Regulatory Impact Statement Addendum: AML/CFT Statutory Reform – additional offences and penalties

Purpose	This document is an addendum to the previous Regulatory Impact Statement: AML/CFT Statutory Reform (the main RIS). This addendum provides further impact analysis on offences and penalties to inform Cabinet decisions. It relies on the context and analysis in the main RIS and they should be read alongside each other.
Decision sought	Cabinet decisions on amendments to the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).
Agency responsible	Ministry of Justice
Proposing Ministers	Hon Nicole McKee, Associate Minister of Justice
Date finalised	22 June 2026

Acronyms and terms used in this paper

Please refer to the main RIS for a comprehensive list of acronyms and terms used.[1] Additional terms used in this paper are outlined below:

AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism
CASH	Cash is defined as physical currency and not other assets that can be quickly converted into cash (e.g. bank deposits) or funds accessed digitally (e.g. by your debit or credit card).
CRYPTO ATM MACHINES	Crypto ATM machines are physical kiosks that allow customers to deposit cash and receive an equivalent amount of cryptocurrency, typically sent to a digital wallet (and vice versa).
IAG	Ministry of Justice's Industry Advisory Group
IFT	International funds transfer
ML/TF	Money laundering and terrorism financing
MONEY REMITTERS	Money or value transfer service
TSOC	Transnational, serious and organised crime
VASP	Virtual asset service providers

[1] See page two of the main RIS

Summary: Problem definition and options

Description of the option the Minister has chosen

To strengthen New Zealand's response to money laundering and terrorism financing (ML/TF) and transnational, serious and organised crime (TSOC), the Associate Minister of Justice proposes to:

1. Restrict persons in trade from accepting cash above a set limit for international funds transfers (IFT) of remittances and virtual assets conversion. Cash transaction limits and virtual assets in scope would be set in regulations, with non-compliance treated as an offence, aligned with penalties for an existing prohibition in the Act.
2. Introduce infringement offences for less serious or straightforward non-compliance with AML/CFT obligations.
3. Increase civil and criminal penalties for serious non-compliance with AML/CFT obligations to align with comparable domestic and international regimes. This includes enabling penalties to be the greater of a multiple of commercial gain or a percentage of turnover where appropriate.

What is the policy problem?

This addendum covers two distinct policy problems:

1. the misuse of cash in high-risk sectors; and
2. weak enforcement responses across the non-compliance spectrum.

Problem one: the misuse of cash in high-risk sectors

Cash-based international funds transfer channels present high money laundering and terrorism financing (ML/TF) risks. Cash is a highly attractive enabler of criminal activity as its physical and anonymous nature, and the lack of audited money trails, helps criminals to evade detection by law enforcement.

In New Zealand, gangs and TSOC groups generate substantial cash profits from illicit activities including drug supply and large-scale fraud and scams. To do so, they must convert physical cash into forms that can be transferred overseas to associates, suppliers, or facilitators, or otherwise integrated into international financial networks.

Money remitters[2] and virtual asset service providers (VASPs)[3] operating crypto ATM machines provide two key channels for converting cash into internationally transferable value. While both service providers are subject to AML/CFT obligations, once cash is accepted, funds can move rapidly offshore with reduced visibility. This makes it harder for law enforcement to identify risk, intervene before funds are transferred offshore or converted into transferable digital value, and recover criminal proceeds.

The New Zealand Police Financial Intelligence Unit (NZFIU) has identified both services as high-risk and vulnerable to criminal misuse in the National Risk Assessment 2024.[4]

[2] Money remitters accept physical cash and transfer a corresponding sum overseas to a beneficiary. Remitters are attractive to transfer money overseas due to their accessibility, speed, and the industry's global reach and established channels.

[3] VASPs carry out a variety of functions including exchange, international transfer, or safekeeping values, such as cryptocurrencies. Unlike other goods or services that may be purchased with cash, virtual assets can enable near-instant, irreversible, international transfers of value.

[4] The National Risk Assessment on Money Laundering, Terrorism Financing and Proliferation Financing is periodically produced by the NZFIU; [fiu-nra2024.pdf]

The evidence base differs across sectors: domestic evidence is stronger for money remitters, while for virtual assets and crypto ATMs the case for intervention is preventative, based on risk assessments, international evidence, and emerging domestic scam cases.

The status quo creates vulnerabilities that undermine the effectiveness of the Act and New Zealand's contribution to global efforts to combat ML/TF. It also risks activity shifting to less regulated services or methods (known as displacement), including across similar cash-based sectors. Without intervention, money remitters and VASPs may continue to be misused to convert and move criminal proceeds offshore.

Problem two: weak enforcement responses across the non-compliance spectrum

Reporting entities have core obligations under the Act that are designed to protect the integrity of New Zealand's financial system and disrupt ML/TF. Effective compliance depends on supervisors and law enforcement having proportionate, graduated, and dissuasive sanctions that reflect the seriousness of non-compliance and risks posed.

The current AML/CFT framework does not provide supervisors and law enforcement an effective enforcement toolkit. For less serious and straightforward non-compliance, responses are often limited to formal warnings or resource-intensive civil or criminal proceedings, which can be disproportionate and may discourage timely intervention. For more serious non-compliance, existing maximum penalties do not adequately reflect the severity of the conduct and may lack sufficient deterrent effect, particularly for larger or multinational reporting entities such as banks or casinos.

International and domestic reviews have identified these weaknesses. The 2021 Financial Action Task Force (FATF) Mutual Evaluation (ME) and 2022 Statutory Review found that the Act does not currently provide AML/CFT supervisors with an effective and proportionate response to non-compliance.

What are the policy objectives?

Further to the high-level objectives outlined in the main RIS, reforms are seeking to achieve specific objectives for each problem:

Problem one: the misuse of cash in high-risk sectors

- Minimising negative impacts on the legitimate use of cash by New Zealanders not engaged in criminal activities.
- Increasing the costs and difficulty of transferring funds offshore by criminals, thereby supporting law enforcement to tackle TSOC.
- Future-proofing the Act by introducing tools that can appropriately respond to changes in risk and evidence of harm.

Problem two: weak enforcement responses across the non-compliance spectrum

- Enabling enforcement responses to non-compliance to be more proportionate, dissuasive, and therefore effective.

What policy options have been considered, including any alternatives to regulation?

Problem one: the misuse of cash in high-risk sectors

Options to prevent harm from cash-based remitters that enable IFT and VASPs that enable cash-for-virtual asset conversion include:

- Retain the status quo.
- Remove the risk by restricting services from accepting any cash at all.

- Make it harder and more expensive for criminals to operate, by restricting services from accepting cash transactions above a limit/s by secondary legislation.
- Dissuade illegal use by introducing offences and penalties to support any restriction.

Any option must be balanced against legitimate use. Cash remains legal tender. Remittance services are essential for some communities, particularly Pacific Recognised Seasonal Employer (RSE) workers, migrants, and the not-for-profit sector. VASPs also support innovation, competition, and economic activity in New Zealand.

Problem two: weak enforcement responses across the non-compliance spectrum

The main RIS has already considered problem two and Cabinet has agreed to introduce an infringement regime and increase penalties for serious non-compliance.

This RIS addendum provides further options to progress Cabinet's direction to strengthen the Act's offence and penalty settings, improve proportionality and deterrence, and align with comparable domestic and international regimes. These options include:

- Introducing 12 new infringement offences to address less serious and straightforward non-compliance.
- Increasing penalties for civil liability acts and 17 specified offences, including 9 increased imprisonment terms and 12 variable financial penalties for commercial gain (up to 300% of gain and/or 10% of turnover).

What consultation has been undertaken?

The following public sector agencies have been consulted on this addendum: Department of Corrections, Department of Internal Affairs (DIA), Financial Markets Authority (FMA), Inland Revenue Department, Ministry of Business, Innovation, and Employment (MBIE), Ministry of Foreign Affairs and Trade, Ministry for Pacific Peoples, New Zealand Police including the NZFIU, Office of the Privacy Commissioner, Reserve Bank of New Zealand (RBNZ), the Treasury and intelligence agencies.

Problem one: the misuse of cash in high-risk sectors

The Ministry conducted a survey with money remitters registered on the GoAML platform and with members of the Ministry's Industry Advisory Group (IAG).[5] Consultation signalled mixed support for restricting the amount a person in trade could accept.

New Zealand's two Crypto ATM providers did not support a complete ban on crypto ATM machines but one provider proposed introducing a $10,000 limit as an alternative.

Problem two: weak enforcement responses across the non-compliance spectrum

The main RIS outlines consultation undertaken on introducing an infringement regime and increasing penalties for seriousness non-compliance.

The IAG was consulted on proposed offences and increased penalties levels, including commercial gain penalties. Feedback generally supported strengthening the effectiveness and proportionality of the enforcement regime, while highlighting the need for appropriate safeguards, including against double jeopardy and the availability of defences.

Is the preferred option in the Cabinet paper the same as preferred option in the RIS?

Yes, the preferred option in the Cabinet paper is the same as the preferred option in the RIS.

[5] The IAG features representatives from key industry stakeholders, including banks, financial services, industry representative bodies, and designated non-financial businesses and parties (such as accountancy and law firms).

Summary: Chosen options

Costs

Problem one: the misuse of cash in high-risk sectors

The following costs relate to restricting remittance services from accepting cash above a limit for IFT and the conversion of cash for specified virtual assets.

Regulated groups (reporting entities[6]):

- Restricting cash transactions will require one-off and ongoing changes to AML/CFT programmes, including updates to systems, staff training, customer processes, and internal controls.
- Money remitters may incur customer transition costs, operational changes, and potential revenue loss where their activities rely on larger cash transactions.
- Crypto ATM operators may face higher impacts, including winding down or exiting the market, loss of existing investments, and forgone future revenue, depending on how thresholds are set.
- Some business models that rely on higher-value cash transactions may become commercially unviable, though this is mitigated by setting thresholds in regulations, informed by evidence on legitimate use, and by preserving non-cash alternatives.
- Cash limits and associated offences and penalties may create uncertainty and dampen growth or innovation among money remitters and VASPs.
- Proposals may increase perceived compliance risk for some services, particularly by banks, potentially contributing to further de-risking if not implemented proportionately.

Government agencies:

- One-off implementation costs to produce guidance and support transition.
- Single supervisor (DIA): Enhanced resourcing to support supervision, investigations and enforcement. Staff training and capability building.

General public:

- By making it harder and more expensive for criminals to operate, the proposals may also increase costs or reduce convenience for legitimate users.
- Indirect impacts may include reduced access, provider exit or reduced market entry, higher prices, or migration to offshore, informal or illegal channels.
- Impacts may particularly affect legitimate users of money remitters, including migrant and Pacific communities, although the scale of impact will depend on threshold design and availability of non-cash alternatives.
- Restrictions may reduce the ability of some RSE workers and migrants to remit funds, potentially increasing financial hardship and affecting labour mobility.

Problem two: weak enforcement responses across the non-compliance spectrum

The main RIS considered the costs for problem two. Additional costs are outlined below.

Reporting entities:

- Higher penalties may increase compliance and risk-management behaviour across reporting entities, potentially including incurring higher costs to strengthen compliance arrangements, governance, and oversight.
- Indirect costs may vary by entity size and compliance maturity, affecting pricing, service availability, market entry, competition, and innovation. Larger entities may be

[6] Some offences and penalties apply to persons in trade, who may not be a reporting entity under the Act.

better positioned to absorb additional costs, while smaller entities may face proportionately higher impacts.

- Increased penalties may increase perceived compliance risk, particularly by banks, potentially contributing to further de-risking if not implemented proportionately.

Government agencies:

- Indicative estimates suggest one person per year could be sentenced to prison for serious non-compliance offences. The Department of Corrections has advised this would occur at a cost of $120,000 per prisoner per year.
- Estimates also suggest an average of three people could be prosecuted per year.
- Higher penalties may increase contested enforcement action, with associated costs for NZ Police (litigation costs), Crown prosecutors, the Public Defence Service and the courts (including legal aid).
- The infringement regime may add minor administrative costs for supervisors, including issuing notices, managing disputes and maintaining systems.

Benefits

Outline the key benefits and where those benefits fall

Problem one: the misuse of cash in high-risk sectors

The following benefits relate to restricting cash transactions above a limit for IFT and cash-to-virtual-asset services.

AML/CFT System:

- More effective and proportionate framework that targets the highest-risk cash sectors and directs government resources where they have the most impact.
- Reduced criminal misuse by increasing the cost and difficulty of converting cash into internationally transferable value.
- Greater system coherence and resilience by treating comparable cash-based activities consistently and limiting displacement between sectors.
- More adaptable and future-proof tools that can be calibrated in response to changing risks and emerging evidence of harm.

Regulated groups

- Greater certainty managing higher-risk transactions, including declining where appropriate.

Government agencies:

- Improved ability to detect, disrupt, and investigate non-compliance in high-risk cash sectors, including through increased reporting and visibility.

Problem two: weak enforcement responses across the non-compliance spectrum

AML/CFT System:

- A more credible, graduated framework enabling earlier and more proportionate responses to less serious non-compliance, while reserving stronger sanctions for serious or repeated conduct.
- Stronger deterrence for serious non-compliance, supporting more efficient use of supervisory and enforcement resources.
- Continued alignment with FATF standards s9(2)(d)

s9(2)(d)

Balance of benefits and costs

Does the SAR indicate the benefits of the chosen option are likely to outweigh its costs?

Problem one: the misuse of cash in high-risk sectors

On balance, the benefits of restricting high-risk cash channels is assessed as outweighing the costs. Key benefits include reducing criminal misuse of money remitters and VASPs, limiting opportunities for displacement between comparable cash-based sectors, and strengthening the effectiveness and credibility of the AML/CFT system.

Reporting entities and legitimate users may face higher costs or reduced access, and some businesses that rely heavily on large cash transactions may need to adjust or exit the market. These impacts are mitigated by focusing on high-risk cash transactions rather than all activity, preserving non-cash alternatives, setting thresholds through regulations, consulting on legitimate use with affected communities (including Pacific and migrant communities), and monitoring displacement effects over time.

Problem two: weak enforcement responses across the non-compliance spectrum

On balance, introducing an improved graduated enforcement regime and strengthening offence and penalty settings is assessed as outweighing the costs.

While reforms may increase compliance, enforcement, and litigation costs for some reporting entities, these are assessed as manageable. They are outweighed by system-level benefits, including stronger deterrence, improved compliance incentives, more proportionate and timely enforcement, and increased credibility of the AML/CFT regime.

The proposals also align offence and penalty settings with comparable and international regimes, supporting global standards, maintaining confidence in the financial system, and
s9(2)(d)

Overall, the reforms impose higher standards and expectations of compliance on regulated entities, but they are assessed as strengthening enforcement effectiveness, compliance incentives, and system resilience over time. Impacts on the prison population are expected to be minimal, as imprisonment remains limited to the most serious cases and is not the primary enforcement pathway for most non-compliance.

Implementation

How will the chosen option be implemented, who will implement it, and what are the risks?

s9(2)(f)(iv)

The proposals will be subject to the one-year transition period, to enable reporting entities to prepare and make the necessary transition.

Regulations will be required to set the cash transaction threshold, prescribe virtual assets in scope, and specify infringement penalties. These are expected to be developed and in force alongside the Bill s9(2)(f)(iv)

s9(2)(d)

The DIA, as the single supervisor, and New Zealand Police will enforce the regime. DIA will leverage its existing Gambling Act infringement regime, including utilising established processes for issuing and managing notices.

During the transition period, there is a risk that virtual assets and IFTs of remittances will continue to be misused by criminals. Agencies will continue to prioritise intelligence and supervisory activity during this period to partially mitigate this risk.

Limitations and Constraints on Analysis

Outline all significant limitations and constraints on the process and content of the SAR

Problem one: the misuse of cash in high-risk sectors

The scope of analysis was constrained by Cabinet and Ministerial direction. Cabinet made in-principle decisions on proposals early, alongside final policy decisions for the Bill. These decisions were made public at that time, limiting consideration of the overall policy direction.

Officials focused analysis on two recommendations from the TSOC Ministerial Advisory Group (TSOC MAG), rather than undertaking a broader review of cash.

Timeframes enabled targeted consultation with affected providers and engagement with the Ministry's IAG. Wider consultation with customers would have provided greater insight into patterns of legitimate use and supported earlier signalling of potential changes.

The domestic evidence base is limited, particularly for misuse of virtual assets. While some scam-related misuse of crypto ATMs is identified, there is no well-developed domestic ML/TF evidence base, constraining assessment of impacts and proportionality of options.

Problem two: weak enforcement responses across the non-compliance spectrum

The scope of analysis for Problem Two was constrained by prior Cabinet decisions. The main RIS concluded that introducing an infringement regime and increasing maximum penalties to address serious non-compliance with AML/CFT obligations were required. Cabinet agreed to the proposals considered in this RIS addendum and as a result, does not revisit whether these tools should be introduced.

Setting infringement offences in primary legislation and penalty levels in regulations limited detailed assessment of behavioural and cost impacts, and reduced opportunities for industry consultation. The offences were not consulted with Legislation Design Advisory Committee (LDAC) due to time constraints but were tested against Cabinet-approved guidance and the LDAC framework as part of policy development.

Analysis of whether increased compliance would result in positive impacts on court workloads, for example through reduced prosecutions, has not been undertaken as this would require modelling beyond the scope of this RIS.

I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the chosen option.

Caroline Greaney
Deputy Secretary, Policy
17 June 2026

Quality Assurance Statement	
Reviewing Agency: Ministry of Justice	**QA rating:** Partially meets
Panel Comment: The Ministry of Justice Regulatory Impact Analysis Quality Assurance Panel has reviewed the Regulatory Impact Statement Addendum prepared by the Ministry of Justice and consider that the information and analysis summarised in the Addendum partially meets the quality assurance criteria. The panel notes that, for the proposal relating to money remitters, there was no public consultation. The preferred option gives the opportunity to consult on threshold design, which would help to mitigate any negative impacts on legitimate users of these services. For the proposals for enforcement responses, consultation was also limited due to time.	

Problem one: the misuse of cash in high-risk sectors

Section 1: Diagnosing the policy problem

What is the context behind the policy problem and how is the status quo expected to develop?

1. For more context on how the Act implements offences and penalties, please see issue four of the main RIS.[8]

Cabinet is concerned about cash being exploited by organised criminals

2. In November 2024, Cabinet established the TSOC MAG to provide independent advice and recommendations on ways that law enforcement and regulatory agencies could work together to more effectively to detect, deter and dismantle TSOC groups.[9]
3. The MAG's Report from April 2025 recommended options to make cash less attractive to criminals and to strengthen the controls on cash within New Zealand.[10] It proposed to ban businesses from accepting cash payments for IFT services and crypto ATM machines.[11] [12]
4. Cabinet agreed in-principle to:
   - prohibit businesses from accepting cash payments of over $5,000 for international funds transfer services with penalties in line with those for equivalent prohibitions on certain cash transactions in the Act, subject to final Cabinet decisions when considering the draft Bill; and
   - prohibit virtual currency Automatic Teller Machines with penalties in line with those for equivalent prohibitions on certain cash transactions in the Act, subject to final Cabinet decisions when considering the draft Bill.
5. Cabinet will make final decisions on the policy proposals in this RIS at the same time as it considers and approves the final Bill for introduction to the House.

[8] See page 50 of the main RIS.
[9] tnoc-mag-cabinet-paper.pdf, page 1
[10] mag-final-report-71025.pdf, page 56
[11] NB: There are differences in recommendations between April and Final Report. tsoc-mag-25-02b-april-report-cash-proceeds.pdf, page 13; mag-final-report-71025.pdf, page 56
[12] Note comments by MAG in the media: Cash in circulation has been rising. Why? | interest.co.nz

While cash is attractive to criminals, it remains a legitimate part of the economy

6. The Ministry largely agrees with the findings of the TSOC MAG on cash. Justice sector agencies have repeatedly noted that cash is highly attractive to criminals and gangs given it can obscure trails of illicit money.[13]

7. Prior to the establishment of the TSOC MAG, New Zealand's 2024 National Risk Assessment described cash as a "key threat driver" that affords anonymity, underpins the criminal economy, and enables predicate offending and money laundering through its conversion into high-value goods.[14] The Assessment also identified money remitters and virtual asset service providers (VASPs) as among the highest-risk sectors in the AML/CFT system.[15]

8. However, the Ministry recognises that cash is legal tender in New Zealand and is legitimately used across the country. RBNZ's 2026 public consultation on reform of cash systems also noted that cash is important because cash can be the only viable option for payment if digital platforms are disrupted.[16] In some cases, cash is the only means of payment for people not able to access financial services.

Background on cash-based money remitters

Cash-based money remitters present the highest risks in the sector

9. International funds transfers (IFTs) refers to services that enable money to be transferred overseas between individuals and businesses. A subset of IFTs are money remitters, which transfer value (known as remittances) internationally on behalf of customers.

10. In New Zealand, remittances can be transferred overseas by a range of providers including banks, digital remitters, and cash-based remitters. Banks and digital remitters require customers to fund transfers through bank accounts, debit/credit cards, or other electronic payment methods, which create transactional records that lower money laundering risks.

11. Cash-based remitters accept physical cash for IFTs and therefore present higher money laundering risks. Cash transactions reduce transparency at the point of entry into the financial system and remitters can facilitate the placement and international transfer without clear transaction records showing the source of funds.

Money remitters are supervised reporting entities under the Act

12. Money remitters are reporting entities under the Act and are supervised by the Department of Internal Affairs (DIA). Money remittance is defined in the Act as part of the broader category of money transfer services.[17]

13. Approximately 100 money remitters are registered with DIA, including a mix of multinational providers (such as Western Union) and smaller operators servicing a particular community, country or region.

[13] Supplementary-Analysis-Report-Criminal-Activity-Intervention-Legislation-Bill.pdf, page 55
[14] fiu-nra2024.pdf, page 10
[15] fiu-nra2024.pdf, page 10
[16] cash services for the future, page 5
[17] Anti-Money Laundering and Countering Financing of Terrorism Act 2009 | New Zealand Legislation – section 5(2)

14. Money remitters are required to comply with obligations under the Act, including customer due diligence, record-keeping, and wire transfer requirements.[18] This includes ensuring originator and beneficiary/payee information is included in payment messages.

Money remitters have legitimate uses for cash

15. Money remitters, including those that operate in cash, provide an important financial service to New Zealanders. They can offer lower-cost international transfers than banks and service customers who may lack access to banking services or whose intended recipient is located in regions with limited or disrupted financial infrastructure.

16. RSE workers from Pacific countries are among the legitimate users of money remitters, often transferring earnings to family members offshore while employed in New Zealand.[19] Immigration New Zealand advises that typical RSE remittance behaviour involves periodic transfers of approximately $500 throughout the year, followed by a larger transfer of $2,000 to $4,000 at the time of final pay. Some workers instead carry cash with them when travelling home, which is limited to $10,000.[20]

17. Research into comparative international jurisdictions found no restrictions on the amount a money remitter could accept for international funds transfer, likely due to concerns on legitimate use and negative impacts on vulnerable people who rely on remittances.

Background on virtual assets and crypto ATMs

Cryptocurrencies and crypto ATMs present the highest risks in virtual assets sector

18. VASPs carry out a variety of functions such as exchange, transfer, or safekeeping of virtual assets. The most widely known virtual asset is cryptocurrency, such as Bitcoin, although the sector encompasses a much broader range of products and services.

19. The majority of VASP activity in New Zealand occurs through non-cash, account-based digital platforms that require customers to use bank transfers or other electronic payment methods. Digital platforms support common retail uses such as investment, trading, and transfers of value. This includes retail-facing platforms such as Easy Crypto and Sharesies, alongside smaller providers offering more specialised services.

20. Cash-based access to virtual assets represents a narrower and higher-risk subset of the sector. At present, the only known mechanism in New Zealand that enables the direct conversion of cash into virtual assets is through crypto ATM machines, which launched in New Zealand in 2023. Crypto ATMs are physical kiosks that allow users to deposit cash and receive a corresponding amount of cryptocurrency transferred to a digital wallet. In some cases, crypto ATMs also support stablecoins, a different form of virtual asset.

21. The economic rationale for legitimate investors using crypto ATMs is less clear than remitters. New Zealand-based crypto ATM operators charge service fees of approximately 10 to 20 percent per transaction. By comparison, online virtual asset exchanges typically offer access to the same assets for fees of less than one percent when transactions are conducted using bank accounts or cards.

---

[18] See section 28 of the Act. Wire transfers refer to transactions that transfer funds by electronic means.
[19] Review of the Money Remittance Market in New Zealand: A report on the problems affecting the remittance services between New Zealand and the Pacific, 2017, prepared by Deloitte for the Treasury.
[20] See section 68 of the Act.

Virtual asset service providers are supervised reporting entities under the Act

22. VASPs are reporting entities under the Act and are supervised by the DIA.

23. Virtual assets are defined in the AML/CFT (Definitions) Regulations 2011.[21] The Act adopts a technology-neutral, activity-based definition of virtual assets that broadly reflects the Financial Action Task Force (FATF) standard. It refers to a digital representation of value that can be transferred or traded electronically and used for payment or investment purposes.

24. While many virtual assets fall within the Act's definition, not all virtual assets can be offered for cash or are suitable to launder money. Consequently, some virtual assets do not present the same high risks as cryptocurrencies.

25. VASPs, including crypto ATM providers, are required to undertake customer due diligence requirements and provide prescribed transaction reporting (PTR) to the NZFIU. This includes all transactions over $1,000 except when the involved parties are known to be based in New Zealand,[22] and any large cash transaction of $10,000.[23]

26. Internationally, there is a growing body of evidence that Crypto ATMs are being used to launder criminal proceeds.[24] Overseas jurisdictions, such as Australia, the United States of America, the United Kingdom, and Singapore are taking action through implementing limits and bans in response to risks of criminal misuse.[25]

A similar offence and penalty framework exists in the Act that could be replicated

28. Cabinet's in-principle agreement provides that the offences and penalties for the proposals should align with existing cash-based prohibitions in the Act. The relevant comparator is provided for in sections 67A (the offence) and 105A (the penalty) which prohibit persons in trade from selling specified articles such as jewellery, watches, precious metals or stones, motor vehicles and ships for cash transactions above a prescribed threshold, set in regulations at $10,000.[26]

29. The framework combines strict liability offences for prohibited conduct with escalating consequences for more culpable behaviour, supporting proportionate and consistent enforcement. Under this approach, the same prohibited cash transaction can attract different legal outcomes depending on whether the conduct was inadvertent, deliberate, or reflects broader failures to meet AML/CFT obligations.

---

[21] AML/CFT (Definitions) Regulations 2011, regulation 4.
[22] Ibid, regulation 15AA
[23] Ibid, regulations 10 and 15AA
[24] iowaattorneygeneral.gov/media/cms/CryptoPresserFactSheet_025A49CA1858C.pdf; $3 million lost to cryptocurrency ATM scams in 12 months may be just the tip of the iceberg | Australian Federal Police; Powers proposed to tackle high-risk products services and channels | AUSTRAC; The role of virtual currency automated teller machines in laundering the proceeds of crime
[25] Crypto ATM providers to meet minimum standards | AUSTRAC; Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026 – Parliament of Australia; FCA takes action against unregistered crypto ATM operators in Leeds | FCA; MAS Issues Guidelines to Discourage Cryptocurrency Trading by General Public
[26] AML/CFT (Definitions) Regulations 2011, regulation 5AC

Is the comparator framework appropriate to be replicated for the proposals?

30. When section 67A was introduced in the Act in 2023, the Criminal Activity Intervention Legislation Bill was assessed for consistency with the New Zealand Bill of Rights Act 1990 (NZBORA). No substantial issues were raised at that time in relation to strict liability. [27]

31. The Ministry considers that the framework raises tensions with established criminal justice principles due to the combination of strict liability, significant financial penalties, and the availability of imprisonment.

32. Strict liability offences are typically associated with lower-level penalties. However, sections 67A and 105A provide for fines of up to $300,000 for individuals (proposed to increase to $500,000 under Problem Two) and up to $5 million for bodies corporate. Non-compliance with section 67A may also attract a term of imprisonment of up to 2 years for individuals (not proposed to increase under Problem Two).

33. Strict liability offences are generally inappropriate where imprisonment is available and must be assessed on a case-by-case basis. The Ministry communicates this position across the public sector when vetting proposed new legislation, and does so for the following reasons:

    - Strict liability offences lack a mental element (*mens rea*), such as knowledge or recklessness, which serves as an important safeguard against disproportionate punishment. The absence of a mental element shifts the burden onto the defendant to demonstrate a defence.
    - Imprisonment represents the fullest imposition of the criminal law and is reserved for morally culpable conduct; conduct which society considers blameworthy and should be subject to denouncement and punishment by way of criminal conviction and imprisonment. Conduct which is morally culpable and blameworthy usually includes a mental element.

Areas of concern where the proposals may limit NZBORA rights

34. The absence of a mental element in section 67A engages the right affirmed in section 25(c) of NZBORA; to be presumed innocent until proven guilty.

35. The potential limit on NZBORA is of particular concern where the proposed offences and penalties apply beyond AML/CFT reporting entities. Most of those subject to the proposals would be part of a highly regulated population; AML/CFT reporting entities that are subject to supervision and expected to understand and comply with clearly defined statutory obligations. In this setting, the acceptance of cash is a controlled commercial activity, where obligations are known and compliance can reasonably be ensured.

36. The proposals, however, will also apply to 'persons in trade' who are not reporting entities. While 67A already captures 'persons in trade', we consider there is a possibility that some (i.e. a local dairy owner that has a remittance service) may not be as informed of their obligations as reporting entities, be unaware of the consequences, and a term of imprisonment may be disproportionate in these circumstances.

37. However, officials also consider that 'persons in trade' ought to be aware of their obligations as they are carrying out highly regulated activities. DIA, as supervisor, already

[27] 20220914-Criminal-Activity-Intervention-Legislation-Bill-Consistency-with-NZBORA-as-amended.pdf, see pages 3-5

invests significant resource in educating and supporting the sector to comply with obligations, such as through guidance and codes of practice.[28]

Recommended approach for replicating these offences and penalties in the Bill

38. Where non-compliance is knowing or reckless (*mens rea*), officials consider imprisonment to be an appropriate penalty given vulnerabilities to ML/TF. The Ministry considers it best practice to require *mens rea* where imprisonment is available. This ensures the most severe penalties are reserved for the most serious conduct and mitigates the risk of unjustified limits on NZBORA rights.

39. If no *mens rea* is required in the offence, it is a strict liability offence. Penalties should not include imprisonment and should be limited to financial penalties, consistent with established criminal justice principles.

40. The recommended approach to offences and penalties in the Bill for virtual assets and IFTs of remittances is as follows:

    - Non-compliance with the restriction should give rise to either a full criminal or strict liability offence. The full criminal offence applies where non-compliance is accompanied by *mens rea,* while the strict liability offence captures instances of non-compliance regardless of intent.
    - Imprisonment and/or a financial penalty should be available where non-compliance is committed knowingly or recklessly.
    - Only a financial penalty should be available where non-compliance occurs without an established *mens rea*.

41. The graduated approach to penalties ensures the regime remains effective, deterrent and enforceable, while reserving imprisonment for the most serious conduct.

What is the policy problem or opportunity?

Policy problem: responding to the misuse of cash in high-risk sectors

42. Gangs and TSOC groups generate substantial criminal proceeds from activities such as drug supply and large-scale fraud and scam offending. Regardless of the underlying activity, criminal proceeds are often generated in cash and are used to sustain criminal operations, maintain power and influence, and fund further offending. To realise profit, gangs and TSOC groups must convert physical cash into forms of value that can be transferred offshore to pay overseas associates, suppliers, or facilitators, or otherwise integrate into international financial networks.

43. Cash presents elevated money-laundering risk because its physical and anonymous nature allows value to enter financial and payment systems without clear records showing the source of funds. Once cash is converted into internationally transferable value and moved offshore, detection, disruption, and recovery of criminal proceeds become substantially more difficult.

[28] See pages 51 – 53 of the main RIS.

44. The following case study demonstrates the relationship between TSOC, IFTs and money laundering: see explanatory note at bottom of page

Illustrative case study: Increased methamphetamine use in New Zealand
Wastewater testing indicated a doubling of meth use in New Zealand in 2024. Since 2020, there has been an increase of 266 percent in meth seized here and offshore. Justice sectors officials have estimated the societal cost of meth to the community to be $1.5 billion in 2024.   As meth is not manufactured in New Zealand, domestic criminals must pay overseas criminal organisations (predominantly in Southeast Asia and South America) to import it to New Zealand (often via the Pacific). By operating in physical cash, criminals make it harder for law enforcement to 'follow the money'. However, to make payments for drug imports, they must make use of international funds transfer services to move their cash revenues offshore. This allows criminals to make payment for meth without alerting law enforcement and further profit from their crimes.

45. Money remitters and VASPs provide two high-risk services through which cash can be converted into internationally transferable value. While both services are subject to AML/CFT obligations as reporting entities, current settings do not sufficiently mitigate the specific risks arising at the point where physical cash is accepted and transferred overseas or directly converted into virtual assets.

46. Money remitters and VASPs can convert physical cash into transferable value that is sent offshore or on-chain almost immediately, before the source of funds can be fully verified. Regulators and law enforcement consequently have less opportunity to identify risk and intervene before funds are transferred offshore or converted into transferable digital value. By contrast, bank-based international transfers operate through account-based systems that generally provide greater transaction visibility and ongoing engagement beyond the initial cash deposit, and are therefore not the focus of this problem definition.

47. The National Risk Assessment 2024 has identified money remitters and virtual assets among the highest-risk sectors within the AML/CFT system.[29] However, the nature of the risk and the available evidence of criminal misuse differs between these sectors.

Sector specific risks and evidence of harm: Money remitters

48. Domestic evidence of criminal misuse is stronger for money remitters, reflecting their established role in facilitating IFTs and their recurring appearance in enforcement and intelligence reporting. Cash-based money remitters offer accessibility, speed, and global reach,[30] which are attractive to transnational drug-traffickers and international scam networks seeking to move criminal proceeds offshore.[31]

49. The elevated risk associated with cash-based money remitters is reflected in domestic enforcement experience. In one recent high-profile prosecution, a money remitter was found to have assisted in laundering approximately $18 million for a drug syndicate, with the owners receiving prison sentences of up to six years.[32] As supervisor, DIA has issued 25 formal warnings to money remitters since 2014, taken six civil proceedings since 2017, and prosecuted three criminal cases for AML/CFT non-compliance.

Cryptocurrencies and crypto ATMs

This explanatory note corrects an error in the above Illustrative case study: Increased methamphetamine use in New Zealand. The RIS Addendum considered by Cabinet stated that "meth is not manufactured in New Zealand…". This statement was incorrect as methamphetamine can be manufactured in New Zealand. The text should instead read: "As meth is not solely manufactured in New Zealand…"

[29] fiu-nra2024.pdf, see page 34
[30] fiu-nra2024.pdf, see page 38
[31] fiu-nra2024.pdf, see page 38
[32] Auckland money launderer Ye Hua has prison sentence reduced on appeal | RNZ News

50. By contrast, domestic evidence of misuse of virtual assets, particularly cryptocurrencies, is less developed. International experience and NZFIU reporting indicate that cash-to-virtual-asset services are an established method for disguising criminal proceeds and placing value in the legitimate financial market.

51. Crypto ATMs are assessed as a high-risk product because they are inherently cash-based and enable rapid, irreversible international transfer of value once conversion occurs. Transactions are difficult to trace due to the pseudo-anonymous nature of cryptocurrency wallets, which do not contain personal identifying information unless later linked to an individual through investigation. This allows cash-to-virtual-asset transactions to occur without using traceable intermediaries, such as banks, including through the use of third-party wallets. Combined with the relatively recent emergence of crypto ATM services and evolving regulatory controls, these characteristics materially increase risk.

52. The Ministry is aware of some recent cases of crypto ATMs being misused for fraud, including scam-related offending.[33] However there is not yet a developed domestic evidence base demonstrating the use of crypto ATMs to launder money or move criminal proceeds offshore. The case for restricting the conversion of cash for virtual assets is therefore preventative and risk-based, informed by international evidence, inherent characteristics of these assets and services, emerging case-studies, and observed limitations in regulatory measures rather than extensive domestic enforcement outcomes.

53. The Ministry and regulatory AML/CFT supervisors have introduced measures to mitigate money laundering risk in high-risk sectors, including the existing limit on cash transactions for certain high-value goods. However, current regulatory settings do not sufficiently constrain high-risk cash transactions in IFTs and virtual assets. As a result, current regulatory settings leave vulnerabilities that undermine the effectiveness of the AML/CFT regime, particularly in constraining high-risk cash transactions and preventing displacement between comparable cash-based services.

54. Without further changes, the Ministry considers that money remitters and VASPs will continue to be vulnerable to cash-based misuse by criminals to launder money.

Policy opportunity: Cabinet has made in-principle decisions to address this problem

55. Cabinet has agreed in-principle to two policy responses to address the criminal misuse of cash in IFT of remittances and virtual assets, drawing on advice from the April report of the TSOC MAG. These include:

- prohibiting businesses from accepting cash payments above a specified threshold of over $5,000 for international funds transfer services; and
- prohibiting virtual currency Automatic Teller Machines (crypto ATMS)

56. The Ministry considers the solutions agreed to in-principle by Cabinet could be refined to ensure that legitimate and low-risk uses continue, consistent with a proportionate, risk-based AML/CFT regulatory approach.

57. To achieve this, the problem definition must be balanced against the legitimate use of cash, IFT of remittances, and virtual assets:

- Cash is legal tender, providing a secure, immediate and private medium of exchange for New Zealanders who rely on it.

[33] The Financial Markets Authority recently received two scam complaints in which crypto ATMs were used to transfer funds to scammers. The victims suffered losses of approximately $1,600 and $13,000 respectively; Tens of thousands lost to crypto ATM scams, ombudsman says | RNZ News

- Remitters provide an important financial service, particularly for seasonal workers from the Pacific, migrants and the not-for-profit sector. Users choose to remit money (including cash) for a variety of reasons including to obtain value-for-money, cultural practice, disrupted financial infrastructure in their home country, or the absence of bank accounts. For many Pacific peoples, remittances play a central role in supporting families and communities overseas.
- Virtual assets and VASPs can offer new economic opportunities by reducing costs and frictions in payments and investment, supporting competition in financial services and contributing to broader productivity and growth objectives.

Impacts on the general public

58. Any major disruption to remittance and virtual asset services would have implications for legitimate customers. By making it harder and more expensive for criminals to operate, restrictions may also increase costs or reduce convenience for some legitimate users.

59. The impacts of the proposals will be different for the customers of each service:

- For money remitters, restricting cash will have impacts for vulnerable customers who use or receive cash because of factors such as age, disability, living remotely, lack of access to bank accounts or weak infrastructure overseas.
- For VASPs, restricting cash for conversion of virtual assets will likely be less significant for vulnerable groups. Rather, it will limit options for those seeking economic freedom, wishing to access new markets conveniently. It also may have a chilling impact on market conditions, which could be contrary to Government policies supporting economic growth.

60. To mitigate negative impacts on users, any restriction would need to be carefully set to capture the appropriate point where impacts on legitimate use is minimised while still impeding criminal activities, having regard to risks and evidence.

What objectives are sought in relation to the policy problem?

61. As outlined in the main RIS, the reforms seek to meet three high-level policy objectives:

- Ensuring the AML/CFT system is effective in meeting the purposes of the Act.
- Reducing unnecessary compliance costs for businesses.
- s9(2)(d)

62. Within these broad high-level objectives, the reforms seek to meet the following specific objectives for problem one:

- Minimising negative impacts on the legitimate use of cash by New Zealanders not engaged in criminal activities.
- Increasing the costs and difficulty of transferring funds offshore by criminals, thereby supporting law enforcement to tackle TSOC.
- Future-proofing the Act by introducing tools that can appropriately respond to changes in risk and evidence of harm.

What consultation has been undertaken?

63. The following public sector agencies have been consulted on the proposals for problem one: Department of Corrections, Department of Internal Affairs (DIA), Financial Markets Authority (FMA), Inland Revenue Department, Ministry of Business, Innovation, and

Employment (MBIE), Ministry for Pacific Peoples, Ministry of Foreign Affairs and Tra de, New Zealand Police including the NZFIU, Office of the Privacy Commissioner, Reserve Bank of New Zealand, the Treasury, and intelligence agencies.

64. Timeframes in which the policy proposals have been developed allowed for some targeted consultation with impacted providers on Cabinet's in-principle decisions.

Consultation with money remitters

65. To gauge stakeholder views on restricting IFT of remittances, the Ministry conducted a survey on Citizenspace with money remitters registered on the GoAML platform[34] and with members of the Ministry's IAG members. The survey was open for two weeks and included the limit amount of $5,000.

66. Only 15 submissions were received, of which nine supported the proposal and six opposed. Of those that were money remitters, five were in support and three opposed.

67. Supporters generally emphasised the crime disruption and AML/CFT benefits, arguing that a limit would close an established vulnerability, strengthen transparency, and align with modern risk-based expectations. Opposition centred on regulatory inconsistency and financial inclusion risks, highlighting that RSE workers, unbanked communities, and culturally cash reliant users may be disproportionately impacted by the proposal. In particular, vulnerable customers may be excluded or pushed toward informal or higher risk services if the rule is not carefully designed.

68. Broader consultation would have helped us to better understand the nature and scale *of* the problem, the full range of options, and the impacts of the proposals. It would have been beneficial to understand the impacts on customers, particularly for known users of remittance services such as RSE workers and migrant communities.

Consultation with crypto ATM providers

69. The Ministry consulted New Zealand's two Crypto ATM providers on prohibiting crypto ATMs. The Ministry met with both operators to hear their views, issues and suggestions. Officials also presented on the work to the IAG as part of seeking feedback on the wider workstream.

70. Both LocalCoin and CoinFlip do not support a blanket ban of crypto ATM machines. In our engagement with one operator, they stated that 'cryptocurrencies are central to the growing digital economy and are increasingly recognised as a legitimate form of investment'. They consider that banning crypto ATMs will take away choice from everyday New Zealanders, reduce financial inclusion and could risk driving customers to unregulated alternatives such as offshore cryptocurrency exchanges.

71. This operator suggested alternative measures to a ban, including introducing a $10,000 transaction limit on cash payments for international fund transfer services. Other options included restricting the sharing of accounts, mandatory scam warnings, and increased monitoring of transactions.

Section 2: Assessing options to address the policy problem

What criteria will be used to compare options to the status quo?

72. The following criterion have been used to assess options:

[34] GoAML is a secure online tool, used by reporting entities to submit reports to the FIU.

Criterion	Description
Effectiveness	How well does the option prevent and dissuade criminal misuse of cash? Will the option safeguard customers from financial loss, fraud, exploitation, and prevent wider harm?
Predictability	Will the option provide clarity and certainty for operators, regulators and users? Is the option likely to change in the future?
Feasibility	Can the option be implemented easily or at great cost, risk, or disruption? This could be to the government, reporting entities or wider sector. Does this option enable the legitimate use of cash?
Proportionate	Does the option match the level of risk and align with a graduated regulatory approach? Is the option an appropriate way to deal with the problem? Does the option allow for penalties that are commensurate to the harm? Does the option support a coherent and consistent approach to similar behaviour?

What scope will options be considered within?

73. Ministerial direction has focused the scope of options considered. Officials were asked to analyse two specific TSOC MAG recommendations relating to cash-based money remitters and crypto ATMs.

74. The type of limit and any threshold value above which cash transactions are restricted has not been considered in this analysis. If progressed, the threshold will be set in in regulations.

What options are being considered?

Approach taken by RIS addendum

75. The options under consideration are split into activities: IFTs of remittances and conversion of virtual assets. Analysis is required for both as each activity involves different ML/TF risk factors, evidence of harm, and impacts on providers and customers.

76. Part A will analyse options responding to the misuse of cash via IFT of remittances. Options will focus on the form the restriction will take.

77. Part B will analyse options responding to the misuse of cash via virtual asset conversion. Options will focus on two sub-issues:

- the scope of the restriction (i.e. who or what is restricted from accepting cash payments); and
- the form the restriction will take (i.e. how to mechanically restrict cash payments).

Part A: Options responding to the misuse of cash via money remitters

Form of the restriction for international fund transfers of remittances

Option one – Status quo

78. The Act would continue to allow money remitters to accept cash for IFTs without limits. Regulators and law enforcement would continue to rely on other measures such as enhanced customer due diligence, sector supervision, and reporting requirements, to manage high risks from remitters.

79. Regulators and law enforcement continue to sanction remitters that do not comply with their obligations under the Act (e.g. to conduct customer due diligence) with civil or criminal penalties. Remitters that knowingly or recklessly facilitate money laundering can also be charged with money laundering under the Crimes Act.[35]

Option two – Limit cash transactions above threshold levels (Ministry preferred)

80. Option two would seek to make it harder and more expensive for criminals to operate. It would allow limits to be set in regulations on the amount of cash that a money remitter or person in trade (referred to going forward as remittance services) could accept for IFTs.

81. Option two would take an evidenced-based approach to setting the type and value of the cash-transaction threshold. Cash transaction limits could involve one total dollar transaction limit, daily or monthly limits, limits for specific customers (such as new customers), or a combination of these options. Any restrictions would aim to minimise the impact on legitimate use while still impeding criminal activities, informed by data on use, ML/FT risks, and harm to New Zealanders. If sufficient evidence arises that transaction limits are not mitigating the risks and harm of criminal misuse of remittance services, then regulations could be made to ban cash-based transactions entirely.

82. The limit would be supported by an offence and penalty that replicates the construction of the prohibition on certain cash transactions for high-value goods above a threshold in section 67A. Section 98 of the Act sets out defences for non-compliance with the Act and would also apply.

Option three – Prohibit cash transactions entirely

83. Option three would stop remittance service providers from accepting cash-transactions for IFT entirely. This prohibition would be a statutory ban in primary legislation.

84. As with option two, the prohibition would be supported by an offence and penalty, including a defence, that replicates the prohibition on certain cash transactions for high-value goods above a threshold in section 67A.

[35] See sections 243 – 245 of the Crimes Act 1961

How do the options compare to the status quo/counterfactual?

International funds transfer of remittances: what form should the restriction on cash transactions take?

	Status Quo	Option two: cash transaction limit set in regulation	Option three: prohibit acceptance of cash transactions in primary legislation
Effectiveness	0	+ Reduces the scale of harm from predicate offending and money laundering by limiting cash remittances. Option provides the ability to ban in future if appropriate. Penalties for non-compliance provide deterrent effect and enforcement options.	+ Comprehensively reduces harm from predicate offending and money laundering by prohibiting cash remittances. Requires users to go through more traceable methods. Penalties for non-compliance provide deterrent effect and enforcement options. Increases displacement risks, as customers may use more underground means for moving money and potentially increase the level of harm.
Predictability	0	- Lower certainty for remittance providers and customers, as future changes to the threshold or potential prohibition remain possible. Aligns approach with similar cash-based risks, such as persons in trade of precious metals or stones.	+ Higher certainty for remittance providers and customers due to a clear and stable prohibition on accepting cash. Implementing a prohibition without consultation increases uncertainty and lack of clarity for other reporting entities.
Feasibility	0	- Disruption and cost impacts for industry. Legitimate use of cash-based remittances could continue. Increased costs could be transferred to customer through increased fees. Transaction limits would reduce some of the sector's vulnerability to misuse, potentially leading to positive changes for the 'de-banked' community. Requires primary and secondary legislation changes, but relatively easy to implement.	- - Significant disruption to industry; some cash-based remitters will no longer be operationally viable. Legitimate users may lose access to a required cash-based financial service. Inconsistent with wider policy considerations on the legitimate use of cash. Lengthy implementation may enable cash operators to transition to digital networks (bank dependant). Requires primary legislation, but easy to implement.

	Status Quo	Option two: cash transaction limit set in regulation	Option three: prohibit acceptance of cash transactions in primary legislation
		A clear threshold provides a more enforceable offence. Regulators and law enforcement focus resourcing efforts on the threshold limit.	A clear threshold, such as ban, provides a more enforceable offence.
Proportionate	0	++ Appropriate to set a prohibition limit as the sector is high risk and there is some evidence of harm. Allows limits to be set at levels that enable legitimate users to still make cash remittances. Penalties are significant but commensurate to the high risk and harm. Most aligned with a risk-based and graduating regulatory approach. Regulation could still be made to ban cash transactions where appropriate and proportionate to risk.	- - Whilst sector is high risk and there is evidence of harm, there are also many legitimate and low-risk users. A blanket ban with significant penalties raises proportionality concerns given the presence of significant legitimate and low-risk use. Not in line with a graduated regulatory approach or the existing prohibition settings. The option encourages the use of less regulated services as there is legitimate need and would likely result in displacement. New Zealand would be the first among comparator jurisdictions to implement this approach.
Overall assessment	0	+ Option two provides a regulatory tool to reduce money laundering risk while preserving legitimate use of cash. Limits can be adapted over time in response to changes in risk and allow low-value transfers to continue for users who rely on cash-based remittance services. Provides a flexible and proportionate approach to managing risk and responding to evidence of harm.	-- Option three would significantly reduce money laundering risk by prohibiting cash-based remittance transactions. However, it would restrict legitimate access to cash-based remittance services, including for migrant and Pacific communities, and may shift activity to informal or unregulated channels. The absence of regulatory flexibility also limits the ability to calibrate the response over time.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

85. Option two is the Ministry's preferred form for a restriction on cash transactions for IFTs of remittances. It would limit persons in trade from accepting cash above a threshold.

86. The Ministry considers option two directly targets criminal misuse by increasing the cost, effort, and exposure of transferring criminal funds. Criminal actors are likely to split up transactions or engage repeatedly, increasing fees, reducing efficiency, and raising the likelihood of detection by supervisors and the NZFIU.

87. Option two preserves legitimate use of cash-based remittances by allowing low-value IFTs to continue, supporting migrant and Pacific communities, RSE workers, and others who rely on cash-based remittances. This approach is more consistent with international comparators, where complete bans on cash-based remittances do not feature, and supports continued public confidence in the AML/CFT system. It will be important to consult the public to ensure the threshold value supports legitimate use.

88. A key strength of option two is its flexibility. Setting cash transaction limits through regulations enables thresholds to be adjusted over time in response to emerging risks, supervisory experience, and evidence of harm. This allows for escalation, including a move to tighter limits or a prohibition, if circumstances change, while avoiding premature over-regulation where domestic evidence does not yet support it.

89. Option two also supports a more coherent offences and penalties framework for high-risk cash transactions. By introducing limits on cash transactions above threshold levels for IFTs, the option aligns the treatment of remittances with existing prohibitions on high-value cash transactions in other high-risk sectors, such as precious metals. This promotes proportionality and consistency across sectors that present comparable money laundering risks and reduces the risk of criminal activity being displaced from one lightly regulated cash-based sector to another. A more aligned framework for offences and penalties also supports New Zealand’s obligations under the FATF standards.

Feedback from other government agencies

90. NZ Police supports restricting cash transactions above a limit for IFT by money remitters.

91. DIA acknowledges the potential benefit of a limit and notes that it would incorporate the threshold into its supervision of the sector, in accordance with a risk-based approach.

92. MBIE supports enabling cash transaction limits through regulations rather than imposing a blanket ban, as this better preserves legitimate use while allowing the regime to respond to risk. MBIE noted that threshold design will be important to minimise impacts, particularly for migrant and Pacific communities, RSE workers, unbanked users and small providers where de-banking limits access to non-cash alternatives.

93. The Ministry for Pacific Peoples have advised that remittance plays a critical role for Pacific peoples supporting families and communities overseas, including participants in the RSE scheme and holders of Accredited Employer Work Visas. Restrictions on cash-based transfers may reduce the ability of some users to remit funds, potentially increasing financial hardship, and affecting labour mobility and foreign policy objectives. Any new restrictions should preserve access to lawful and practical rchannels as there is a risk that activity shifts toward informal or less regulated channels where banking infrastructure is limited. The overall impact will depend on how transaction thresholds are calibrated in practice and new offences and penalties imposed, including how they apply across transactions and users.

Part B: Options responding to the misuse of cash via virtual asset conversion

Sub-issue 1: Scope of the cash transaction restriction on virtual asset conversion

94. Sub-issue one considers options for the scope of the restriction (i.e. who or what is restricted from accepting cash payments).

Option one: Status quo

95. Option one would maintain the status quo and not introduce any restriction on the conversion of cash into virtual assets.

Option two: Targeted restriction applied to crypto ATMs

96. Option two would apply a restriction on cash transactions only to crypto ATM machines, as agreed in-principle by Cabinet. Operators would be required to either remove machines (in the case of a prohibition) or ensure that machines only accept cash payments up to a specified threshold.

Option three: Preventative restriction applied to specified virtual assets in regulation (Ministry preferred)

97. Option three would restrict the amount of cash that a person in trade could accept for conversion into virtual assets, as specified in regulation. The option targets the conversion of cash into virtual assets directly, rather than the specific technology or business model used. This allows regulations to be updated in response to changes in technology, access methods, risks and evidence of harm.

98. Regulations would specify cryptocurrencies as within scope, thereby capturing cash-to-virtual-asset conversion facilitated through crypto ATM machines.

99. By applying to all persons in trade, the restriction would capture a broader range of activity, including actors outside the VASP sector. For example, option three would capture a money remitter who converts virtual assets for cash from their own wallet.

100. Exemptions are available for low-risk providers where appropriate. Under the Act, Cabinet and the Minister can issue exemptions from AML/CFT obligations based on criteria, including the risks posed by the applicant's business.

Option four: Restriction applied to specified virtual assets in primary legislation

101. Option four would specify virtual assets, or classes of virtual assets, subject to the restriction in primary legislation. Cryptocurrencies are proposed initially given their current accessibility for cash conversion.

102. The option would enable Parliament to respond to changes in access, risk and evidence of harm. It also reflects that not all virtual assets can be purchased with cash or present significant ML/TF risks. Virtual assets such as tokenised financial assets operate within identity-verified environments that do not pose the same high risks as cryptocurrencies.

103. As with option two, exemptions could be granted for genuinely low-risk providers where appropriate.

How do the options compare to the status quo/counterfactual?

Virtual asset conversion: What scope should the restriction on cash-transactions have?

	Status Quo	Option two – crypto ATMs only	Option three – restriction applicable to all virtual assets in primary legislation (narrowed in regulation)	Option four – restriction applicable only to virtual assets specified in primary legislation
Effectiveness	0	+ Reduces current crypto ATM misuse; limited control over displacement to new cash-conversion services and technology. Option takes targeted approach, capturing concerning use of technology identified by domestic case studies. Treats crypto ATM machines as the sole enabler of cash-for-cryptocurrency transactions, which may become out-of-date quickly. Does not constrain cash-for-virtual asset conversion. Greater likelihood of displacement of harm if new methods of cash-to-virtual-asset conversion emerge outside the scope of the prohibition.	++ Reduces current and future misuse and manages displacement through technology-neutral scope More effective at addressing current and emerging methods of converting cash into virtual assets. Technology neutral approach mitigates displacement of criminal misuse in the future enabled by new technology. Broad definition of virtual assets would automatically apply to new cash-based virtual assets. Regulations provide faster tool to enable supervisors and law enforcement to respond quickly to criminal misuse.	+ Reduces misuse for listed assets only; effectiveness declines as new assets or access methods emerge Option captures identified high-risk virtual assets, supported by some domestic case studies. Specifying virtual assets in the Act could result in legislative lag and an enforcement gap in the future that is vulnerable to misuse. Focus of prohibition is less centred on risks from cash and behaviours of organised criminals, which are highly adaptive. Greater likelihood of displacement of harm into other virtual assets in the future.
Predictability	0	**0** Comparable to the status quo for providers and customers. The option would be clear to providers, customers, and supervisors that scope of restriction would apply to crypto ATM machines. Certainty may diminish if new cash-for-virtual asset technologies	- Lower initial predictability for providers and customers until regulations specify scope. Certainty improves once regulations are made. 'Virtual asset' is already defined in regulations.	- Higher initial certainty and clarity for providers and customers, as virtual assets in scope are explicitly listed in primary legislation. Predictability reduces over time if legislative amendments are needed. Likely to change in future.

	Status Quo	Option two – crypto ATMs only	Option three – restriction applicable to all virtual assets in primary legislation (narrowed in regulation)	Option four – restriction applicable only to virtual assets specified in primary legislation
Predictability continued	0	develop outside the scope of the restriction. Unlikely to change in future but potentially could become not fit-for-purpose.	Primary legislation provides clarity that restriction could apply to all virtual assets that are converted by cash. Likely to change in future.	
Feasibility	0	- Increased costs and disruption on crypto ATM providers dependent on the form of the restriction. Some costs to Government agencies supervising and enforcing the restriction. The value of the limit threshold will determine whether users can legitimately use cash. Operationally simple to implement and enforce, given the small number of operators and physical locations of ATM machines. Construction of the option better supports a total ban of ATMs than a value limit.	- More complex to implement initially, but more sustainable in long-term for regulators to maintain fit-for-purpose restriction. Officials are not aware of other VASPs beyond the crypto ATM sector that offer cash-for-virtual asset conversion. Lack of public consultation prevents certainty that no one else will be affected. The option consequently is likely to have the same disruption and cost impact as option two. Option potentially minimises chilling effects on the market from a restriction, particularly for lower-risk or innovative digital-asset activities that do not share the same AML/CFT risk profile.	- Operationally simple to implement, but less adaptable over time for regulators. Repeated legislative amendment may be necessary to reflect changes in technology, access, or risk. Disruption and cost impacts are similar to options two and three. Aligns with the existing prohibition, where high-value goods are specified in legislation. However, virtual assets have enhanced risks as they are emerging fast-developing technology that can also be pseudo-anonymous. High-value goods are physical items long-established to retain value. Option may best minimise chilling effects on the market as the specific types of assets are already defined in primary legislation.
Proportionate	0	**0/+** Option implements a targeted approach, partially aligned to identified risks.	++ Option implements a preventative graduated regulatory approach.	+ Option supports a graduated regulatory approach. Aligned with currently identified risks, but less capable of

	Status Quo	Option two – crypto ATMs only	Option three – restriction applicable to all virtual assets in primary legislation (narrowed in regulation)	Option four – restriction applicable only to virtual assets specified in primary legislation
Proportionate continued	0	Targets crypto ATMs but under-captures other cash-to-virtual asset methods, increasing displacement risk. Not yet informed by developed domestic evidence base of harm. Significant risk that alternative providers will emerge to fill the gap of ATMs. Those 'persons in trade' would be out of scope of the prohibition and evade accountability. The construction of the prohibition (as above) means the offence is out of step with the approach to cash in other high-risk areas, enabling an incoherent system that encourages displacement. The option is arguably less appropriate for a strict liability offence as the prohibition is disconnected from the problem definition. The option captures the provision of technology rather than the act of accepting cash and transferring it internationally.	Most closely aligned with identified risks, by targeting the conversion of physical cash into virtual assets, while allowing lower-risk activity to be excluded through regulatory scope. Not yet informed by developed domestic evidence base of harm. Broad preventative scope assessed as appropriate and proportional given it is responding to the highest AML/CFT risks. Excluding virtual assets that do not present comparable AML/CFT risks, potentially reduces negative outcomes for market growth. Including 'those in trade' in scope would coherently mitigate risks of displacement and enable commensurate offences and penalties for equivalent behaviour. As the option's preventative approach is driven by risk rather than by evidence of harm, setting a calibrated threshold value or enabling some legitimate use could mitigate proportionality concerns.	remaining proportionate as technologies and access models evolve. Not yet informed by developed domestic evidence base of harm. The targeted scope supports coherence with other parts of the AML/CFT framework and allows the restriction's offences and penalties to be commensurate to risks of harm. Potential to provide criminals opportunities to take advantage of new retail cash-for-virtual asset options in the future due to regulatory lag. By being reactive, some criminals could avoid accountability despite exhibiting equivalent behaviour. As with option two, the option avoids imposing equivalent regulatory burdens on activities that do not present comparable AML/CFT risks, potentially reducing negative outcomes for market growth.
Overall assessment	0	**0/+** Option two is narrowly scoped, providing short-term clarity. Displacement risk increases as new cash-conversion technologies and services emerge.	**++** Option three best balances effectiveness and proportionality, enabling a future-resilient restriction focused on cash-to-virtual-asset conversion.	**0** Option four offers upfront certainty but is less adaptable to technological change and vulnerable to regulatory lag over time.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

104. Option three is the Ministry's preferred scope for a restriction on cash transactions for virtual asset conversion. It would apply a restriction to the acceptance of cash by persons in trade for conversion into virtual assets, rather than to a specific technology or asset class, with the virtual assets in scope specified through regulation.

105. The Ministry considers option three directly targets the source of risk: the conversion of physical cash into internationally transferable virtual assets. By focusing on cash-to-virtual asset conversion, the option reduces opportunities for criminal actors to circumvent controls by shifting between different service providers or access methods.

106. A key advantage of option three is its ability to manage displacement risk and remain effective as technology evolves. By focusing on the activity rather than the delivery mechanism, it ensures similar risks are treated consistently across sectors and reduces the likelihood that gaps can be exploited as business models change. This provides a more effective and durable response than a technology-specific approach.

107. The option enables targeted and proportionate implementation through regulation. While the primary power is broad, regulations would confine the restriction to virtual assets that can be directly purchased with cash and present the highest ML/TF risk (such as cryptocurrencies). This safeguard limits unnecessary impacts on lower-risk activities while reducing compliance costs and preserving legitimate market activity.

108. While option three introduces some initial uncertainty until regulations are finalised, this can be managed through clear regulatory scoping and consultation. Over time, the ability to adjust scope through regulation supports a regime that remains fit for purpose as risks and technologies evolve.

109. Any potential chilling effect or market uncertainty associated with a broader enabling power can be mitigated through clear regulatory design, consultation, and the use of exemptions for genuinely low-risk providers. The restriction applies only to transactions involving physical cash, which is the highest-risk entry point, and does not affect most legitimate virtual asset activity conducted through non-cash channels.

110. On balance, option three delivers the highest net benefits over time. It improves the effectiveness and resilience of the AML/CFT system, manages displacement risk, and allows controls to evolve in line with emerging technologies and evidence of harm, while maintaining proportionality through targeted regulatory design.

Feedback from other government agencies

111. New Zealand Police supports widening the scope to capture virtual assets where a cash-transaction limit is applied (refer to problem two).

112. DIA supports applying the definition of virtual assets to broaden the scope of the restriction.

113. MBIE considers the choice between options three and option four to be finely balanced. Both address displacement risk more effectively than a crypto ATM specific approach. Option three provides greater flexibility to respond to new cash-to-virtual asset models but creates greater uncertainty for VASPs and consumers, and may have a wider chilling effect on adjacent digital-asset activity if the scope is not clearly confined. Option four provides greater upfront certainty by specifying the affected virtual assets in primary legislation, and may better align the primary legislation with the current evidence base.

Sub-issue 2: Form of the cash transaction restriction on virtual assets

114. Sub-issue two considers the form the restriction would take (i.e. how cash payments are restricted).

Option one: Status quo

115. The Act would continue to allow persons in trade, including crypto ATM providers, to accept cash in exchange for virtual assets. Regulators and law enforcement would rely on existing AML/CFT obligations, reporting requirements, and general criminal offences to manage risks.

116. Additional requirements could be introduced through regulation-making powers, including new information collection and due diligence requirements.36 However, these measures are unlikely to mitigate the key risks associated with virtual assets, including wallet pseudo-anonymity and wallet-sharing practices.

117. Offences and penalties available to regulators and law enforcement correspond to non-compliance with requirements in the Act and general criminal offences in the Crimes Act.[37]

Option two: Restrict cash transactions to above threshold levels (Ministry preferred)

118. Option two would restrict the amount of cash that a person in trade can accept in exchange for virtual assets, making it more difficult and costly for criminals to exploit these services.

119. The option would enable regulations to set out:

- the virtual assets subject to restriction (e.g. cryptocurrencies, stable-coins);
- the circumstances in which restrictions would apply (e.g. tighter restrictions could apply for new customers); and
- the dollar thresholds, above which cash-based transactions would be restricted.

120. Regulations would need to be informed by data on legitimate use, ML/TF risks and evidence of harm to New Zealanders and calibrated to minimise impacts on legitimate users while reducing criminal misuse.

121. Under this proposal, regulations could be made to ban cash payments for some or all types of virtual assets where evidence shows limits are insufficient.

122. The limit would be supported by offences and penalties, including a defence, that aligns with the existing prohibition on high-value cash transactions under section 67A.

Option three: Restrict cash transactions entirely

123. Option three would ban a person in trade from accepting cash payments for virtual assets (or a class of virtual assets) entirely. This option would be included in primary legislation and supported by the same offences and penalties as option two.

[36] Section 30(b) of the Act enables the Government to prescribe further requirements to mitigate the risks of technologies that might favour anonymity via regulations.
[37] See sections 243 – 245 of the Crimes Act 1961

How do the options compare to the status quo/counterfactual?

Virtual asset conversion: What form should the restriction on cash transactions take?

	Status Quo	Option two – cash transactions limit set in regulation	Option three – prohibit acceptance of cash transactions in primary legislation
Effectiveness	0	+ Reduces the scale of harm from predicate offending and money laundering by limiting the acceptance of cash to convert virtual assets. Option provides the ability to ban in future if appropriate. Penalties for non-compliance provide deterrent effect and enforcement options.	++ Comprehensively reduces harm from predicate offending and money laundering by prohibiting the acceptance of cash to convert virtual assets. Requires users to go through more traceable methods. Penalties for non-compliance provide deterrent effect and enforcement options. Increases displacement risks, as customers may use more underground means for moving money and potentially increase the level of harm.
Predictability	0	- Less certainty for crypto ATM operators, VASPs and persons in trade as operations could either continue, continue with a limit, or be prohibited. Also, less clear for customers. Aligns approach with similar cash-based risks, such as persons in trade of precious metals or stones.	- Provides certainty that the sector cannot accept cash, even if the impact on a business is to wind down operations. Risks creating an environment where other high-risk sectors become concerned that their services will also be banned, potentially negatively impacting market.
Feasibility	0	- Crypto ATMs operating in New Zealand already impose daily limits on transactions (at $9,500) so thresholds can be imposed. Setting lower thresholds will entail disruption and costs for industry. Legitimate use could continue. Operators already charge high fees for use of crypto ATM machines. Increased costs could be transferred to customer. Requires primary and secondary legislation changes, but relatively easy to implement.	- Significant disruption and costs to industry from removal of crypto ATM machines. Legitimate users may lose access to a required cash-based financial service. One year implementation period provides New Zealand's two providers sufficient lead in time to phase out operations. A clear threshold, such as complete restriction, provides a more enforceable offence.

	Status Quo	Option two – cash transactions limit set in regulation	Option three – prohibit acceptance of cash transactions in primary legislation
Feasibility continued	0	A clear threshold supports a more enforceable offence. Regulators and law enforcement to focus resourcing efforts on the threshold limit.	
Proportionate	0	++ Allows regulators to take a graduated enforcement approach to high-sector risk, while reflecting limited evidence of harm. Proportionality depends on thresholds being calibrated to target higher-risk transactions. Thresholds could be lowered (potentially to zero) or multiple thresholds could apply to minimise harm (for example, daily and weekly limits or limits for new users), if evidence shows this is necessary to mitigate risk and harm. Regulations allow limits higher-risk transactions be set while still enabling controlled legitimate use. Penalties are significant, in order to be proportionate to the high sector-risk of misuse by transnational criminals, but better supported by safeguards.	-- The penalties under section 67A are significant to reflect the high sector-risk of misuse by criminals. Applying section 67A-level penalties to this option raises proportionality concerns given limited domestic evidence of harm. The option takes an approach to the misuse of cash that will be inconsistent with cash payments in other high-risk sectors (such as remittance) and does not allow for a graduated response that can be calibrated to differing levels of risk and misuse.
Overall assessment	0	++ This option provides additional regulatory tools to limit the harms that vulnerable people are exposed to. Limits could be adapted in response to changes in risk, whilst still enabling the provision of services. Ultimately, cash transactions for high-risk virtual assets could be banned if sufficient evidence of harm emerges. Provides adaptable tools to manage risk while preserving some legitimate use.	- This option would do the most to minimise harm from cash payments for virtual assets and would ban Crypto ATM operators. However, there is still limited domestic evidence to suggest this option is proportionate.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

124. Option two is the Ministry's preferred form for a restriction on cash transactions for virtual asset conversion. It would introduce limits on cash transactions above threshold levels through regulation.

125. Option two directly targets the risk associated with higher-value cash transactions used to convert into virtual assets. By limiting the amount of cash that can be accepted, the option increases the cost and frequency of transactions, making transaction patterns more observable to supervisors and law enforcement and increasing the likelihood of detection. Overall, the option makes it more difficult for criminal actors to move illicit funds.

126. A key advantage of option two is that it enables a graduated, risk-based response. Thresholds can be calibrated to target higher-risk transactions while allowing controlled legitimate use and can be adjusted over time in response to changes in risk and evidence of harm, up to and including a prohibition where necessary. This provides a more proportionate and adaptable response than an immediate ban.

127. Option two also provides a more proportionate penalty framework. While offences and penalties are necessary to deter non-compliance, applying maximum penalties equivalent to a full prohibition may not be commensurate with the current domestic evidence base. A transaction-limit approach ensures penalties remain aligned with risk, while still allowing escalation if warranted.

128. Although some criminal misuse is likely to persist, option two increases the overall cost, risk, and difficulty of laundering cash through virtual assets, without displacing activity as significantly as a full prohibition. It also avoids the immediate disruption to legitimate users and businesses associated with a ban.

129. On balance, the Ministry considers option two delivers the highest net benefits by strengthening the effectiveness of the AML/CFT regime while maintaining proportionality and enabling a graduated regulatory response. It provides the tools to constrain higher-risk cash transactions now, while retaining the flexibility to respond to increasing evidence of harm over time, including through increasingly tighter limits or a prohibition if warranted.

Feedback from other government agencies

130. New Zealand Police supports a full ban on Crypto ATMs. They have expressed concern that the daily thresholds and enhanced CDD requirements set in some jurisdictions have done little to mitigate the risks inherent in Crypto ATMs.

131. DIA acknowledges the potential benefit of a limit and notes that it would incorporate the threshold prohibition into its supervision of the sector, in accordance with a risk-based approach.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

132. Yes, the Minister's preferred options in the Cabinet paper is the same as the Ministry's preferred option.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	**Comment**	**Impact**	**Evidence Certainty**
Additional costs of the preferred option compared to taking no action			
Reporting entities	**One-off and ongoing** One off and ongoing compliance costs to update AML/CFT programmes, systems, and staff training. Potential revenue loss for remittance providers reliant on higher-value cash transactions. Higher impacts on crypto ATM operators, including possible exit from the market and loss of sunk investment. Regulatory adjustment costs associated with threshold and scope updates over time. Potential for bank de-risking	Medium	Medium - High
Legitimate customers	**Ongoing** Reduced access to cash-based remittance or virtual assets above the threshold. Possible increases in transaction costs or inconvenience. Risks that Pacific communities, migrants and seasonal workers relying on remittance services are disproportionately impacted, particularly where access to non-cash alternatives is limited.	Low-medium	Low - medium
DIA (single supervisor)	**One-off and ongoing** One-off implementation costs for guidance, training, and supervisory updates. Ongoing supervision, investigation, and enforcement activity.	Low–medium	Medium
NZ Police	**One-off and ongoing** Increased demand for financial-intelligence analysis and prosecution support. Possible increase in investigation workload for cash-based non-compliance.	Low–medium	Medium
Department of Corrections	**Ongoing** Any increase in prison population for non-compliance is likely to be minimal (less than 1). The Department of Corrections has advised: “this is one of a wider suite of policy proposals that could increase the prison population, which, when considered collectively, could have funding implications for the Crown. This relates to both the operational costs for each additional prisoner (of $120,000 per prisoner per annum), and the infrastructure requirements for the prison	Low	Low

	network, which already has very limited capacity and low resilience.”		
Courts	**Ongoing** New prosecutions for non-compliance with cash-transaction limits.	Low	Medium
Others	**Ongoing** Risk of activity shifting to less visible, illegal or offshore services if poorly implemented, particularly where banking infrastructure in destination countries is limited. Residual money laundering risk remains.	Low – medium	Low - medium
Total monetised costs		N/A	N/A
Non-monetised costs		Medium	Medium
Additional benefits of the preferred option compared to taking no action			
Reporting entities	Clear statutory basis to refuse high-risk cash transactions. Greater consistency in managing cash-based AML/CFT risk.	Low	Low
Legitimate customers	Indirect benefits from reduced criminal misuse of cash-based services. Improved integrity and trust in remittance and financial services.	Low	Low
DIA (single supervisor)	Improved ability to deter and disrupt high-risk cash-based money laundering activity.	Medium	Medium
NZ Police	Improved ability to disrupt organised crime and the offshore movement of criminal proceeds.	Medium	Medium
Department of Corrections	No additional benefits to the status quo.	N/A	Low
Courts	No additional benefits to the status quo.	N/A	Low
Others	Reduced downstream harm from money laundering and predicate offending. Supports international confidence in New Zealand’s risk-based AML/CFT framework.	High	Low-medium

	Protection of international reputation and capital flows.		
Total monetised benefits		N/A	N/A
Non-monetised benefits		High	Low - Medium

Section 3: Delivering an option

How will the proposal be implemented?

133. As indicated in the main RIS, the Government intends to s9(2)(f)(iv) which is intended to enable reporting entities to become familiar with the changes and make the necessary transition.

134. Proposals will require regulations be developed to set the transaction limit value, prescribe virtual assets in scope, and infringement penalties. Officials intend for regulations to be developed, publicly consulted, and in force at the at the same time as the Bill is passed in s9(2)(f)(iv)

135. A potential unintended consequence of transition period is that virtual assets, particularly cryptocurrencies, and IFT of remittances will continue to be misused by criminals until the proposals become operational. Agencies will continue to prioritise intelligence and supervisory activity during this period to partially mitigate the risks from the transition period.

136. DIA officials currently consider the money remittance and VASP sectors as its highest risk sectors and applies significant supervisory resource to them. This will continue through until the proposal is enacted to ensure the risks are mitigated as best possible. For the money remittance sector, this is also supported by a National Strategy work programme item to establish a cross-agency coordination mechanism to combat money remitters actively avoiding regulatory oversight.[38]

How will the proposal be monitored, evaluated, and reviewed?

137. As indicated in the main RIS, New Zealand will undergo a MER in 2028/29 which will comprehensively evaluate our AML/CFT system for both effectiveness and technical compliance with Recommendations. The MER, and our subsequent rating by the FATF, will be an early indication of the impact of these proposals and where there might still be gaps or improvements.

138. The prohibition will be integrated into existing AML/CFT regulatory supervision arrangements. Supervisors and New Zealand Police will monitor compliance trends and reporting, enforcement activity, and indicators of displacement through routine monitoring and intelligence sharing. Where necessary, additional data on cash-based transactions and compliance outcomes may be collected to support monitoring

[38] Anti-Money Laundering and Countering Financing of Terrorism Work Programme, 2026 – 2030, see page 3.

139. Any requirements set in regulation will require ongoing monitoring. This includes the list of specified virtual assets and any limits or thresholds supporting a restriction on cash-transactions. Where noteworthy changes in risk, legitimate use and harm are identified in relation to the proposals, officials will provide advice to the Minister and Cabinet, as provided for in the Act, to ensure regulations remain fit-for-purpose. Reporting entities and other stakeholders impacted by the proposals will be able to raise system issues and apply for any exemptions through established channels.

140. MBIE noted in their feedback that implementation should monitor whether restrictions increase prices, reduce service availability, or displace activity into informal or higher-risk services.

Problem two: weak enforcement responses across the non-compliance spectrum

Section 1: Diagnosing the policy problem

What is the context behind the policy problem and how is the status quo expected to develop?

Key information from the main RIS

Less serious and straight-forward non-compliance

141. The main RIS assessed two options to expand intermediary enforcement tools under the AML/CFT Act; an infringement offence scheme and an administrative offence regime. It concluded that an infringement regime best addressed the policy problem to fill the enforcement gap, providing tools to sanction less serious and straight-forward non-compliance with the Act. [39]

Serious non-compliance

142. The main RIS assessed three high level options for addressing serious non-compliance:

1) increasing the maximum fines and penalties to bring them into line with comparable domestic regimes;
2) introducing a penalty unit system which would use penalty units to calculate maximum fines; and
3) tying penalties to another factor such as the size of the business or the commercial gain from offending.

143. The main RIS concluded that options one and three would best address serious non-compliance with AML/CFT obligations.[40]

Cabinet agreed to strengthen enforcement responses across the non-compliance spectrum in 2025

144. On 30 June 2025, Cabinet agreed to introduce a power, to be given effect through secondary legislation, to develop an infringement offence scheme for acts of non-compliance with the Act [CAB-25-MIN-0225 refers].

145. Cabinet also agreed in principle to:

[39] See page 66 of the main RIS
[40] See page 71 of the main RIS

- increase maximum penalties (financial and imprisonment) for civil pecuniary penalties and criminal penalties in line with those in comparable domestic regimes to ensure penalties are proportionate and dissuasive in all instances; and

- enable the maximum civil pecuniary penalties and criminal financial penalties to be the greater of the prescribed maximum fine, a multiple of commercial gain or percentage of turnover to ensure penalties are proportionate and dissuasive in all instances.

146. Cabinet agreed that final decisions on penalty levels would be sought when a draft Bill is presented to Cabinet for introduction to the House of Representatives.

But infringements offences will now be included in primary legislation

147. Parliamentary Counsel Office (PCO) have advised their drafting preference is to include the specific acts or omissions constituting an infringement offence in primary legislation. While fees for each individual infringement offence will continue to be progressed in secondary legislation.

148. Cabinet will make final decisions on the which infringement offences should be included in the Bill at the same time as it considers the final Bill ahead of introduction of the AML/CFT statutory reform package.

What is the policy problem or opportunity?

149. Reporting entities have core obligations under the AML/CFT Act that are designed to protect the integrity of New Zealand's financial system and to disrupt money laundering and terrorism financing (ML/TF). Effective compliance with these obligations depends on supervisors having access to proportionate, graduated, and dissuasive sanctions that reflect the seriousness of non-compliance and the risks presented.

150. The current AML/CFT framework does not provide supervisors and law enforcement with a sufficiently flexible or graduated enforcement toolkit across the full spectrum of non-compliance. Consequently, supervisors are constrained in their ability to respond proportionately, escalate enforcement in a way that promotes sustained compliance, and consistently across the full spectrum of non-compliance. This reduces deterrence, weakens the overall effectiveness of the enforcement framework, and increases the risk that harmful conduct persists or escalates.

151. For serious non-compliance, existing maximum penalties do not adequately reflect the severity of the conduct and may lack sufficient deterrent effect, particularly for larger or multinational reporting entities such as banks or casinos. Many penalty levels have remained unchanged since 2009 and have not kept pace with inflation, evolving risks, or comparable regulatory regimes, diminishing compliance incentives over time.

152. This problem is compounded when non-compliance is repeated, regardless of whether it occurs at the lower or higher end of the severity spectrum. Further, as criminal activity becomes more complex and better resourced, static and outdated penalty settings further reduce the deterrent effect of enforcement action and limit the practical options available to the courts.

153. The following case study demonstrates an example of concerning behaviour that falls into the enforcement gap for serious non-compliance.[41]

[41] SkyCity Casino Management Limited

Illustrative case study: New Zealand penalties compared to international benchmarks

Current penalty levels risk New Zealand being seen as a weaker link in the international community. Comparable jurisdictions, including Australia, Canada and the United Kingdom allow the implementation of significantly larger penalties.

In 2024 Australia imposed an AUD $67 million penalty on SkyCity Adelaide, whereas DIA was only able to obtain an NZD $4.16 million penalty to SkyCity in New Zealand for similar non-compliance.

154. For less serious and straightforward instances of non-compliance, available responses are often limited to formal warnings or resource-intensive civil or criminal proceedings, which can be disproportionate and may discourage timely intervention. As a result, supervisors face an enforcement gap for conduct that falls between these thresholds, where a warning may be ineffective, but court proceedings would be unnecessary.

155. The following case study demonstrates an example of concerning behaviour that falls into the enforcement gap for less serious non-compliance:

Illustrative case study: Failure to file an annual report by the specified deadline

The annual report is a strict requirement for all businesses with obligations under the Act and is an important product for the AML/CFT supervisors to understand the risks attached to its regulated population. A reporting entity must file their annual report by the specified deadline under s 60 of the Act

As the annual report is a clearly defined requirement for businesses, a formal warning or enforceable under-taking can be an insufficient response to non-compliance with section 60. This is particularly so for reporting entities that have failed to do so multiple times. However, the next available option for the supervisors to address this non-compliance would be to take proceedings against businesses for committing a civil liability act under section 78. The penalty for non-compliance includes a term of imprisonment of not more than two years and a fine of no more than $300,000 for an individual or a fine of up to $5 million dollars for a body corporate.

The Ministry considers such action is an inappropriate use of court resources and while the penalty may be dissuasive, we do not consider that the penalty level is a proportionate response to this type of non-compliance.

156. International and domestic reviews have identified these weaknesses. The 2021 Financial Action Task Force (FATF) Mutual Evaluation and 2022 Statutory Review acknowledged the Act does not currently provide AML/CFT supervisors with an effective and proportionate response to non-compliance.

157. Without intervention, less serious but persistent non-compliance could continue without effective sanction. For more serious non-compliance, some reporting entities may continue to treat penalties as a cost of doing business rather than a deterrent. Law enforcement agencies may continue to prioritise cases involving the highest available penalties, resulting in some charges not being brought or being deprioritised where alternative offences with stronger penalty settings are available.

Policy opportunity

158. The main RIS has already considered the problem definition for problem two. Cabinet has agreed to introduce an infringement regime for less serious and straightforward non-compliance and to increase penalties for serious non-compliance.

159. This RIS addendum provides further options to deliver Cabinet's direction to strengthen the Act's offence and penalty settings, which require consideration.

What objectives are sought in relation to the policy problem?

160. As outlined in the main RIS, the work programme seeks to meet three high-level policy objectives:

- Ensuring the AML/CFT system is effective in meeting the purposes of the AML/CFT Act.
- Reducing unnecessary compliance costs for businesses.
- s9(2)(d)

161. Additional objectives are sought in relation to problem two:

- Improving the possible responses to non-compliance to be more proportionate, dissuasive and effective.

What consultation has been undertaken?

162. The main RIS outlines the consultation undertaken on whether to include an infringement offence and penalty regime in the Act, and whether and how to increase penalties for the top-end of seriousness.[42]

Less serious and straight-forward non-compliance

163. The timeframes for preparing the infringement offences for inclusion in the Bill did not allow for consultation beyond DIA and New Zealand Police, due to PCO preference to include the offences in primary legislation during drafting. A further limitation is that the proposed offences were not consulted with LDAC due to these time constraints; however, this is partially mitigated as each offence was tested against the Cabinet-approved LDAC framework and with DIA.

164. DIA has been closely consulted on the design of the offences, given its role as AML/CFT supervisor responsible for administering infringement notices and its sector expertise in identifying offences that are workable and appropriate.

165. The Ministry consulted the IAG early in policy development on potential infringement offences. However, the final list has since changed significantly. The updated list was re-shared with the IAG as part of consultation on the draft Amendment Bill, which ran for two weeks and focused on identifying any major unintended technical implications ahead of Cabinet consideration.

Serious non-compliance

166. The timeframes for preparing the penalty levels for inclusion in the Bill did not allow for consultation beyond DIA and New Zealand Police.

167. The Ministry has also consulted the IAG on the increased maximum and variable penalty levels where non-compliance is motivated by financial gain, as part of consultation on the draft Amendment Bill. However, industry was not consulted on early policy proposals.

[42] See page 12 of the main RIS

Feedback from the IAG on offences and penalties

168. Reporting entities on the IAG supported reforms that strengthen the effectiveness, proportionality and impact of the enforcement regime but noted there needed to be checks and balances.

169. One bank expressed concern in relation to the amendments to section 74 which clarifies the ability of penalties to be applied per instance of offending. While not directly related to the issues in this RIS, the concern noted the importance of adhering to the double jeopardy rule and not encouraging responses to non-compliance that are disproportionate with the offending.

170. The same bank also sought clarity on how enforcement options would interact in circumstances where more than one enforcement option could be applied at once. For example, where a penalty is applied for breach of a civil liability act is paired with a referral of non-compliance to a relevant licensing authority. Businesses are still liable for only one financial penalty for instances of non-compliance. However, the Supervisor will continue to be enabled to progress non-financial enforcement options to address non-compliance. This supports a proportionate and graduated enforcement approach within the AML/CFT system.

171. One law firm raised general concerns about the proposed offences and penalties in the Bill. They noted they would pay particular attention to whether the construction of the offences and penalties in the final version would include *mens rea* elements and have defences available, such as a 'reasonable excuse' defence. In the table at Appendix Five, officials have identified *mens rea* and defences despite not being the focus of this RIS. Further, we note that section 98 provides a general defence to obligations in Part 2 of the Act, and this section is not amended by the Bill.

Section 2: Assessing options to address the policy problem

Approach taken by RIS addendum

172. The criteria, scope and options for problem two are structured into two parts to reflect the different regulatory responses required to achieve the policy objective. These include:

    a) Part A considers options for an infringement regime to address less serious and straightforward non-compliance.

    b) Part B considers options to amend penalty levels to address serious non-compliance, including where non-compliance is for commercial gain.

173. Less serious and more serious non-compliance require different responses within a graduated enforcement framework. More serious conduct requires stronger penalties to meet FATF expectations that sanctions be effective, proportionate, and dissuasive. In contrast, infringement offences provide a more appropriate tool for addressing less serious non-compliance and straightforward non-compliance.

Part A: Responding to less serious and straightforward non-compliance

What criteria will be used to compare options to the status quo?

174. The following criterion have been used to assess infringement offences:

Criterion	Description
Workable	Whether the infringement offence can be operationalised and used in the circumstances for which it is intended; avoids undue complexity, uncertainty, or burden for regulators and industry; and aligns with existing limitation periods, evidentiary thresholds, and procedural requirements.
Appropriate	Whether the infringement offence is addressing less serious and straightforward non-compliance that does not justify criminal or civil sanctions; is consistent with legislation guidelines, (e.g. LDAC and Cabinet guidance) and broader justice principles, including proportionate penalties and an efficient justice system?
Effective	Whether the infringement offence fills an identified enforcement gap, provides a credible, timely, and dissuasive enforcement option, and supports a graduated and risk-based approach to enforcement.

What scope will the options be considered within?

175. The Ministry developed a framework to ascertain the scope for possible offences for inclusion in the infringement regime. Our framework involved:

- Identifying known deficiencies in the AML/CFT system. Consideration was given to obligations of the Act that were often breached by reporting entities but lacked a proportionate and efficient response. We focused on non-compliance that is typically considered minor contraventions of the law and would go otherwise unaddressed by the Supervisors.
- Comparing similar domestic infringement schemes. For example, the Financial Markets Conduct Act 2013 (FMCA) creates similar obligations for specific reporting practices, reporting deadlines and record keeping requirements that are similar to obligations in the AML/CFT Act.
- Comparing options against infringement offences in Australia, as a comparable foreign jurisdiction. While reliance on overseas legislation is not always appropriate[43], officials have taken this approach given both countries operate under the same FATF standards. Many affected reporting entities in New Zealand, such as banks, are Australian-based and already subject to similar obligations, so alignment reduces compliance complexity across jurisdictions.

What options are being considered?

Option one – Status Quo / Counterfactual

176. Option one would maintain the status quo, with no infringement offence regime introduced under the Act. This would leave an enforcement gap for less serious and straight forward non-compliance with AML/CFT supervisors relying on existing tools that are not proportionate or effective in all circumstances.

177. As a result, less serious non-compliance would continue to be addressed using measures that do not provide appropriate or dissuasive responses.

[43] The Legislation Design and Advisory Committee at Chapter 24, Creating criminal offences.

178. The AML/CFT regime would also remain less aligned with FATF expectations, increasing the risk that at New Zealand's next mutual evaluation we may receive lower ratings on both the technical compliance and effectiveness standards relating to AML/CFT supervisor powers and enforcement.

Option two – Introduction of an infringement offence regime (Ministry preferred)

179. Option two would introduce an infringement offence regime, outlined in **Appendix One.**

180. The option would provide supervisors with an additional enforcement tool to respond to less serious and straightforward non-compliance under the Act. The option addresses areas where existing tools are not well suited or where non-compliance occurs frequently and is difficult to address proportionately.

181. The 12 offences are designed to cover a range of existing obligations under the Act, including areas that affected by the statutory reforms outlined in the main RIS.

How do the options compare to the status quo/counterfactual?

	Option One – Status Quo	Option Two – Introduction of an infringement offence regime
Workable	0	++ Offences consulted with DIA to ensure they will be usable from a supervisory perspective. Offences have been designed to be consistent with related legislative mechanisms (e.g. the Summary Proceedings Act 1957) to ensure that they are enforceable and viable in New Zealand's wider legislative framework. Offences have been designed to be interoperable with existing infringement scheme mechanisms required to operationalise the infringement scheme.
Appropriate	0	++ The offences have been considered against the LDAC framework and designed to address straight forward questions of fact on minor contraventions of the law that are/or are likely to be committed in volume. The proposed offences have been considered in the wider context of the Act to ensure that align with its intent and purpose. The offences are clearly defined and will not create new or unduly burdensome requirements on businesses with obligations under the Act.
Effective	0	++ Enables responses to non-compliance from smaller reporting entities and in instances where court involvement is not warranted but a response beyond a formal warning/censure is desired. Increases certainty of consequences of non-compliance (where otherwise responses beyond formal warnings are not wanted) and therefore increases dissuasiveness.

	Option One – Status Quo	Option Two – Introduction of an infringement offence regime
		Proposed offences have been designed from a holistic approach to the Act that acknowledges a wide range of areas where non-compliance can occur.
Overall assessment	0	++

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

182. The Ministry's recommended option is to progress option two, which introduces the specified infringement offences. Option two equips the infringement regime with a set of clearly defined offences that can be readily operationalised by supervisors to address non-compliance in the identified enforcement gap. The option enables supervisors to respond appropriately to less serious and straightforward non-compliance across the full range of obligations under the Act.

183. The offences have been designed to align with existing legislative frameworks and LDAC guidance, ensuring they are workable in practice and address minor contraventions that occur in volume, without creating new and difficult to understand obligations.

184. Officials consider the proposed infringement offences best support a proportionate and effective offence and penalty framework, better aligning the Act with its broader objectives and international compliance expectations.

Is the Minister's preferred option in the cabinet paper the same as the agency's preferred option in the RIS?

185. Yes, the Minister's preferred option in the Cabinet paper is the same as the Ministry's preferred option.

Part B: Responding to serious non-compliance

186. Part B considers options to amend penalty levels to address serious non-compliance, including where non-compliance is for commercial gain.

What criteria will be used to compare options to the status quo?

187. The following criterion have been used to assess serious non-compliance.

Criterion	Description
Proportionate	Does the option allow for penalties that are commensurate to the harm? Does the option make sense within the wider legal framework? Does the option support a coherent and consistent approach to similar behaviour?
Dissuasive	Does the option support sanctions sufficiently significant to outweigh any perceived benefit from non-compliance or criminal behaviour?

Effective	Does the proposed change enable the AML/CFT Act to meet its purposes, by changing behaviour and ensuring compliance? Does the proposal align with international best practice?

What scope will the options be considered within?

188. The scope of options for consideration has been limited by Cabinet decisions to:

- whether to increase the penalties in the Act to ensure they are proportionate and dissuasive in all instances; and
- if penalties should be increased:
  - what level they should be increased to; and
  - whether the maximum penalty should be set as a percentage of commercial gain or total revenue.

What options are being considered?

Option one – Status Quo / Counterfactual

189. Option one would maintain the current penalty settings for civil and criminal non-compliance under the Act, with no change to existing maximum penalties. As a result, penalties may remain insufficient to address more serious non-compliance in all cases.

190. This would be partially mitigated by reforms agreed to by Cabinet in 2025, which will allow monetary penalties to be applied per instance of non-compliance, enabling more proportionate responses to repeated or systemic breaches. However, these changes do not ensure that penalties are consistently proportionate and dissuasive, nor do they achieve Cabinet's objective of aligning penalty settings with comparable domestic regimes.

Option two – Increasing penalties for more serious non-compliance, including variable financial penalties (Ministry preferred)

191. Option two would update penalty settings for civil and criminal non-compliance under the Act to ensure they are proportionate, effective, and dissuasive. This includes increases to maximum fines and, where appropriate, maximum terms of imprisonment.

192. The option introduces variable financial penalties for certain offences, allowing fines to be set as the greater of a fixed amount or a proportion of commercial gain or turnover. This enables penalties to better reflect the scale and seriousness of offending, particularly for large reporting entities, and supports proportionate and dissuasive responses to serious non-compliance.

193. Penalty changes are targeted to provisions that require alternative means of setting a dissuasive penalty, particularly where the size of a reporting entity and the scale of non-compliance necessitate it. Commercial gain penalties are proposed for provisions where stronger deterrence is required against conduct undertaken for financial benefit.

194. To summarise the changes, option two involves:

- 17 increases to maximum fines to retain their dissuasiveness and alignment with other penalties.
- 9 increases in the maximum term of imprisonment.
- 12 variable financial penalties of up to 300 per cent of commercial gain and/or 10 per cent of turnover.

195. Further detail, including rationale, on the specific changes to penalties are available in **Appendix Five.**

How do the options compare to the status quo/counterfactual?

196. Options analysis is set out below.

	Option one – Status Quo	**Option two – Inclusion of proposed offences**
Proportionate	0	+ Penalties have been consistent with comparable statutory regimes that govern complex and regulated financial behaviour (e.g. the Financial Markets Conduct Ac). Variable fines allow penalties to match serious offences by very large reporting entities, ensuring that non-compliance with the Act cannot be deemed a 'cost of doing business'. The risk of disproportionately large penalties is mitigated by the experience of New Zealand courts in applying similar variable fines regimes in similar contexts (e.g. the Commerce Act1986).[44]
Dissuasive	0	+ Connecting maximum penalties to the gain resulting from the non-compliance or turnover helps deter reporting entities from breaching their AML/CFT obligations for financial gain, even where the potential gains are highly significant. When imposing sentences the courts have regard to the maximum penalty available, so increasing penalties will result in more appropriate sentencing for serious and criminal non-compliance. The offences have been considered against the LDAC framework which notes that in a commercial context it may be appropriate for variable fines (e.g. linked to commercial gain).
Effective	0	+

[44] The Law Commission has noted that a New Zealand court is unlikely to ever impose excessively disproportionate penalties with commercial gain formulations. A $12 million pecuniary penalty was imposed on Telecom for breach of section 36 of the Commerce Act 1986, however a potential maximum of $279.2m could have been imposed.

		The proposed penalties have been considered in the wider context of the Act to ensure that penalties are consistent with the seriousness of the offences and the purpose of the Act. Provides a more complete toolkit for reporting entities to respond to a wide range of non-compliance, thereby more strongly incentivising compliance with the regime. Variable fines are not impacted by inflation, ensuring they continue to incentivise compliance over the long-term.
Overall assessment	0	+

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

197. The Ministry's recommended option is to progress option two and amend the full list of penalties set out in Appendix Five. These penalties will modernise the AML/CFT regime, align it with other comparable domestic regimes, and ensure that law enforcement are able to apply appropriately dissuasive and proportionate penalties to the most serious cases of non-compliance.

198. If New Zealand does not modernise the penalties in the Act, serious non-compliance will continue to not be treated as such. Penalties will continue to be small in comparison to our closest partners such as Australia and the United Kingdom (where penalties for serious non-compliance are typically much larger than in New Zealand). This could have consequences both in terms of how reporting entities view the consequences of non-compliance, and for how the FATF scores New Zealand's AML/CFT penalties system in our next mutual evaluation.

199. The FATF standards for both technical compliance and effectiveness establish that AML/CFT supervisors should be equipped to impose appropriate and proportionate penalties for non-compliance. Our offence and penalties regime will be directly assessed at our next mutual evaluation. Implementing the preferred option helps bring New Zealand in to line with the FATF standards by addressing deficiencies identified in our previous mutual evaluation and the 2022 Statutory Review of the Act. s9(2)(d)

200. The proposed penalty framework builds on the existing approach in the Act, under which imprisonment is available for some offences where a mental element is not required (i.e. strict liability). In developing these proposals, officials have not further extended the duration of imprisonment to strict liability offences. This is because the absence of a *mens rea* element reduces the level of culpability associated with the conduct, meaning that financial penalties alone are a more proportionate response.

Is the Minister's preferred option in the cabinet paper the same as the agency's preferred option in the RIS?

201. Yes, the Minister's preferred option in the Cabinet paper is the same as the Ministry's preferred option.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	Higher maximum and variable penalties may affect compliance and risk management behaviour, requiring increased investment in governance, oversight, and compliance systems. Indirect costs may vary by entity size and maturity, potentially affecting pricing, service availability, competition, and innovation, with smaller entities more likely to face proportionately higher impacts.	Medium	High
Regulators	Minor administrative cost for infringement regime. This includes service and publication of infringement and reminder notices. Increases in penalties are unlikely to make a significant difference as the processes for applying penalties will remain unchanged.	Low	High
Others (eg, wider govt, consumers, etc.) *For fiscal costs, both increased costs and loss of revenue could be relevant*	Indicative estimates suggest one person per year could be sentenced to prison for serious non-compliance offences, at a cost of $120,000 per prisoner per year. Estimates also suggest an average of three people being prosecuted per year. Higher penalties may increase the likelihood of contested enforcement action, with associated costs for NZ Police (litigation costs), Crown prosecutors, the Public Defence Service and the courts (including legal aid). No expected increase in the volumes of proceedings, though a greater proportion of cases will now possibly be heard in the High Court, instead of the District Court, given the increase in penalty levels. Increased penalties may lead banks to regard some services as higher compliance risk, potentially contributing to further de risking if settings are not implemented in a proportionate and genuinely risk-based manner. Additional/new offences may require small additional investigative resource. Additional costs to Ministry front-line teams responsible for operationalising the infringement scheme. Expected volumes to be minimal given officials estimate no more than 1000 infringement notices would be issues by DIA each year.	Low	Medium
Total monetised costs	N/A	N/A	N/A

Non-monetised costs		Low	Low
Additional benefits of the preferred option compared to taking no action			
Regulators	Regulators better equipped to proportionately and effectively address non-compliance.	Low	Medium
Courts	Alternative action out of courts will save Court costs. Reduced costs from not bringing court proceedings, proving the elements of the offence, and by issuing infringement notices. Increased range of offences will enable greater alternative action.	Low	Medium
Others (eg, wider govt, consumers, etc.)	The fee collected from infringements would be payable to the Crown Bank Account rather than to the enforcement body. Ensures offences are proportionate and dissuasive in light with international standards.	Low	Medium
Total monetised benefits	N/A	N/A	N/A
Non-monetised benefits		Low	Medium

Section 3: Delivering an option

How will the proposal be implemented?

202. For information on how the reforms will be implemented, please see section three of the main RIS.[45]

203. DIA advises it will leverage its existing infringement regime under the Gambling Act 2003 to implement the infringement regime. This includes established processes for issuing, managing, and enforcing infringement notices. Decisions to issue infringements are made individually in accordance with policies and following discussion at an internal oversight panel. Recipients will retain their existing rights to dispute or appeal infringement notices.

204. Infringement fees will be introduced through regulations. Officials intend for these regulations to be developed and publicly consulted s9(2)(f)(iv)

How will the proposal be monitored, evaluated and reviewed?

205. For further information on monitoring, please see section three of the main RIS.[46]

206. Monitoring of the infringement scheme will be undertaken by DIA, working in coordination with the Ministry of Justice. DIA advises that existing processes includes monitoring the extent to which the different infringement offences are applied over time, to determine their effectiveness as a response to non-compliance (compared to other enforcement options available).

[45] See page 89 of the main RIS
[46] See page 90 of the main RIS

Appendix One: Proposed list of Infringement offences

No #	Trigger	Offence
1	Commencement as a reporting entity	Failure to have an AML/CFT compliance programme in writing upon commencement as a reporting entity (excludes high-value dealers)
2	Commencement as a reporting entity	Failure to have an appointed AML/CFT compliance officer on commencement as a reporting entity.
3	Commencement as a reporting entity	Failure to have a risk assessment in writing on commencement as a reporting entity.
4	Reporting deadline	Failure to provide an annual report by the required date under section 60 of the Act.
5	Formation of a DBG	Failing to notify the supervisor in writing within 30 days of a lead entity of a DBG (on formation)
6	Changes to a DBG	Failing to notify the supervisor in writing of withdrawal, termination or changes to a DBG.
7	Audit deadline	Failure to provide a copy of an independent evaluation of a risk assessment or AML/CFT programme when required under section 59B(5)
8	Request for independent audit	Failure to provide a copy of an audit of a risk assessment or AML/CFT Compliance programme conducted in the applicable timeframe (as required under s59(2)) if required under s 59B(5) or s 132(2)(a) of the Act.
9	On notice under s 132(2)(a)	Failure to produce verification records of a person's identity (as required to be kept by s 50(2) of the Act) under notice pursuant to s 132(2)(a) of the Act.
10	On notice under s 132(2)(a)	Failure to produce records relating to a business relationship (as required to be kept by s 51(a) or (c) of the Act) under notice pursuant to s 132(2)(a) of the Act.
11	On notice under s 132(2)(a)	Failure to produce records relating to a transaction (as required to be kept by s 49(1) of the Act) under notice pursuant to s 132(2)(a) of the Act.
12	On-site inspection	Failure to provide information that the AML/CFT supervisor reasonably requires for the purpose of an on-site inspection conducted under s 133(2) of the Act.

Appendix Two: Introduction of variable fines for civil and criminal conduct

No #	Current maximum penalty	Proposed maximum amendment	Rationale for proposed amendment
1	**Section 78 / 90** Civil liability acts Individual • Section 90(2): $100,000 pecuniary penalty (for s78(b), (c), (d) or (g)) • Section 90(3): $200,000 pecuniary penalty (for s78(a), (da), (e), (f) or (h)) Body corporate/partnership • Section 90(2): $1,000,000 pecuniary penalty (for s78(b), (c), (d) or (g)) • Section 90(3): $2,000,000 pecuniary penalty (for s78(a), (da), (e), (f) or (h))	**Section 90(2) and (3)** Individual The greater of: • $500,000 pecuniary penalty; or three times the value of any gain resulting from contravention Body corporate/ partnership: The greater of: • $5,000,000 pecuniary penalty; or • Three times the value of any gain resulting from contravention; or 10% of turnover	The MER noted civil pecuniary penalties are low relative to the seriousness of noncompliance. Aligning with comparable domestic regimes will ensure appropriate penalties can be applied to larger reporting entities and serious breaches, encourage compliance, and avoids compliance costs being treated as a cost of doing business. Courts retain discretion to apply proportionate penalties within statutory limits. This proposal aligns penalties for s90(2) with s90(3) of the Act, simplifying civil liability provisions. Consolidating penalties and leaving assessment to the Court supports consideration of all relevant factors. The new penalty levels also aligned with comparable provisions in the Financial Markets Conduct Act 2013 (FMCA). Civil liability acts [e.g. failing to conduct customer due diligence (CDD) or adequately monitor accounts] may enable commercial gain (e.g. by maintaining business relationships that otherwise would not occur). In such cases, commercial gain penalties are appropriate. The general defence in section 98 remains available for obligations in Part 2 of the Act.
2	**Section 91 / 100** Criminal liability for civil liability acts where non-compliance is committed with a knowing or reckless state of mind Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Four years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or • Three times the value of any gain resulting from contravention; or 10% of turnover	The rationale mirrors s90(2) above, the amendment ensures penalties for non-compliance are proportionate, dissuasive, and effective. It aligns maximum financial penalties for criminal offending with civil breaches of the same conduct, while reflecting the additional element of intent. The penalties remain appropriate given the potential for imprisonment. The increase is broadly consistent with FMCA offences e.g. insider trading has a criminal maximum of 5 years imprisonment/$500,000 for an individual and $2.5m fine for a body corporate, and a civil maximum of $1m for an individual or $5m for a body corporate. Civil liability acts may enable commercial gain. In such cases, variable penalties are appropriate. The general defence in section 98 remains available for obligations in Part 2 of the Act.
3	**Section 92 / 100** Failing to report suspicious activity. Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Four years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or • Three times the value of any gain resulting from contravention; or 10% of turnover	Submitting Suspicious Activity Reports (SARs) is central to detecting and investigating ML/TF. The proposed increase aligns with other AML/CFT requirements under section 91, and comparable provisions, and similarly serious conduct, in the FMCA and the Commerce Act (e.g. knowingly failing to comply with financial reporting standards and contravening disclosure requirements). The increase reflects the intentional nature of offending. Section 92 incorporates *mens rea* into the *actus reus*, which requires the reporting entity to have formed a suspicion but failed to report it within three working days, inferring knowledge of the obligation. Failing to report suspicious activity could enable commercial gain. In such cases, variable penalties are appropriate. A specific defence, covering information believed to be privileged, is available.
4	**Section 93 / 100** Knowingly provide false or misleading information relating to SARs/PTR Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Four years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or • Three times the value of any gain resulting from contravention; or 10% of turnover	Providing false/misleading information impairs criminal investigations under multiple statutes. Higher penalties would better reflect the seriousness of offending and its impact on communities. Police have commented that they continue to see cases where reporting entities intentionally fail to report suspicious activities for profit. This increase would keep penalties consistent with criminal liability for other AML/CFT requirements under section 91, for comparable misconduct, and broadly for comparable misconduct in other domestic regimes such as the FMCA. Providing a false or misleading statement in relation to suspicious activity or prescribed transaction reporting could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. The general defence in section 98 remains available for obligations in Part 2 of the Act.
5	**Section 94 / 100** Knowingly make unlawfully disclosure of SARs/PTRs Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Four years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or • Three times the value of any gain resulting from contravention; or 10% of turnover	This offence relates to tipping off. Tipping off allows criminals to alter their behaviour, conceal or destroy evidence, and flee or escape detection before or during an investigation This increase would keep penalties consistent with criminal liability for other AML/CFT requirements under section 91. This conduct is no less serious than s91 offences and broadly with comparable conduct under the FMCA and the Crimes Act. Making an unlawful disclosure in relation to an investigation in relation to suspicious activity or prescribed transaction reporting could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. The general defence in section 98 remains available for obligations in Part 2 of the Act.
6	**Section 95 / 100** Failure to keep or retain SAR/PTR records Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Two years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or	As this offence is strict liability, we consider increasing imprisonment inappropriate. The lower proposed imprisonment term reflects the lack of *mens rea* element. This small change aligns with proposed s100 increases. Failure to keep records is a civil liability act with penalties under s90 and 100. Intentional failure to keep or retain SAR records could still be prosecuted and would entail penalties of up to four years in prison (see above). Section 100 penalties are justifiably larger given the mental element.

No #	Current maximum penalty	Proposed maximum amendment	Rationale for proposed amendment
		• Three times the value of any gain resulting from contravention; or 10% of turnover	Failing to keep or retain suspicious activity or prescribed transaction records could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. The general defence in section 98 remains available for obligations in Part 2 of the Act.
7	**Section 96 / 100** Obstructing investigation relating to SAR/PTR Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Four years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine or • Three times the value of any gain resulting from contravention; or 10% of turnover	This increase would keep penalties consistent with criminal liability for other AML/CFT requirements under section 91. Obstructing an investigation can frustrate investigations, enable continued criminal activity, and undermine crime-fighting efforts. Increasing the maximum penalty allows the courts to apply greater penalties for the most serious instances of offending and aligns us with comparable domestic and international regimes. Section 96 is a strict liability offence with a proposed increase for the term of imprisonment. *Mens rea* is not provided for in section 96 as it is in sections 102 and 111, which provides for 'wilful' obstruction of the AML/CFT supervisor or answering questions from a Customs officer. Officials consider the *mens rea* element of the offence could be amended to align with the other obstruction offences. Defence of 'without lawful justification or excuse' available.
8	**Section 97 / 100** Contravention of 47(1) or 48A(1) (disclosure of information relating to SARs and PTRs) Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Two years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or • Three times the value of any gain resulting from contravention; or 10% of turnover	As this offence is strict liability, we consider increasing imprisonment inappropriate. The lower proposed imprisonment term reflects the lack of *mens rea* element. Disclosing information of suspicious activity in proceedings or failing to report certain prescribed transactions could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. Defence of 'without lawful justification or excuse' available.
9	**Section 101 / 105(1)** Structuring transactions Individual: • Two years imprisonment; and/or $300,000 fine Body corporate/partnership: • $5,000,000 fine	Individual: • Five years imprisonment; and/or $500,000 fine Body corporate/ partnership: • $5,000,000 fine	Raising the penalty for individuals to $500,000 and imprisonment to 5 years better brings penalties into line with market manipulation and insider trading which we consider most comparable offending. It also better reflects the seriousness of this conduct. This offence is one of the most serious in the Act. The offence does not include the same actus reus as the money laundering offence, however, the resulting harm can effectively be the same. The act of the structuring offence may occur where money laundering has been successful, but where there is not enough evidence to trace back to the predicate offence. Proposed increases reflect the intentional nature of offending. Section 101 incorporates *mens rea* elements into the construction of the prohibited conduct. It needs to be proven that structuring is carried out to avoid application of AML/CFT requirements. This infers the reporting entity has knowledge that they are not complying with their obligations. Penalty settings should be at the upper end within the AML/CFT Act given comparable seriousness of this offence to ensure consistency and proportionality across the Act.
10	**Section 102 / 105(2)** Wilfully obstructing AML/CFT Supervisor Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	Individual: • One year imprisonment; and/or $100,000 fine Body corporate/ partnership: • $1,000,000 fine	Obstructing the supervisor seeks to undermine the purpose of the Act. We consider the current penalties considerably out of alignment with comparable offences/penalties under the AML/CFT Act, and comparable regimes. Proving the *mens rea* standard is challenging and provides inherent protections against non-intentional actions. Proving 'wilfully' and 'knowing that' are not straightforward and requires proof that the person knew what they were doing when the obstructed or provided false or misleading information. NB: This increase would extend to the new offences relating to the Financial Intelligence Unit and section 143 of the Act [CAB-25-MIN-0225 refers].
11	**Section 103 / 105(2)** Knowingly provide false or misleading information to AML/CFT Supervisor Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	Individual: • One year imprisonment; and/or $100,000 fine Body corporate/ partnership: • $1,000,000 fine	Providing false or misleading information seeks to undermine the purpose of the Act. We consider the current penalties considerably out of alignment with comparable offences/penalties under the AML/CFT Act, and comparable regimes. Proving the *mens rea* standard is challenging and provides inherent protections again non-intentional actions. Proving 'wilfully' and 'knowing that' are not straightforward and requires proof that the person knew what they were doing when the obstructed or provided false or misleading information. Defence of 'without reasonable excuse' available.
12	**Section 67A / 105A** Accepting cash transaction above a thresholds for high-value goods Individual: • Two years imprisonment; and/or $300,000 fine Body corporate / partnership: • $5,000,000 fine	Individual: • Two years imprisonment; and/or $500,000 fine Body corporate/ partnership: The greater of: • $5,000,000 fine; or three times the value of any gain resulting from contravention.	As this offence is strict liability, we consider increasing imprisonment inappropriate. The lower proposed imprisonment term reflects the lack of *mens rea* element. This aligns with increases to section 91: criminal liability for civil liability acts. This change supports the amendments relating to the use of cash and the high-risk nature of cash. It supports the changes made to make cash a less attractive option and deter the use of cash for illicit activities by, in conjunction with changes in problem one, deterring cash-related offending. Accepting cash transactions above a threshold for high-value goods could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. The general defence in section 98 remains available for obligations in Part 2 of the Act.

No #	Current maximum penalty	Proposed maximum amendment	Rationale for proposed amendment
13	**Section 106 / 112** Failure to report cash moved into/out of New Zealand Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	**Mirror Customs and Excise Act s 25** Individual: • Three months imprisonment; and/or The greater of: • $20,000 fine; or three times the value of any gain resulting from contravention. Body corporate/ partnership: The greater of: • $100,000 fine; or three times the value of any gain resulting from contravention.	As this offence is strict liability, we consider increasing imprisonment inappropriate. The lower proposed imprisonment term reflects the lack of *mens rea* element. This will bring penalties into alignment with the Customs and Excise Act s25 (providing a false/misleading report on inbound goods). This change supports the amendments relating to the use of cash and the high-risk nature of cash. It supports the changes made to make cash a less attractive option and deter the use of cash for illicit activities by, in conjunction with changes in appendix two, deterring cash-related offending. Failing to report cash moved into/out of New Zealand could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. Defence of 'without reasonable excuse' available. Further defence in section 109 available.
14	**Section 107 / 112** Failure to report cash received in New Zealand from overseas Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	**Mirror Customs and Excise Act s 25** Individual: • Three months imprisonment; and/or The greater of: • $20,000 fine; or three times the value of any gain resulting from contravention. Body corporate/ partnership: The greater of: • $100,000 fine; or three times the value of any gain resulting from contravention.	As this offence is strict liability, we consider increasing imprisonment inappropriate. The lower proposed imprisonment term reflects the lack of *mens rea* element. This will bring penalties into alignment with the Customs and Excise Act s25 (providing a false/misleading report on inbound goods). This change supports the amendments relating to the use of cash and the high-risk nature of cash. It supports the changes made to make cash a less attractive option and deter the use of cash for illicit activities by, in conjunction with changes in problem one, deterring cash-related offending. Failing to report cash received in New Zealand could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. Defence of 'without reasonable excuse' available. Further defence in section 109 available.
15	**Section 108 / 112** Structuring cross-border transportation of cash Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	**Mirror Customs and Excise Act s389** Individual: • Six months imprisonment; and/or The greater of: • $20,000 fine; or three times the value of any gain resulting from contravention. Body corporate/ partnership: The greater of: • $100,000 fine; or three times the value of any gain resulting from contravention.	This will bring penalties into alignment with the Customs and Excise Act s389 (knowingly importing or exporting prohibited goods). Section 108 makes it an offence to structure cross-border transportation of cash to avoid the application of any AML/CFT requirements. Proposed increases reflect the intentional nature of non-compliance. As with section 101, the offence incorporates *mens rea* elements into the construction of the prohibited conduct. The Act requires prosecutors to prove that structuring is carried out to avoid the application of AML/CFT requirements. This construction infers knowledge that they are not complying with their obligations. This change supports the amendments relating to the use of cash and the high-risk nature of cash. It supports the changes made to make cash a less attractive option and deter the use of cash for illicit activities by, in conjunction with changes in appendix two, deterring cash-related offending. Structuring the cross-border transportation of cash received could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities.
16	**Section 110 / 112** Knowingly provide false or misleading info for cash report Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	**Mirror Customs and Excise Act s 351** Individual: • Three months imprisonment; and/or The greater of: • $20,000 fine; or three times the value of any gain resulting from contravention. Body corporate/ partnership: The greater of: • $100,000 fine; or three times the value of any gain resulting from contravention.	This will bring penalties into alignment with the Customs and Excise Act s351 (false or misleading statement intending to deceive). This change supports the amendments relating to the use of cash and the high-risk nature of cash. It supports the changes made to make cash a less attractive option and deter the use of cash for illicit activities by, in conjunction with changes in appendix two, deterring cash-related offending. Providing a false or misleading statement in relation to a cash report could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. Defence of 'without reasonable excuse' available.
17	**Section 111 / 112** Wilfully obstructing or not answering questions from Customs officer Individual: • Three months imprisonment; and/or $10,000 fine Body corporate/partnership: • $50,000 fine	**Mirror Customs and Excise Act s358** Individual: • Three months imprisonment; and/or The greater of: • $20,000 fine; or three times the value of any gain resulting from contravention. Body corporate/ partnership: The greater of: • $100,000 fine; or three times the value of any gain resulting from contravention.	This will bring penalties into alignment with the Customs and Excise Act s358 (failure to give Customs access to records). This change supports the amendments relating to the use of cash and the high-risk nature of cash. It supports the changes made to make cash a less attractive option and deter the use of cash for illicit activities by, in conjunction with changes in appendix two, deterring cash-related offending. Wilfully obstructing a Customs officer could enable commercial gain. In such circumstances, it is appropriate that commercial gain penalties may be applied to such profit-generating activities. Defence of 'without reasonable excuse' available.