML/CFT Act in New Zealand will be a reporting entity under the AML/CFT Act, whereas an overseas person that is not carrying on business in New Zealand is unlikely to be a reporting entity under the AML/CFT Act.

Among other requirements, a reporting entity must establish, implement and maintain a compliance programme that complies with the requirements in the AML/CFT Act, is based on a risk assessment and includes internal procedures, policies and controls to detect money laundering and the financing of terrorism, and manages and mitigates the risk of money laundering and financing of terrorism.

Overseas companies

The Companies Act 1993 requires an overseas company that commences to carry on business in New Zealand to register under Part 18 of the Companies Act within ten days of doing so. An overseas company is a body corporate that is incorporated outside New Zealand.

The application of the carrying on business rules to an overseas company that does not have an office or other physical presence in New Zealand is uncertain. However, relatively minimal activity can constitute carrying on business. It is an aggregate assessment that takes into account all of the relevant overseas company's activities in New Zealand.

Fair trading legislation

The Fair Trading Act 1986 (FTA) regulates conduct by persons in trade in New Zealand. Subject to a limited 'in-trade exemption', it is not possible to contract out of the FTA.

The FTA sets out a series of 'unfair conduct' prohibitions. The most important prohibition provides that 'no person shall, in trade, engage in conduct that is misleading or deceptive or is likely to mislead or deceive'. In addition, under the FTA, the making of unsubstantiated representations or false or misleading representations in connection with the supply, or possible supply, of goods or services is also prohibited. These prohibitions are similar to the fair dealing prohibitions in relation to financial products and financial services outlined in the paragraph titled 'Fair dealing in relation to financial products and financial services' above.

The FTA also contains a prohibition on including or enforcing any term in a standard form consumer contract or standard form small trade contract that the court has declared to be an 'unfair contract term'. The FTA sets out a so-called 'grey list' of terms that may be unfair in such a contract.

In 2022, a new prohibition on unconscionable conduct was introduced. Unconscionable conduct is not defined in the FTA; therefore, it is left to the courts to determine what type of conduct will be unconscionable. This prohibition applies whether or not: (1) there is a system or pattern of unconscionable conduct; (2) a particular individual is identified as disadvantaged; or likely to be disadvantaged, by the conduct; or (3) a contract is entered into. In addition, it cannot be contracted out of.

Unsolicited electronic messages

The Unsolicited Electronic Messages Act 2007 (UEMA) regulates the sending of commercial electronic messages with a 'New Zealand link'. Under the UEMA, a person must not send, or cause to be sent, a commercial electronic message (such as an email, text, or instant message) with a New Zealand link without consent from the recipient.

The UEMA requires that all commercial electronic messages with a New Zealand link must include accurate sender information and a functional unsubscribe function (ie, a clear and operational 'opt-out' feature).

Prudential regulation

New Zealand has prudential regulatory regimes that apply to banks, non-bank deposit takers (NBDTs) and insurance companies. The New Zealand Reserve Bank has regulatory, licensing and supervisory oversight of finance companies, insurers, building societies and credit unions, and it operates New Zealand's wholesale payment and settlement systems.

NBDTs are entities that offer debt securities to the New Zealand public and are in the business of borrowing and lending money, or providing financial services, or both. This includes finance companies, credit unions and building societies, and can include entities offering certain types of fintech services (see, for example, the paragraph titled 'Platforms that provide fiat currency wallet or lending/deposit services' in Section 2), but excludes registered banks.

A major reform of New Zealand's regulatory regime in relation to banks and NBDTs is currently underway with the Deposit Takers Act 2023 (DTA) having received Royal Assent on 6 July 2023. The DTA will come into force on a staggered basis, with the initial focus being on the implementation of the 'depositor compensation scheme' which came into force on 1 July 2025. It is expected that the DTA will fully come into force in 2028, establishing the new regime in respect of deposit takers, after a multi-year work programme to develop policy, standards and regulations to support the commencement of the new regime.

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

Aside from taxation and certain AML/CFT regulations (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Section 1), there are no specific regulatory regimes that apply to crypto assets (eg, Bitcoin or USDC) and crypto services (eg, cryptocurrency trading and crypto lending/deposit programs) in New Zealand. However, the provision of crypto assets and crypto services in New Zealand may be regulated under regulatory regimes of general application.

Regulatory regimes applicable to crypto assets

A determination of the regulatory regimes that apply to crypto assets and providers of crypto services requires analysis of the particular crypto assets and crypto services being provided. Below is a high-level indication of the regulatory regimes that may apply to providers of crypto assets and/or crypto services (with a focus on cryptocurrency exchange providers).

Registration requirement for crypto asset platforms

A crypto asset or crypto service provider is required to be registered on the Financial Service Providers Register for any financial services (see the definition titled 'Financial services' under Section 1) that it provides. This may include, in relation to a cryptocurrency exchange provider, the following financial service categories:

- operating a money or value transfer service;
- keeping, investing, administering, or managing money, securities, or investment portfolios on behalf of other persons;
- operating a financial product market; and/or
- providing a regulated client money or property service.

The provider may also be required to join an approved dispute resolution scheme and comply with certain ongoing obligations (see the paragraph titled 'Registration of financial service providers' under Section 1).

Fair dealing in relation to financial products and financial services

A crypto assets or crypto service provider may also be subject to the fair dealing regulatory regime outlined in the paragraph titled 'Fair dealing in relation to financial products and financial services' under Section 1, which prescribes standards for dealing in financial products and the supply (or possible supply) of financial services.

If the fair dealing regulatory regime does not apply, the provider may nevertheless be required to comply with the FTA regulatory regime outlined in the paragraph titled 'Fair Trading Legislation' under Section 1.

Platforms that facilitate trading crypto assets that are financial products

A crypto assets or crypto service provider may also be subject to the requirement to be licensed to operate a financial product market (see the paragraph titled 'Financial product market' under Section 1) if one or more of the crypto assets traded on the platform are a financial product under the FMC Act.

The correct FMC Act classification of a particular crypto asset (ie, whether it will constitute a financial product) requires an analysis of the specific features of that crypto asset. By way of example, while we consider that prominent cryptocurrencies such as Bitcoin and Ether do not constitute a financial product under the FMC Act, certain stablecoins (for example, USDC) will likely constitute a financial product.

Platforms that provide fiat currency wallet or lending/deposit services

If the provider offers a fiat currency wallet account or a lending/deposit service (whereby the client provides fiat currency to the platform in exchange for, for example, interest) to clients in New Zealand that essentially operates as a deposit account (and so the funds in that account may not necessarily be used immediately to convert into cryptocurrency) and those funds are at any point not held in a separate trust account maintained with a registered bank, then this could be considered a debt security (and, therefore, a financial product) and attract a considerable regulatory burden (see the paragraph titled 'Regulated offers of financial products' under Section 1).

The provision of a fiat currency wallet account or a lending/deposit service may also trigger the application of the regulated client money or property service regulatory regime if the provider of the crypto service holds, pays, or transfers client money or client property in connection with crypto assets that are financial products (see the paragraph titled 'Client money or property services' under Section 1).

If a fiat currency wallet account or a lending/deposit service is a debt security, this could result in the provider being subject to the complex NBDT regulatory regime (see the paragraph titled 'Prudential regulation' under Section 1).

A lending and deposit service in relation to crypto assets (whereby the client provides crypto assets to the provider in exchange for, for example, interest paid in the form of crypto assets) may also

constitute a financial product, requiring the provider to comply with the onerous disclosure and governance rules in the FMC Act (see the paragraph titled 'Regulated offers of financial products' under Section 1).

Registration as an overseas company

The requirement to be registered as an overseas company in New Zealand (including a number of continuing obligations) under the Companies Act 1993 would apply to providers offering crypto assets or services that are carrying on business in New Zealand (see the paragraph titled 'Overseas companies' under Section 1). Registration as an overseas company would also invoke the application of New Zealand's anti-money laundering regime (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Section 1).

Taxation of crypto assets

Until recently there was no specific New Zealand tax legislation dedicated to crypto assets. Therefore, the general tax provisions prevailed and crypto assets are treated as property under New Zealand law so the usual tax rules for property sales applied. While New Zealand does not have a capital gains tax, income tax is payable on any profits derived from the disposal of property that was acquired for the purpose of resale. The Inland Revenue Department's general view is that crypto assets such as Bitcoin will generally be presumed to be acquired for resale, meaning they are treated the same as gold bullion. It is possible that some other crypto assets may be treated as acquired for some other purpose (such as staking income) and therefore the proceeds of sale would not be taxed.

Recently, the New Zealand tax laws were updated to provide for two changes specific to crypto assets:

- the New Zealand GST legislation was updated to confirm that crypto assets are not subject to GST when sold. However, this does not extend to non-fungible tokens (NFTs) which are still potentially subject to GST;
- the income tax legislation was amended so that crypto assets are generally exempt from the financial arrangement rules. These rules are intended to apply to financial instruments such as certain bonds so interest income payable on redemption is instead taxed gradually over the period of the investment.

Inland Revenue has also provided its interpretation of the tax treatment of forks and airdrops, along with employee remuneration paid in crypto assets. Further developments to clarify the tax treatment of more advanced crypto asset transactions, such as decentralised lending, has been expected for some time but there has been very little development on this front. We are not aware of any upcoming changes that would impact the taxation treatment of crypto assets at this stage.

Regulatory developments

There are currently no laws specifically aimed at regulating providers of crypto assets or related products and services (with the exception of those detailed in the answer to Section 7 below). However:

- legislators are considering taxation aspects of crypto assets;
- some major reforms of the AML/CFT Act have already been implemented and further reforms are expected to follow (see also Section 7);
- the Reserve Bank of New Zealand is consulting on the future of money, with potential plans for a New Zealand-issued central bank digital currency; and
- following a Parliamentary inquiry established in July 2021 to consider ‘the current and future nature, impact and risks of cryptocurrencies’, a select committee of the New Zealand Parliament has released a report with 22 recommendations for the New Zealand Government, including recommendations to bring certain digital assets within the ambit of the regulated client money or property service and the regulated financial advice regimes (see the paragraphs titled ‘Client money or property services’ and ‘Financial advice’ under Section 1). However, the report did not recommend a bespoke regulatory regime to be adopted in New Zealand for digital assets.

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

Like the position in relation to crypto assets and crypto services, there are no specific regulatory regimes that apply to fintech payment service providers (eg, electronic money) and/or digital wallets. We summarise the potentially applicable regimes below:

- Part 18 of the Companies Act 1993, which requires the registration of overseas companies carrying on business in New Zealand (see the paragraph titled ‘Overseas companies’ under Section 1) and the AML/CFT Act, if the provider is carrying on business in New Zealand/ required to register as an overseas company (see the paragraph titled ‘Anti-money laundering and countering financing of terrorism’ under Section 1).
- The FSP Act, which requires persons in the business of providing a financial service (see the definition titled ‘Financial services’ under Section 1) to register under that Act and, in certain circumstances, to join an approved dispute resolution scheme (see the paragraph titled ‘Registration of financial service providers’ under Section 1).
- The provisions of the FMC Act and the corresponding regulations that apply to regulated offers of financial products in New Zealand. Similarly to the position outlined above in relation to fiat currency wallets offered in connection with crypto assets, onerous disclosure and governance obligations arise where the payment or digital wallet services offered by a provider constitute a regulated offer of debt securities (see the paragraphs titled ‘Regulated offers of financial products’ under Section 1 and ‘Platforms that provide fiat currency wallet or lending/deposit services’ under Section 2).

- Certain laws of more general application that would apply – dealing with issues such as unsolicited emails, privacy, and fair dealing (see, for example, the paragraphs titled ‘Privacy and data protection’, ‘Fair trading legislation’ and ‘Unsolicited electronic messages’ under Section 1).

In May 2022, the Retail Payment System Act was passed into law. It introduced a new regulatory regime that governs New Zealand’s retail payments system and entities involved in the retail payments system (such as banks, merchants, non-bank merchant acquirers and card schemes).

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.

There are no government-led innovation hubs or accelerators specific to fintech. In addition, the relevant regulators in New Zealand have taken the view that New Zealand’s legislation is sufficiently flexible, along with the principled approach of regulators, that no specific sandbox is needed.

However, there are a number of initiatives that can provide support to fintech businesses. For example:

- there is an R&D tax incentive that is delivered jointly by Callaghan Innovation and the Inland Revenue Department and offers a 15 per cent tax credit on eligible research and development (R&D) expenditure; and
- Callaghan Innovation is a government innovation agency that also provides a range of innovation and R&D services, including assisting with technology and product development, experts and R&D funding.

We note for completeness that Callaghan Innovation is currently being disestablished and will cease operations at some point in 2026, with most of its products and services being transferred to the Ministry of Business, Innovation and Employment, alongside other public government agencies. However, the R&D tax incentive remains available as that is administered through the Inland Revenue Department.

There are also various private sector initiatives promoting fintech. For example, the New Zealand Financial Innovation and Technology Association (FinTechNZ) is an industry working group that is funded by members from the following sectors: financial services providers, technology innovators, investor groups, government regulators and financial educators. The purpose of FinTechNZ is to contribute to the prosperity of New Zealand through technology innovation.

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

On 29 March 2025, the Customer and Product Data Act 2025 (CPD Act) was enacted, setting out significant new rights for consumers and small businesses to control access to their data (known as the Consumer Data Right or CDR).

In brief, the CDR is intended to create a statutory right for consumers and small businesses to require entities holding their data such as banks ('data holders') to share that information with accredited third-party services such as product comparison websites ('accredited requestors'). Customers can also require that data holders carry out certain 'designated actions'.

The first designated sector is the banking sector which will be required to comply with the CDR, and various regulations and standards under the CPD Act, by 1 December 2025. This is intended in part to facilitate the provision of third-party services to banking customers, including budgeting tools, comparison services, and customised financial insights. It will be extended to other sectors in due course, with the electricity sector likely to be the second designated industry.

Significantly, the CPD Act enables 'action initiation' – allowing authorised third parties to make decisions on behalf of customers. For example, fintechs could be authorised to initiate customer payments, or change a customer's online profile, with the customer's prior consent. For now, based on the designation regulations, action initiation will be limited to single-person payments via New Zealand's BECS system in NZD, below specified limits, from accounts with existing electronic payment capabilities.

The CPD Act applies to information about 'customers' (whether an individual or a business), such as their account information, and also to 'product data', that is, information about the goods or services offered by the data holder. 'Consumer data' includes personal information within the meaning of the Privacy Act.

To enable the sharing of data under the regime, data holders within a designated sector will be required to make data available in a standardised, machine-readable format via application programming interfaces (APIs). Data holders will be required to follow various technical standards specified in regulations. Accredited requestors will need to be formally accredited and will be required to meet various criteria for the purposes of accreditation, including detailed security requirements.

6. Regulation of virtual asset service providers.

Like the position in relation to crypto assets, crypto services and fintech payment service providers, there are no specific regulatory regimes that apply to virtual asset service providers (VASPs). We summarise the potentially applicable regimes below:

- Part 18 of the Companies Act 1993, which requires the registration of overseas companies carrying on business in New Zealand (see the paragraph titled 'Overseas companies' under Section 1) and the AML/CFT Act, if the VASP is carrying on business in New Zealand/required to register as an overseas company (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Section 1, and 'Anti-Money Laundering (AML) and the Travel Rule in Crypto Asset Transaction' under Section 7).
- The FSP Act, which requires persons in the business of providing a financial service (see the definition titled 'Financial services' under Section 1) to register under that Act and, in certain circumstances, to join an approved dispute resolution scheme (see the paragraph titled 'Registration of financial service providers' under Section 1).

- The provisions of the FMC Act and the corresponding regulations that apply to regulated offers of financial products in New Zealand. Similarly to the position outlined above in relation to fiat currency wallets offered in connection with crypto assets, onerous disclosure and governance obligations arise where services offered by a VASP constitute a regulated offer of debt securities (see the paragraphs titled 'Regulated offers of financial products' under Section 1 and 'Platforms that provide fiat currency wallet or lending/deposit services' under Section 2).
- Certain laws of more general application that would apply – dealing with issues such as unsolicited emails, privacy, and fair dealing (see, for example, the paragraphs titled 'Privacy and data protection', 'Fair trading legislation' and 'Unsolicited electronic messages' under Section 1).

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

Regulation 10AAA of the AML/CFT (Definition) Regulations 2011 provides that a person who keeps or administers virtual assets is a financial institution for the purposes of the AML/CFT Act. VASPs are therefore subject to the broad range of compliance obligations imposed on reporting entities by the Act and accompanying regulations.

Specifically, VASPs have customer due diligence obligations on all customers with whom the VASP has a business relationship, and any customers seeking to engage in 'occasional transactions'. 'Occasional transactions' include any virtual asset transactions valued at NZD 1,000 or more (individually or through several, linked transactions).

The AML/CFT Act also imposes identification and verification obligations on reporting entities in respect of wire transfers if that entity is an ordering, beneficiary or intermediary institution (section 22(3)).

Prior to 1 June 2024, reporting entities were only required to comply with the Travel Rule in relation to a transfer of fiat currency, or a transfer of fiat currency to virtual asset. Since 1 June 2024 and the enactment of the AML/CFT (Definitions) Amendment Regulations (No 2) 2023, reporting entities have also been required to comply with the Travel Rule in relation to virtual asset to virtual asset transfers.

The Guidelines provide that a 'virtual asset to virtual asset transfer' 'includes any transfer where the value is in the form of a virtual asset *at each end*' (emphasis original). Therefore, it includes a transfer of a virtual asset from one wallet to another, but does not include a transfer to or from an un-hosted or self-hosted wallet where there is no other VASP (or equivalent entity) involved.

A reporting entity's obligations will depend on whether it is an ordering, beneficiary or intermediary institution for each transaction conducted:

- An *ordering* institution means any person who has been instructed by a person (the payer) to electronically transfer virtual assets/funds controlled by the payer to a person (the payee) who may or may not be the payer on the basis that the transferred virtual assets/funds will be made available to the payee by a beneficiary institution.

- A *beneficiary* institution, in relation to a wire transfer from an ordering institution, means any person who receives those virtual assets/funds and then makes those assets/funds available to a person (the payee) by crediting them to an account held by the payee or paying it to the payee.
- An *intermediary* institution, in relation to a wire transfer, is a person that participates in a transfer of virtual assets/funds that takes place through more than one institution but is not an ordering institution or a beneficiary institution.

Ordering institutions

The requirements imposed on ordering institutions depend on the value of the wire transfer and whether the transfer is cross-border or domestic.

NZD 1,000 OR MORE

For wire transfers valued at the equivalent of NZD 1,000 or greater the ordering institution must:

1. Identify and verify the identity of the originator:
 - (i) If the transfer is a domestic wire transfer (ie, the VASP is satisfied that the ordering, intermediary and beneficiary institutions are all located in New Zealand), the ordering institution is only required to obtain the originator's account number and any information that enables the transaction to be identified and traced to the originator within three working days of a request being made by a beneficiary institution.
 - (ii) For a transfer that is not a domestic transfer, the ordering institution must obtain the originator's full name; account number; and address or national identity number or customer identification number or date and location of birth.

Verification of the identity of the originator must be carried out before the wire transfer is ordered and all information obtained by the reporting entity must accompany the transfer.

2. Obtain the beneficiary's name and account number or any unique transaction reference. Although VASPs are not required to verify information obtained about the beneficiary of a transaction, the Guidelines note that VASPs may be required to consider the beneficiary of a wire transfer as part of meeting enhanced customer due diligence requirements.
3. Transmit the relevant originator and beneficiary information to the beneficiary institution, or to any intermediary institution in the chain. The requirement to transmit relevant originator and beneficiary information does not apply if the transfer is to an un-hosted wallet.
4. Maintain a record of the information gathered for a period of at least five years after:
 - (i) the end of the business relationship, if the transfer is conducted by a customer with whom the reporting entity has a business relationship; or
 - (ii) the completion of the wire transfer, if the transaction is an occasional transfer.

In many cases the originator will be an existing customer of the ordering VASP. Accordingly, the VASP will have already conducted customer due diligence and obtained and verified the originator information required to be obtained, verified and reported to the Financial Intelligence Unit.

NZD 1,000 OR LESS

For wire transfers valued at the equivalent of NZD 1,000 or less, the ordering institution must ensure the following information accompanies each wire transfer:

- The originator's name and account number or other identifying information that allows the transaction to be traced back to the originator.
- The beneficiary's name and account number or unique transaction reference number.

The ordering institution is not required to verify this information for transactions under NZD 1,000 unless the institution considers there are grounds to report a suspicious activity in relation to the transfer.

Beneficiary institutions

Beneficiary institutions do not have the same identification and verification requirements as ordering institutions. Rather, the only obligation on beneficiary institutions is to develop and use effective risk-based procedures, policies and controls for:

- determining what reasonable steps the reporting entity will take to identify any international wire transfers that lack the required originator information; and
- determining what risk-based policies or procedures the reporting entity will apply if an international wire transfer does not contain any of that information.

Intermediary institutions

There will be limited circumstances where a VASP is merely an intermediary institution. Intermediary VASPs must provide all required information received from the ordering institution to the beneficiary institution as soon as practicable. If that is not possible, the intermediary institution must keep a record of what information was received.

As with beneficiary institutions, intermediary institutions must have adequate AML/CFT policies in place.

Supervising agency

The relevant supervising agency will depend on the activities undertaken by the VASP. For most VASPs the supervising agency will be the Department of Internal Affairs. However, for VASPs: (1) providing a 'licensed market service' (an entity licensed by the FMA); (2) participating in a Financial

Markets Conduct offer as the issuer or offeror of the financial products; or (3) keeping, investing, administering, or managing money, securities, or investment portfolios on behalf of other persons, the relevant supervising agency will be the FMA.

Where a VASP provides both DIA and FMA services, the DIA and FMA will liaise and determine the relevant reporting entity. If the DIA and FMA cannot agree, the AML/CFT co-ordination committee must appoint the AML/CFT supervisor for that entity.

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

The law governing the validity, perfection and priority of security interests in New Zealand is contained in the Personal Property Securities Act 1999 (PPSA). The PPSA applies to 'security interests' in 'personal property' and provides for a broad definition that covers 'traditional' security interests such as mortgages and charges as well as other collateral arrangements. It also applies to so-called 'deemed' security interests including assignments of receivables and leases for a term of more than one year. The PPSA provides for a number of different categories of 'personal property', including:

- chattel paper;
- documents of title;
- goods;
- intangibles;
- investment securities;
- money; and
- negotiable instruments.

The PPSA does not specifically address the categorisation of crypto assets and there is limited New Zealand case law on this matter. In addition, the particular characterisation of an interest in digital assets will depend on the features of that asset. We would expect that it is likely that many forms of digital asset will constitute an investment security or an intangible.

Creating and perfecting security interests

Where New Zealand law determines matters of perfection, the two main methods of perfecting the security interest are taking 'possession' (in the case of certain categories of collateral including 'investment securities') and by registering a financing statement (in the case of any type of collateral).

Possession

In the context of investment securities specifically, the PPSA contains 'deemed' possession rules. In particular, the PPSA provides that (generally speaking) a person takes possession of an investment security if:

- in the case of an investment security that is evidenced by a security certificate, the person takes physical possession of that certificate; or
- in the case of an investment security that is traded or settled through a clearing house or securities depository, the clearing house or securities depository, as the case may be, records the interest of the person in the investment security; or
- in the case of an investment security that is not evidenced by a security certificate and that is not traded or settled through a clearing house or securities depository, the records maintained by the issuer, or on behalf of the issuer, record the interest of the person in the investment security; or
- in the case of an investment security that is held by a nominee, the records of the nominee record the interest of the person in the investment security.

There is no New Zealand case law or legislation considering the application of these provisions in the context of digital assets.

Registration

Whereas possession only perfects security interests in certain types of collateral, registration perfects security interests in *all* types of collateral (including intangibles).

The registration of a financing statement is carried out electronically on the Personal Property Securities Register (PPSR). Certain specified information must be contained in the financing statement (in particular, the name and address of the debtor and the secured party, the debtor's company number and a description of the collateral). The fee payable on registration of a financing statement is nominal (NZD 8.05 or NZD 16.10). A financing statement may be registered either before or after the relevant document has been entered into or a security interest has attached.

There is no stamp duty in New Zealand.

Will the courts in New Zealand recognise and enforce a foreign governing law clause in a crypto asset contract?

Under New Zealand law, the governing law of a security agreement will determine issues relating to the contractual aspects of a security interest under that agreement. However, with respect to the recognition of the validity, perfection and priority of a security interest, the PPSA has specific conflict of laws rules. These conflict of laws rules are complex and they vary for different categories of collateral. In addition, there is no established practice as to how those conflict of laws rules apply in the specific case of digital assets. Clients entering into secured

transactions involving crypto assets with a New Zealand nexus should engage with New Zealand counsel to discuss the potential application of the PPSA and New Zealand law more generally to the transaction.

If, pursuant to the laws of New Zealand, the laws of another jurisdiction govern the creation, validity and perfection of a security interest, and the secured party in question has obtained a valid and perfected security interest under the laws of that jurisdiction, a New Zealand court would recognise said secured party as having a valid and perfected security interest; the secured party would not need to observe or undertake any formalities, notification requirements or other procedures in New Zealand in enforcing its security interest in the relevant collateral.

Enforcement of security interest

Secured parties may enforce a security interest in accordance with Part 9 of the PPSA under one of the following methods:

1. Sale of collateral: section 109 of the PPSA allows a secured party to take possession and sell collateral when the debtor is in 'default' under the security agreement. There are certain notice requirements that may apply in certain circumstances (and some of which can be waived). If a secured party elects to sell collateral, it owes a duty to the debtor and to other secured parties to obtain the best price reasonably obtainable as at the time of sale. The sale may be by auction, public tender, private sale or another method.
2. Application of collateral: if a secured party has priority over all other secured parties, it may apply an accounts receivable or investment security to satisfaction of the secured obligation (we note however this option is not available for general intangibles).
3. Retention of collateral: if a secured party has priority over all other secured parties, it may (on notice) take the collateral in satisfaction of the secured obligation. If the collateral provider rejects this option, then it must sell the collateral in accordance with (1) above.

At any time after default but before one of the above steps is taken, the collateral provider may satisfy the obligations it owes through repayment or some other remedy (plus expenses). Parties also have the option to contract out of certain enforcement provisions under Part 9 of the PPSA.

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

The New Zealand courts generally enforce mechanisms by which contractual parties voluntarily submit to foreign jurisdictions, placing significant value on contractual autonomy and certainty.

Parties can submit to foreign jurisdictions through the use of exclusive, or non-exclusive jurisdiction clauses.

- An exclusive jurisdiction clause is a contractual provision that prescribes the forum for any dispute arising out of the contract.
- A non-exclusive jurisdiction clause generally gives the contracting parties a choice.

Whether a clause is properly construed as exclusive or non-exclusive is fundamental, because it will influence the New Zealand court's approach to its enforceability.

Exclusive jurisdiction clauses

The New Zealand courts recognise that parties to a contract have a prima facie entitlement to enforce a voluntarily bargained exclusive jurisdiction clause. A party asking the New Zealand court to deny such a clause its operative effect faces a heavy burden. A court will only exercise its discretion to assume jurisdiction contrary to an exclusive jurisdiction clause if there is strong cause or exceptional circumstances.

An example of 'strong cause' is where there is a risk of separate trials concerning the same subject matter with different outcomes in two jurisdictions. Another is where the rights of third parties may be impacted, those third parties not being a part of the contractual submission to jurisdiction.

Non-exclusive jurisdiction clauses

The prima facie entitlement does not apply to non-exclusive jurisdiction clauses. Where a contract contains a non-exclusive jurisdiction clause the New Zealand court will engage in a balancing exercise to determine the more appropriate forum to hear the dispute.

Relevant factors include:

- where relief can be granted (if relief can only be granted in one jurisdiction, this will weigh in favour of that jurisdiction determining the dispute);
- cost and convenience;
- location of witnesses and documents;
- governing law;
- strength of the case;
- where judgment will be enforced;
- whether one party is seeking a tactical advantage; and
- any procedural advantages.

Crypto assets

To date there is no New Zealand case explicitly dealing with the validity of an exclusive jurisdiction clause in a dispute involving crypto assets. One of the relevant contracts in *MB Technology Ltd v Orbis Blockchain Technologies Ltd* [2025] NZHC 1012, [2025] NZCCLR 416 contained an exclusive jurisdiction clause in favour of New Zealand, however the validity of that clause was not in issue. Similarly, in a related proceeding, [2022] NZHC 1257, the parties agreed that a settlement agreement would be 'construed in accordance with the laws of the Republic of Singapore'. The

New Zealand High Court therefore applied Singaporean law to interpret the relevant agreement. This approach was endorsed on appeal ([2024] NZCA 47).

Although the enforceability of exclusive jurisdiction provisions were not in dispute in *MB Technology*, that series of litigation helpfully demonstrates that:

- disputes regarding crypto assets will be determined by the New Zealand courts with regard to ordinary principles of contractual interpretation; and
- the New Zealand courts will respect contractual choices of law and jurisdiction.

These observations are consistent with recent trends observed in the New Zealand courts.

Parties can expect that exclusive jurisdiction clauses in disputes concerning crypto assets will be legally binding and enforceable in the event a dispute arises in the New Zealand courts.

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

There are no specific regulatory regimes that apply to the IP of crypto assets (as discussed in Section 2). More generally, innovations and inventions are protected under the New Zealand IP regime, which includes copyright, patents, trademarks and designs. Copyright arises automatically for original works, while patents, trademarks and designs require registration. Ownership is generally with the creator or inventor, but for computer-generated works, the Copyright Act 1994 provides that the author is the person who made the necessary arrangements for the work's creation (typically the person inputting prompts or configuring the system, provided this is supported by the facts). If the work is created by an employee in the course of employment, the employer will usually own the rights.

In the context of blockchain technology, there are no restrictions on what a person can name a token or coin on the blockchain; for example, a token on the Ethereum network could be named 'Bitcoin' regardless of its actual association. However, if a business seeks IP protection over a brand associated with a crypto asset, it must pursue a separate trademark application through the usual legal channels.

IP rights are enforced through civil proceedings, with remedies including injunctions and damages. Infringement is assessed on a qualitative basis and includes adaptations of works, such as converting code into a different language or format.

When seeking protection overseas, rights holders consider commercial significance, risk of infringement, enforceability, and cost, as well as relevant international treaties (eg, the Berne Convention and the Madrid Protocol). IP over crypto assets can be monetised locally, subject to general IP and financial services laws. There are no specific restrictions on monetising IP in crypto assets, but providers must comply with applicable regulatory and tax requirements (as discussed in Section 2).



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