The CASH Report

conversations around suspicious happenings

July 2024

New Zealand Financial Intelligence Unit

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

Message from the Manager, Financial Intelligence Unit

Dan Frost

Kia ora koutou,

After a hiatus, I am pleased to finally reveal the revised and renamed newsletter format to all of you!

Last year, the Financial Intelligence Unit (FIU) consulted a targeted audience to identify if this product was having the effect we wanted, primarily delivering relevant insights to promote awareness, and understanding of the AMLCFT risks to New Zealand (NZ).

We listened to the feedback and reviewed previous editions to gauge its effectiveness. The resulting outcome is what you now see in front of you.

Our aim is to publish The CASH Report bi-monthly—six publications per year— and provide relevant insights to the AMLCFT community, to forewarn and forearm the AMLCFT eco-system of new or emerging risks, and trends.

Last month, I was privileged to travel to the 30th Annual Egmont FIU Plenary, which was represented by approximately 180 heads of FIUs from around the globe. The key theme for this year's plenary was 'the FIU of the Future', which was conducted through several workshops over the duration of the Plenary.

It was great to renew relationships with NZ's traditional partners, develop new relationships with other FIUs, meet with other Heads of FIUs and discuss how we can work together as part of strengthening international relationships to combat money laundering (ML), financing of terrorism (FT) and proliferation financing (PF).

Key takeaways for me were seeing how many FIUs were making effective use of freezing powers as part of the Asset Recovery process; and how AI and ML is really critical to FIUs in the detection of illicit money flows, in particular frauds and scams.

The last theme was how cooperation between FIUs, law enforcement agencies both domestically and internationally, is a force multiplier to combat money laundering organizations and organised crime.

The most important underlying theme emanating from the Plenary, was that people are our most critical component to combatting ML/TF and PF. For without our people, we cannot prevent criminals and bad actors from causing harm to our communities.

In closing I thought it would be good to finish with a whakatuaki and one that reflects my editorial:

He aha te mea nui ki tēnei ao? Māku e ki atu. He tangata, he tangata, he tangata!

'What is the most important thing in the world? I say that it is people, it is people, it is people!'

CONTENTS

EDITORIAL STAFF

Executive Editor

Zane Verran

Managing Editor

SMJSH8

Conversations Around Suspicious Happenings

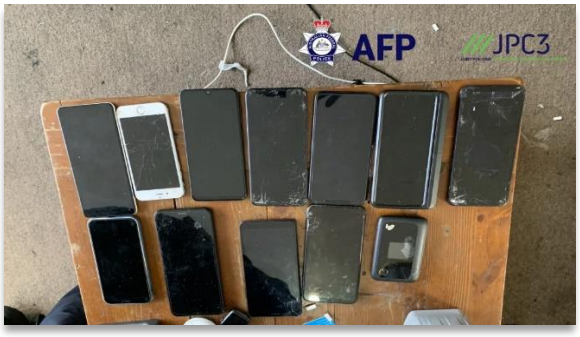
The Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act became law in October 2009. The Act's purpose is to detect and deter money laundering and contribute to public confidence in the financial system.

The CASH Report is produced by the Financial Intelligence Unit (FIU) as part of its obligations under section 142(b)(i) of the AML/CFT Act 2009. The *Report* comprises FIU holdings and open-source media reporting collected since the last edition.

The FIU is part of the New Zealand Police Financial Crime Group (FCG), and comprises the FIU, the Asset Recovery Unit (ARU), the Money Laundering Team (MLT), and Virtual Assets Team (VAT).

NEW ZEALAND AML/CFT NEWS

New Zealand Police target online scammers



Confiscated electronic devices allegedly used by the scammers.

Photo RNZ via Australian Federal Police

Between 14 and 17 April 2024, law enforcement authorities (LEAs) from 19 countries executed search warrants on individuals linked to the 'phishing kit' website LabHost. According to media, more than 40,000 fraudulent sites were created on the website, with subscribers (i.e. alleged offenders) paying monthly subscription rates for hosting and cloning services. Since its founding in 2021, it is estimated LabHost received more than NZ$2 million from subscriptions. New Zealand Police (Police) have so far identified three domestic suspects. The investigation remains on-going.

Relevance: *Online fraud and scams often involve money-laundering and terrorist financing methods because the illegally obtained funds are almost inevitably layered and reintegrated into the legitimate economy. 'Placement' has already occurred with the funds coming from legitimate sources.*

Operation Camperdown offers further evidence of the global characteristics of financial crime, and the importance for reporting entities to alert customers of scams.

NZ NEWS: HIGHLIGHTS

Search of 3 properties

leads to valuable electronic devices and documents seized in global operation
(page 2)

NZ$4.16m penalty

for AML/CFT breaches by SkyCity
(page 3)

JP guilty

of money laundering
(page 4)

NZ$100,000 seized

in Operations Scissor, Razor, and Snip
(page 3)

Police seize drugs and $100,000 cash

In May, Police executed four search warrants in Christchurch that led to the arrest of four people and the seizure of significant quantities of illicit drugs. These included MDMA, ketamine, LSD, cocaine, cannabis, and steroids. Electronic devices and NZ$100,000 in cash were also taken.

Relevance: *Proceeds from illicit drug sales, usually in the form of cash, are laundered into the mainstream economy by criminals. Seizure like this prevent potential destabilising effects to the financial system, including inflation. In small rural communities this can be particularly noticeable.*

SkyCity and Internal Affairs negotiate deal over AML/CFT breaches

On 21 May, Julian Cook, Chairman of SkyCity, acknowledged the company's breach of its AML/CFT obligations. This follows a 15-month Internal Affairs (DIA) investigation of SkyCity's AML/CFT compliance. DIA found breaches in the company's risk assessments; establishing, implementing, and monitoring AML/CFT compliance programmes; monitoring of accounts and transactions; enhanced customer due diligence; and termination of existing business relationships. A submission to the court for penalties totalling NZ$4.16 million has been tabled.

Relevance: *This case serves as a strong reminder that no matter the size, reputation, or type of operation, complying with AML/CFT obligations is a requirement for all reporting entities.*

Police seek 'million-dollar money mule'

Police are seeking the whereabouts of Ayom Wek, a 31-year-old they believe is based in Auckland Central. Wek is wanted in connection with an investigation into serious fraud involving term deposits scams worth around $1.8 million. Anyone with information should call 105 and cite reference number 240525/8716.

Relevance: *Money mules transfer or move illegally acquired money on behalf of someone else and may be unwitting, witting, or complicit in the criminal activity.*

Disgraced former JP laundered money for organised crime group

Source: New Zealand Herald. Photo/ Belinda Freak

Herbert Armitage, an 83-year-old former Justice of the Peace (JP), laundered over $520,000 in illegal proceeds from the manufacture and supply of methamphetamine for an organised crime group. According to the NZ Herald, Armitage laundered the money through "his own account, and an account he held power of attorney over which belonged to a woman in a rest home." Armitage had no prior convictions—often referred to as a 'Clean Skin'—and accepted cash deliveries from the criminal group's leader at his home. He then made 28 payments through six accounts to the criminal boss. He received over $100,000 as payment for his criminal actions.

Relevance: *The methodology displayed in this case is not novel, however the turning of a JP is particularly noteworthy. The organised crime group involved almost certainly intended for Mr Armitage's community standing and reputation to assist in masking the real source of the funds. Ultimately, this was not effective because risk-assessment tools, especially automated-versions employed by financial institutions, are designed to monitor all transactional activity. As someone with a prominent public function, a JP arguably falls under the definition of Politically Exposed Persons (PEP) according to international guidelines issued by the Financial Action Task Force (FATF). However, this differs from the interpretation provided by the AML/CFT Act 2009, under which a JP's function is likely excluded.*

POLi Payments likely invalidate banking guarantee

A recent Consumer NZ investigation revealed using POLi—a system that allows customers to pay merchants directly without the need for an intermediary such as VISA or Mastercard—will likely invalidate your banking guarantee due to breaches to your bank's terms and conditions. This potentially leaves customers more vulnerable because reimbursement rests on so-called 'Goodwill Gestures' by their bank. Indeed, using a third-party service, like POLi, could invalidate your bank's guarantee for all subsequent internet banking transactions. The key security issue for the banks is the need for customers to enter their login details, including their passwords, on POLi. Scammers can imitate the POLi website and dupe customers into clicking a false link, such as through an email or text, before eliciting them to enter sensitive information.

Relevance: *Australian banks stopped accepting POLi in 2023, partly over security concerns. New Zealanders using POLi, should consider reaching out to their banking provider for clarity. It should be emphasised that scammers also imitate the websites of banks, and as such, caution should be exercised when conducting any online transaction.*

INTERNATIONAL AML/CFT NEWS

European Union

The European Union adopts new package aimed at strengthening AML/CFT Efforts

Four key measures were adopted:

- Immediate, unfiltered, direct and free access, for people with legitimate interest, to beneficial ownership information held in national registries and interconnected at European Union (EU) level.
- Enhanced Due Diligence measures, including for top-tier professional football clubs.
- An EU-wide limit of €10,000 on cash payments.
- The creation of a new authority—the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)—to be based in Europe's financial capital, Frankfurt.

These form part of a wider AML/CFT package that also includes the Sixth AML Directive, and the EU 'single rulebook' regulation.

Relevance: *Monitoring EU efforts in the AML/CFT space offers an indication of global trends and accepted norms. As it concerns New Zealand, the most significant difference between these new EU measures and our domestic regime is the lack of a central Beneficial Ownership registry.*

INTERNATIONAL AML/CFT NEWS: HIGHLIGHTS

CFO arrested

in alleged US$67 million money laundering scheme
(page 9)

EU adopts new AML/CFT measures:

BO registries now available to the public
(page 5)

AU$67 million fine

For SkyCity Adelaide
(page 6)

CA$6 million fine

For crypto exchange Binance
(page 7)

The Netherlands

Independent ATMs present significant money laundering risks

The Dutch documentary television programme Zembla, in conjunction with several European newspapers, investigated the use of ATMs operated by independent companies. They revealed significant money laundering and terrorism financing vulnerabilities, including using non-certified cash transporters. According to their findings, non-bank affiliated ATMs are largely unregulated and can be used to 'wash' dirty money.

In response, Zembla received many responses from private and public agencies. This includes the Dutch FIU, which stated it had not conducted research on the matter due to a lack of substantive reporting.

Relevance: *A 2016 research paper into New Zealand's payment systems noted national ATM data did not include independent ATM operators. This is because this data is not collected by Payments NZ—a limited liability company governing Aotearoa's core payment systems, and whose shareholders are: ANZ, ASB, BNZ, Citibank, HSBC, Kiwibank, TSB Bank and Westpac.*

Australia

SkyCity Adelaide hit with massive penalty for AML/CFT breaches

On 17 May 2024, SkyCity Entertainment announced its Australian subsidiary, SkyCity Adelaide, had reached an agreement with the Australian Transaction Reports and Analysis Centre (AUSTRAC) to pay a penalty of AU$67 million for breaches of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CFT Act). SkyCity Adelaide admitted it breached S36 of the AML/CFT Act by not conducting ongoing Customer Due Diligence for certain high-risk customers and customers transacting through higher risk channels. Its AML/CFT Programme also contravened S81 of the AML/CFT Act by failing to meet requirements of the AML/CFT Act and AML/CFT Rules.

Relevance: *The announcement is significant for both the size of the penalty and the offender—SkyCity. The most common method to launder money through casinos is by opening an account and converting dirty money into tokens or chips and then withdrawing most of the cash shortly thereafter. Depending on the jurisdiction, casinos with a junket operator relationship offer more complex options to 'wash' money; however, following a Royal Commission in the Gambling sector by the Victorian Government in 2021 (here), alongside an earlier risk assessment into junket operations by AUSTRAC in 2020 (here), junket operations are now banned in most Australian casinos. SkyCity halted New Zealand junket tours in 2021.*

AUSTRAC has accepted an Enforceable Undertaking from Sportsbet Pty Ltd

Following a prolonged campaign into the corporate bookmaker sector, AUSTRAC has ordered Sportsbet to appoint an external auditor to examine its AML/CFT compliance regime. Sportsbet has determined the best possible means to ensure compliance is through an Enforceable Undertaking to AUSTRAC. The undertaking is binding, and Sportsbet must now comply with the ongoing remedial plan. Failure to adhere to it could see the matter brought to the Federal Court, which could then order the payment of financial penalties. The Australian judicial system has a history of stern gambling sector decisions; in 2017, Tabcorp was ordered to pay AU$45 million in penalties for contravention of the AML/CFT Act.

Relevance: *The New Zealand FIU does not possess the regulatory power for Enforceable Undertakings to ensure compliance. These are delegated to the three sector supervisors (under Section 81, 82, and 83 of the Anti-money Laundering and Countering Financing of Terrorism Act 2009).*

Canada

Largest Cryptocurrency Exchange hit with Administrative Penalty

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) imposed a CA$6 million (NZ$7 million) administrative penalty on Binance Holdings Limited.[1] The company failed to register as a foreign money services business, and failed to report large virtual currency transaction of CAN$10,000 or more in the course of a single transaction, together with the prescribed information as required under Part 1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations.

Relevance: *This is a good example of a business whose services have only recently been captured by AML/CFT regulations, but who should have known that their activities must comply with the legislation. The recent Phase Two AML/CFT updates in New Zealand—especially those around Virtual Asset Service Providers—are applicable in this case, and the relevant reporting entities should take notice.*

[1] The largest cryptocurrency exchange by trading volume, Binance was created in 2017 by Chinese-Canadian Changpeng Zhao. Zhao, who until recently served as the company's CEO, previously pleaded guilty to money laundering charges in the US and was sentenced to four months in prison in April this year.

Self-proclaimed 'Crypto King' arrested

The Durham Regional Police Service and the Ontario Securities Commission arrested Aiden Pleterski—the 'Crypto King'—and Colin Murphy after a 16-month investigation. This is believed to be the largest fraud case ever in the region. Pleterski is alleged to have raised CA$41.5 million (NZ$49.2 million) from investors, and investing only 1.6% of the total, spending the rest on luxury goods, real estate, and travel. He potentially faces 14 years in prison.

The case is especially interesting because Pleterski frequently publicised his wealth via social media. This likely ruffled the feathers of his unhappy investors, leading one to kidnap Pleterski in 2022, and another to attempt a break-in of a home previously owned by him.

Relevance: *Investor scams are nothing new, but few fraudsters are so brazened as to publicise their wealth on social media, as is alleged to have occurred in this case. Investors can limit their risk by selecting investment professionals who can draw upon certified financial providers. In New Zealand, the investment market and related services involve four key terms: Financial Adviser; Financial Advice Provider (FAP); Financial Advice Service (FAS), and Financial Service Provider (FSP).*

Financial Advisers must be engaged by a licensed FAP to provide FAS on the employer's behalf. As such the employer, usually a company, must be licensed by the Financial Markets Authority (FMA) or be an authorised body. It must also be registered on the Financial Service Providers Register (FSPR—found here). Many Financial Advisers working for Registered FAPs are also registered as individuals on the FSPR. According to the FMA's 2017 guidance, "[b]eing registered on the FSPR demonstrates a business or individual has met basic 'negative vetting' requirements"—essentially a good conduct and character register. FAPs must declare the services offered. Depending on these services, the FAP will need to be licensed or certified by the FMA, RBNZ, and/or the Commerce Commission. License holders are proactively monitored and supervised by their respective sector supervisor. In addition, all FSPs—those listed under S5 of the Financial Service Providers (Registration and Dispute Resolution) Act 2008—must be registered on the FSPR.

The laws and regulations which govern the financial investments market are complex, and for good reason. For those interested in the sector, the New Zealand Companies Office offers useful guides (found here).

UK

National Crime Agency secures first Unexplained Wealth Order in Northern Ireland

After nearly six years, the National Crime Agency (NCA) has secured its first Unexplained Wealth Order (UWO) under the Criminal Finances Act 2017 in Northern Ireland against a man suspected of involvement in paramilitary activity, cigarette smuggling and money laundering. The case demonstrates the common nexus between terrorism-type activities and the more 'traditional' organised crime typologies, where the latter are often used to fund the former.[2] According to The Irish Times, the suspect's only declared source of income since 2008 was the sickness benefit, despite him constructing a property worth an estimated NZ$570,000.[3]

Relevance: *New Zealand's Criminal Proceeds (Recovery) Act 2009, does not contain a UWO clause. A High Court may make a disclosure of source order under S109(A), but the provisions for this are more directed than a UWO under the Criminal Finance Act 2017 in the UK, and its application remains practically difficult. The two Acts make an interesting comparison.*

USA

Chief Financial Officer arrested over alleged involvement in US$67 million Money Laundering Scheme

US prosecutors released indictment charges against Weidong Guan, Chief Financial Officer (CFO) of a multinational media company, alleging his involvement in a transnational money laundering scheme. The scheme allegedly involved a team who purchased tens of thousands of prepaid debit cards on a cryptocurrency platform. The prepaid debit cards were loaded with unlawfully obtained funds, which were then offered at discount rates on the dollar in exchange for crypto.

In the process, the money laundering team apparently "knowingly purchase[d] tens of millions of [US] dollars in crime proceeds," which were then layered in transactions to the company's bank accounts designed to conceal the source of funds.[4] Transactions were achieved by using stolen personal information to open various financial (bank, debit card, and crypto) accounts. Some funds were transferred from the company's accounts into personal accounts before further

---

[2] In the UK, a UWO is a civil power and investigatory tool. Once a person is reasonably suspected of involvement in, or being connected to others in, serious organised crime, they are required to explain the nature and extent of their interest in property, how the property was obtained, how it is held (such as in a trust), and any other information as may be specified by a High Court Order. Use of it is limited to enforcement authorities and not the wider law enforcement community. Failure to comply can lead to criminal or civil action.

[3] Alan Erwin, "Aidan Grew subject of first 'unexplained wealth order' in Northern Ireland," The Irish Times, 17 May 2024, https://www.irishnews.com/news/northern-ireland/aidan-grew-subject-of-first-unexplained-wealth-order-in-northern-ireland-HOGYEWIPN5H5NEMGY4V77C76E4/.

[4] United States of America v. Weidong Guan, a/k/a/ "Bill Guan," Sealed Indictment, United States District Court, Southern District of New York, 3 June 2024, p. 1, https://www.justice.gov/usao-sdny/media/1354021/dl.

layering into other personal accounts held in crypto and fiat currencies across different institutions. Various banks and cryptocurrency platforms raised alerts—including 1,700 automated emails from just one bank— to Guan about the suspicious nature of the funds and transactions in the company's accounts. It is alleged the CFO "made false statements about the source of the company's increased funds," claiming they were profit-derived or from donations.[5]

Relevance: *The indictment offers a detailed view of the alleged offending and useful walkthrough of money laundering methodology. The alleged use of prepaid debit cards and the opening of financial accounts under stolen identities is noteworthy, but it remains unclear on what crypto platform these purchases occurred. In this case, some prepaid debit cards were loaded with "fraudulently procured unemployment insurance benefits obtained using stolen personal identification information of US residents."[6] Similar risks exist for New Zealand residents, whose identity information can be obtained through online scams. Travelling overseas can increase the risk of this occurring due to the need to provide confidential information when crossing international borders. Different threat actors and security vulnerabilities in regional network infrastructure can also create persistent or severe risk exposure leading to higher chances of penetration.*

The Financial Crimes Enforcement Network Advances Beneficial Ownership (BO) Improvements

This year, the Financial Crimes Enforcement Network (FinCen) has made several efforts to raise awareness around the importance of BO information. Most recently, this included a bilingual Beneficial Ownership Engagement outreach event in Puerto Rico, with both state and trade associations attending. The holding of a bilingual event by a federal agency is noteworthy for the US and shows the value placed on this initiative. FinCen previously hosted a webinar on BO information reporting requirements on YouTube, releasing a guide, FAQ webpage, and videos on the matter (accessed here). The Beneficial Ownership Information reporting requirements call on reporting companies (a definition of which can be found here) to file information online. Reporting companies need only submit this information once unless BO details change.

Relevance: *New Zealand entities and individuals doing business in the US should consider the implications of these new requirements. The use of a central database registry by FinCen creates efficiencies for both the public and private sectors by reducing duplications. In New Zealand, reporting entities are required to engage with, and submit information to, multiple agencies for BO-related matters.*

[5] United States of America v. Weidong Guan, a/k/a/ "Bill Guan,", p 2.
[6] United States of America v. Weidong Guan, a/k/a/ "Bill Guan,", p 2.

NEWS FROM OUR PARTNERS

New Zealand Government

Minister attends international Scam and Fraud Prevention Meetings

The Minister of Commerce and Consumer Affairs, the Honourable Andrew Bayly, travelled to Singapore in June to join international discussions about scams and fraud. As these crimes frequently involve organised crime groups operating across international borders, preventative measures require effective international cooperation between government agencies. Consequently, the Minister was joined by an Australian delegation led by the Minister for Financial Service and the Australian Banking Association. They met with Singapore's Minister for Home Affairs, as well as local industry, to discuss international trends and insights, anti-scam technology and regulatory approaches to disrupting scams.

Te Tari Taiwhenua | Department of Internal Affairs

Formal warning issued to lawyer

The DIA has issued a formal warning to Peter S Brinsley for failing to meet AML/CFT obligations relating to the establishment, implementation, and maintenance of an AML/CFT programme, alongside failure to conduct CDD and report transactions.[7] Report entities play a critical role in AML/CFT regimes, and without their accurate and timely submissions, the threats created through criminal exploitation of vulnerabilities will continue.

Te Mana Tātai Hokohoko | Financial Markets Authority

Crowdfunding Service License for Equitise cancelled

The FMA cancelled the crowdfunding service license of Equitise Pty Ltd, with effect of 3 April 2024. Equitise failed to file its audited 2023 financial statements and to provide the FMA its 2023 annual agreed upon procedures report and other information. Despite being deregistered in August 2023 for failing to file its annual confirmation, Equitise continued to provide crowdfunding services.

---

[7] DIA does not assert Mr Brinsley was engaging in money laundering, or the financing of terrorism.

Te Pūtea Matua | Reserve Bank of New Zealand (RBNZ)

RBNZ opens consultations on Government-backed Digital Currency

In April, RBNZ opened consultations for a possible digital currency that would be backed by the government and available to the public. It would be denominated in New Zealand dollars and issued by the Reserve Bank. It is calling the initiative 'Digital Cash'. Essentially, RBNZ is assessing potential options for utilising a form of government-issued cryptocurrency to ensure New Zealand stays abreast of new and emerging technologies and trends.

The initiative is currently in Stage Two (of four). Consultations are open until 26 July 2024. More information can be found here.

Te Tari Hara Tāware | Serious Fraud Office (SFO)

Roading subcontractor sentenced on bribery charges

An unnamed roading subcontractor has been sentenced to 12 months home detention and been ordered to pay $300,000. They are the third subcontractor to plead guilty in an ongoing case, alongside Frederick Pou and Richard Motali. Two others, Jason Koroheke and Aurelian Mihai Hossu, the latter of whom also pled guilty, worked for Broadspectrum. The SFO alleges the subcontractors submitted both real and fake invoices to Broadspectrum, which were then authorised by Koroheke. Once paid, the subcontractors allegedly provided gifts to Koroheke to the alleged value of more than $1 million. Koroheke has pleaded not guilty. A trial date has been set for Monday 1 July 2024.

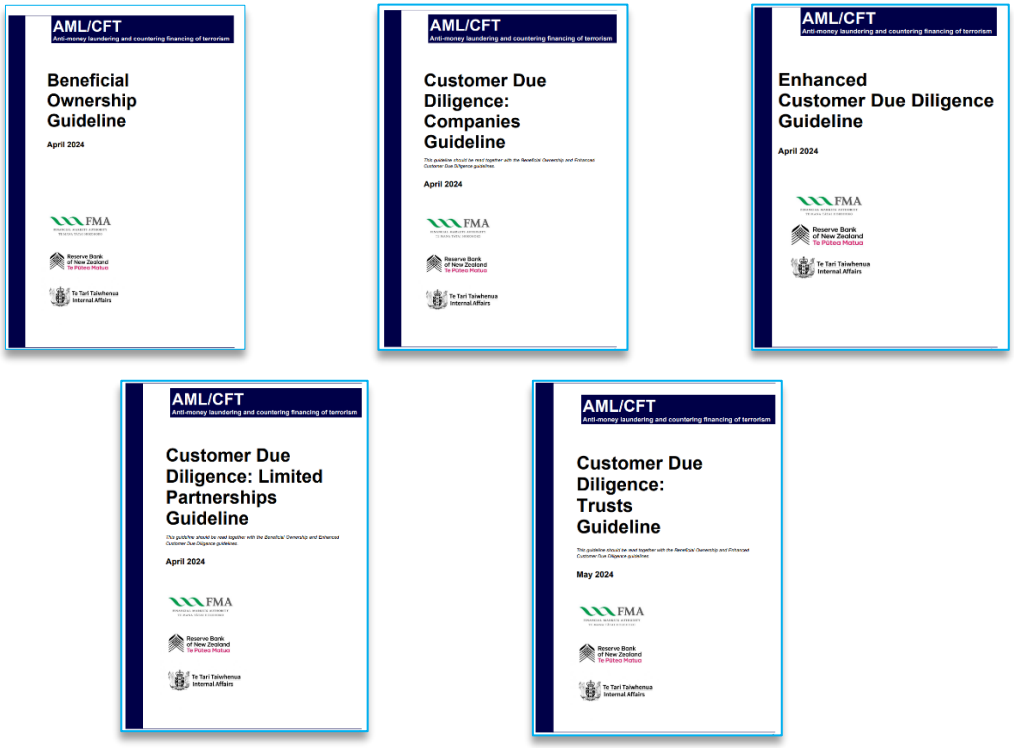
NEW ZEALAND AML/CFT GUIDANCE

Phase 2 AML/CFT Updates

On 29 April 2024, the three sector supervisors (Reserve Bank of New Zealand, Financial Markets Authority, and Department of Internal Affairs) released updated AML/CFT guidelines. The Enhanced Customer Due Diligence Guidelines, AML/CFT Customer Due Diligence: Companies, AML/CFT Beneficial Ownership Guideline, AML/CFT Customer Due Diligence: Limited Partnerships 2024 and Sole Traders and Partnerships 2024, and AML/CFT Customer Due Diligence: Trusts 2024, address recent changes under the Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Amendment Regulations 2023, that commenced on 1 June 2024. These comprise the second stage of regulatory amendments, with the third stage set for 1 June 2025. The second stage "introduces new obligations for entities that already have existing AML/CFT obligations."[8] In most cases, the updated Enhanced Customer Due Diligence (ECDD) process requires additional information to be obtained and verified by reporting entities for new customers or existing customers conducting an occasional transaction or activity. New customers falling under certain high-risk criteria must have ECDD undertaken. One of the more substantive ECDD changes is the requirement to determine source of wealth and source of funds.

The DIA has also released new guidelines for liquidators (accessed here).

All reporting entities are encouraged to review these updates.



[8] "Changes to AML/CFT Act Regulations," Ministry of Justice, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/aml-cft-review/.

INTERNATIONAL AML/CFT GUIDANCE, TYPOLOGIES, AND CASE STUDIES

Australia

New Guidance to Help Combat the use of Foreign Students as Money Mules

AUSTRAC, through its public-private partnership—Fintel Alliance—released new guidance "to help businesses identify and report suspicious activity related to criminal networks targeting vulnerable international students and temporary residents as money mules." As part of the Financial Crime Guide series, the work is easily accessible and sets out how money mules are recruited, indicator activities, how to stop such activities and where to report them.

Relevance: *This methodology persists in New Zealand. Threat indicators, such as cash deposits or wire transfers inconsistent with expected student income or expenses, must be monitored. AML/CFT teams from New Zealand financial organisations, would benefit from reading the document as the close relationship between the two countries' financial sectors mean methodologies are frequently encountered across jurisdictions.*

Organisations and Initiatives

BASEL Institute of Governance

Informal Networks and Anti-Corruption Quick Guide Series 23

This updated release introduces informal networks, how they function, and who they benefit. It talks about the importance of focusing on neutralising informal networks. To a large extent, this requires behavioural and attitudinal change rather than relying on conventional anti-corruption instruments.

Relevance: *In underdeveloped regions, informal networks often provide access to goods and services that otherwise would not be available through formal channels. The individuals and groups who use them do not always do so for illegal or malicious reasons. As access to goods and services improves, it can be challenging to convince those involved in otherwise legitimate activities to embrace a (formal) financial system. This is especially relevant for countries with large immigrant or migrant worker communities who may not be familiar with the financial system and/or rely on informal networks for remittance services out of habit.*

Bellingcat

How to get Started: Investigating Payment gateway Online

Payment gateways are the technology that processes a transaction by taking payment information, verifying it against a financial institution, and confirming that the transaction is legitimate before completing it. This article provides an easy 'how to' guide to check the payment gateway in use by a website, and whether those websites may be masking how the transaction is being reported/recorded. The example used in this case is a non-consensual AI Deep Fake pornography website, which is illegal in many jurisdictions.

Relevance: *Understanding how payment gateways work can be a useful tool in a reporting entity's risk assessment toolbox. It can indicate whether a potential customer (i.e. a business) is masking their payment system from their own customers and/or the payment gateway providers. This can be a valuable clue in identifying the nature of the business and could be applied to CDD/ECDD/KYK scenarios, where a risk assessment may raise further questions about how a customer is conducting their payments.*

TRACE

Briefing Paper: Illicit Money Flows in the EU

TRACE conducted 30 case studies examining traditional and novel money laundering cases, revealing the impact of new technologies on these streams. New technologies, such as decentralised financial products, increase the ability of offenders to mask their activities by bypassing traditional financial institutions thereby providing an extra layer of anonymity. Unsurprisingly, a notable rise in the use of non-fungible tokens was detected. Recommendations include: the need for state-of the-art technology for LEAs, FIUs, and judicial authorities; more robust AML rules to accommodate developments in virtual assets and related services; and stronger cooperation between public and private sectors.

Relevance: *While this briefing paper offers recommendations to enhance the capabilities and efficiencies of FIUs and LEAs, it is useful for reporting entities, especially those involved in virtual assets, as it provides an indication of factors impacting the sector supervisors.*

A Checklist for the Analysis of Suspicious Transaction Reports (STRs)

The TRACE Project—an initiative by 17 organisations from across the EU to improve cross-border investigations—has recently developed an AI tool to assist in the investigation of illicit money flows (IMFs) within the context of money laundering. Three aspects were identified to help Law Enforcement Agencies and Financial Intelligence Units analyse STRs: a geographic risk model; red flag checklists; and a set of benchmarks for both detecting and investigating IMFs and STRs. In each of these three areas, the AI tool

models variables and generates outputs in visual formats, which can then be further interrogated by the user.

Relevance: *The TRACE geographic risk model follows well-established practices; however, an underlying component is the presumption that "the more secretive a transaction is, the more likely it has an illicit component."*[9] *This creates a weakness in the approach because financial crime can be effectively hidden within legitimate structures and activities—with the openness of these conversely serving as the cover. The red flag checklists and benchmarks components are already used by various LEAs and reporting entities. Of course, the use of AI significantly enhances analytical speed. While TRACE specifically focusses on the issues and needs of LEAs and FIUs within the context of the European Union, the transnational component is relevant to other jurisdictions, including New Zealand.*

Canada

The Role of Virtual Currency Automated Teller Machines (ATMs) in Laundering the Proceeds of Crime

FINTRAC reviewed Suspicious Activity Reports to identify key attributes of virtual currency ATM activity related to ML/TF. It assessed that virtual currency ATMs "are becoming a key tool in the placement stage of money laundering," and determined that entities dealing in virtual currencies, such as virtual currency ATMs, are considered money services businesses under Canadian legislation. Similar to recent Phase 2 amendments in New Zealand, this brings certain obligations to reporting standards, maintenance of records, CDD, and compliance [New Zealand amendments can be found here and here]. The advisory shows the sector needs greater regulatory oversight and self-implemented controls and mitigation measures by reporting entities.

Relevance: *There are 98 crypto ATMs throughout New Zealand, 40 of which are within the Auckland region. These are high-risk and provide opportunities to structure transactions; operators should be aware their machines are targeted for converting fraudulently obtained fiat and/or virtual currency. Operators are required to comply with applicable AML/CFT obligations, including the collection and retention of customer records, and the reporting of suspicious transactions to the FIU.*

---

[9] TRACE, "A Checklist for the Analysis of Suspicious Transaction Reports," Briefing Paper, 14 May 2024, https://trace-illicit-money-flows.eu/checklist-for-the-analysis-of-suspicious-transaction-reports/.

UK

Role of Organised Crime Groups in Rural Crime

The UK's National Rural Crime Network (NRCN) released a report revealing the extent of organised crime in rural offending. The research "very clearly demonstrates that a significant proportion of rural crime constitutes organised criminality." Apart from theft of commodities and assets, offending also involved profits gained "from gambling activities associated with wildlife offences." Unfortunately, the extent of mapping for these offences across the UK is low.

Findings also suggest a relationship between wildlife and drug offences across the sample pool, further highlighting apparent organised crime links. Money laundering predicates included the theft of vehicles and machinery for use in ATM thefts, subsequent disassembly, and shipment overseas. The NRCN released an accompanying 10-Point Plan to address these crimes.

Relevance: *Apart from demonstrating how in-depth research can reveal underlying trends to long-existent issues, revelations about the organised theft of machinery, tools, and vehicles for use in subsequent ATM thefts presents interesting potential crime-mapping opportunities since the stolen cash will need to be placed and then layered.*

HM Treasury releases AML/CFT Supervision Report

The eleventh AML/CFT supervision report provides information on the performance of AML/CFT supervisors in the 2022-23 financial year. Unlike New Zealand, supervisors in the UK are required to submit information collected for the purposes of performing their functions to HM Treasury, which publishes a consolidated review of the sector supervisor's performance under S51 of the Money Laundering Regulations. The report is timely considering the UK is busy updating its money-laundering regulations and supervision regime. That update includes the upcoming FATF-inspired Effectiveness Framework for the sector supervisors, which introduces a set of metrics across a range of supervisory activities, including educational activity, a risk-based approach, risk-based enforcement, and effectiveness of supervisory interventions.

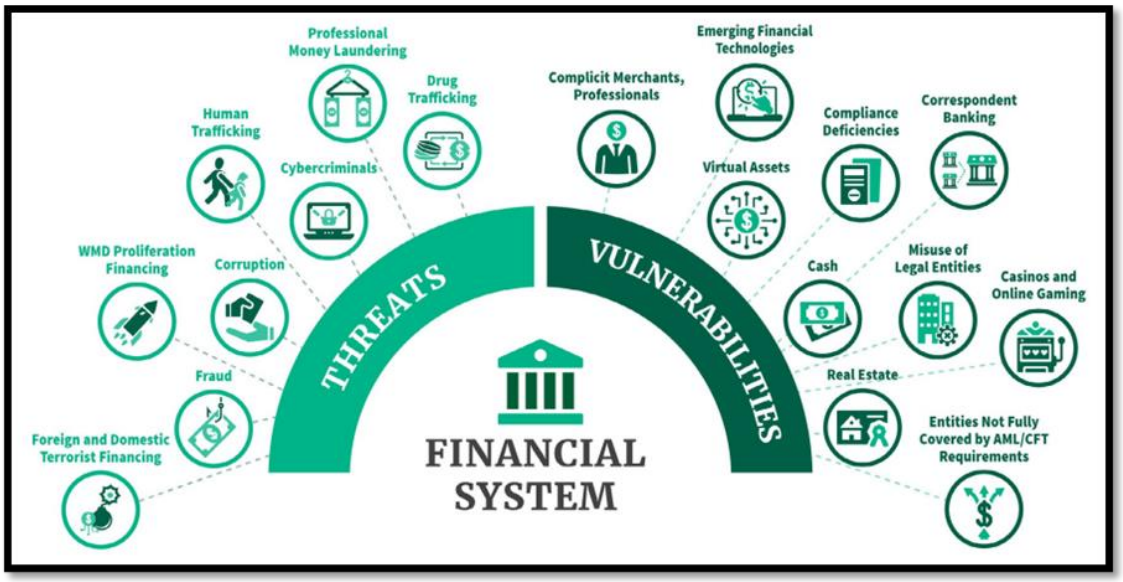
Relevance: *The development and introduction of an Effectiveness Framework for supervisors by HM Treasury encourages measuring effectiveness of interventions and enforcement by risk-categorisation to provide better data for empirical assessment.*

US

US Department of the Treasury releases National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing

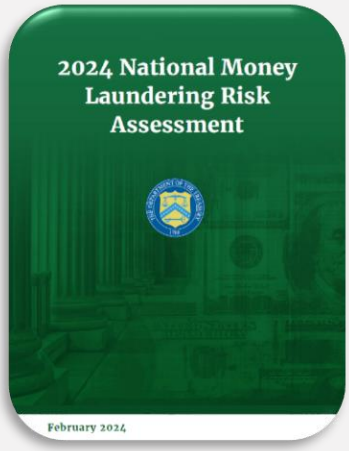
In February, the US Department of the Treasury released its three National Risk Assessments (NRAs). The US NRAs effectively serve as a threat and vulnerabilities horizon warning for New Zealand, with changes observed a harbinger of things to come.

NRA Identified Key Threats and Vulnerabilities



Source: *2024 National Strategy for Combating Terrorist and Other Illicit Financing* (Washington, D.C.: U.S. Department of the Treasury, May 2024), p. 5.

Money Laundering

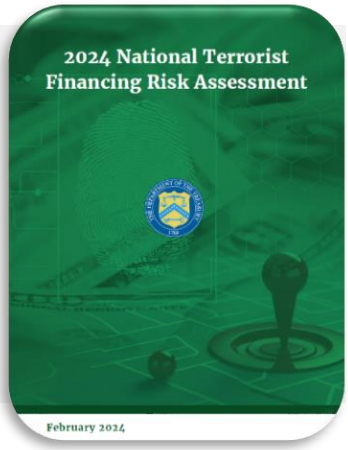


Fraud, drug trafficking, cybercrime, human trafficking and human smuggling, and corruption remains the largest generators of illicit proceeds identified within the Money Laundering NRA. Fraud continues to be the largest driver among these. Due to recent global changes stemming from geopolitical upheaval, COVID-19, and technological developments, the "broader illicit finance ecosystem…has substantially evolved," with increased exploitation of virtual assets and digital peer-to-peer payment systems. The report also addresses the threat posed by professional money laundering organisations linked to foreign state entities or officials. These often do not exhibit predicate offences, although they may be associated with other transnational organised crime groups that do.

Relevance: *Cases of healthcare fraud, especially those centred around COVID-19-related funds, will be interesting for New Zealand investigators and serve a useful waypoint for future policy considerations. The discussion on Chinese Money Laundering Organisations and Networks is timely for New Zealand as it calls into focus the use of these by (ordinary) Chinese nationals seeking to evade the Chinese government's currency controls.*

Terrorist Financing

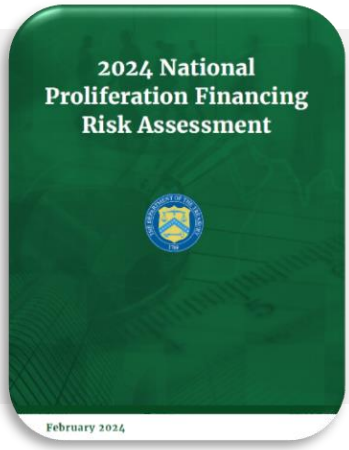
This NRA reveals that the most common financial connections between individuals in the US and foreign terrorist groups involves the solicitation of funds or direct sending of funds overseas using cash, registered money services, or virtual assets. It also discusses the exploitation by Hamas of the international financial system by attracting unwitting donor support in both fiat and virtual currencies, including utilising crowdfunding websites and sham charities under the guise of humanitarian support or aid.



Relevance: *The shift towards decentralised networked structures facilitated by online communication has allowed a change in terrorist financing. The abuse of crowdfunding and online fundraising is just one consequence of this and is a developing trend. The underlying processes are like 'regular' scams, whereby money is fraudulently elicited from donors by appealing to their sense of humanity and empathy for persons or communities in distress. Considering ongoing conflicts in the Middle East, Sudan, Myanmar, and Ukraine, reporting entities may wish to alert their customers of this trend.*

Proliferation Financing

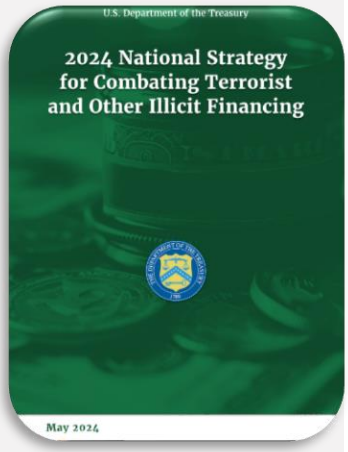
The third NRA highlights the expanded efforts of Russia to support its ongoing illegal war in Ukraine. Increasing, as it has, its use of front companies and transhipment networks to source material and dual-use components in breach of United Nations Security Council resolutions Russia itself voted for. It also addresses incidences of hacking of virtual asset service providers by the Democratic People's Republic of Korea. Other threat actors assessed include Iran, the People's Republic of China, Syria, Pakistan, and non-state actors.



FIU Comment: *The US assessment of Russian involvement stands in stark contrast to the 1st Follow-Up Report to the FATF's Mutual Evaluation Report of the Russian Federation released by the Eurasian Group—a regional body similar to the FATF and an associate member of the latter, which includes the likes of Russia and Belarus—upgrading the Russian Federation's rating to 'largely compliant'.*

Relevance: *Sector supervisors and reporting entities would benefit from considering the points raised within this NRA. New Zealanders have traditionally seen themselves as somewhat apart from issues of proliferation owing to geographic distance. However, the global financial system is not handicapped by this, and proliferation financing need not involve weapons or weapon components directly in order to contravene legal obligations.*

2024 National Strategy for Combating Terrorist and Other Illicit Financing



In May, the US Department of the Treasury released the above National Strategy to address risks identified in the three 2024 NRAs. According to the press release, the Strategy "details how the United States will build on recent historic efforts to modernize the US anti-money laundering/countering the financing of terrorism (AML/CFT) regime, enhance operational effectiveness in combating illicit actors, and embrace technological innovation to mitigate risks." The National Strategy provides a summary of the key illicit finance threats and vulnerabilities, many of which are directly applicable to the New Zealand context. Annex 3 of the National Strategy also offers a detailed breakdown of past, current, and future AML/CFT/CPF actions and priorities.

This is an important piece of work that builds upon significant AML/CFT changes undertaken by the US in 2024.

Relevance: *Of interest to domestic readers are the sections on large-scale fraud schemes, ransomware attacks, and the vulnerability of the real estate sector, all of which are seen in New Zealand. Annex 3 provides an interesting comparison of AML/CFT/CPF efforts in the US vis-à-vis New Zealand. Apart from differences of scale, the introduction of a Beneficial Owners register, and efforts to capture activities within the arts and antiquities market are two immediate contrasts to New Zealand. Those wishing to establish a business presence in the US should review this strategy as it offers signposts for further reading and/or guidance.*

New Sanctions Announced Against Russia

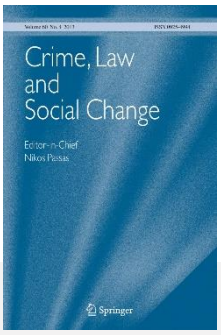
The US Department of the Treasury in conjunction with the US Department of State announced over 300 new sanctions against a range of individuals and entities. Restrictions have been extended to include 'secondary sanctions risk' from foreign financial institutions in third-party countries offering support to Russia. These include logistics and trading companies that assist in transporting and/or transferring goods to Russia. Many mainland China-based entities and individuals are listed in the release, alongside an explanation of their role in assisting the Russian state in its illegal activities.

FIU Comment: *The UK also announced new sanctions against Russia (found here).*

Relevance: *Sector supervisors and reporting entities are advised to review the list, noting any potential connections between those named on it and New Zealand.*

MEDIA LIBRARY

Journals



- Lawrence, S., van Ruth, S., Elliott, C. *et al.* Characteristics and situational aspects of seafood fraud: a comparative crime script analysis. ***Crime, Law and Social Change*** (2024): no page no. https://doi.org/10.1007/s10611-024-10149-7

According to the authors, "Food fraud can be defined as the practice of misleading consumers or customers about a product for financial gain…" This often includes undeclared species substitution and use of additives. Apart from ecological and biodiversity concerns, food fraud carries public health risks, and generates illegally obtained profits needing integration into the mainstream economy. Of the cases examined, all lead offenders owned legitimate seafood businesses, and crimes were conducted by senior leaders who exploited their resources, relationships, and existing supply chain networks for illicit behaviour. This differs from previous studies, which found a prevalence for "complex and opaque" supply chains to conduct illegal activities.

Relevance: *The article demonstrates how financial crime can be effectively hidden within legitimate structures and activities. The subject cases deliberately exploited their longstanding industry reputations to mask their illegal activities because they "perceived that the risk of checks or sampling was low..." This serves as a reminder for compliance officers and auditors to look beyond the activity or transaction itself and consider the nature of the action within the context of the business and larger industry. Reputation alone should not be reason to downgrade due diligence. The discussion around whistleblowing will also be of interest to intelligence practitioners when assessing source collection factors. This article should interest MPI, DOC, MBIE, financial service providers, and all patrons of New Zealand fish & chips shops.*

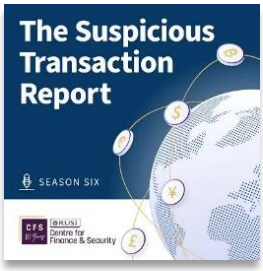
- Hong, Sunmin, Jeong, Dohyo, and Kim, Pyung. "Have offender demographics changed since the COVID-19 pandemic? Evidence from money mules in South Korea." ***Journal of Criminal Justice*** 91. (March-April 2024): no page no. ISSN 0047-2352. https://doi.org/10.1016/j.jcrimjus.2024.102156

International travel restrictions from COVID-19 altered money mule demographics identified by the Seoul Metropolitan Police Agency in South Korea. They saw "a decrease in the percentage of non-Korean money mules, an increase in the proportion of female individuals engaged in money mule activities, and a rise in the average age of money

mules after the outbreak of the pandemic." The authors contend that the findings "hold significant implications for developing targeted policy interventions…"

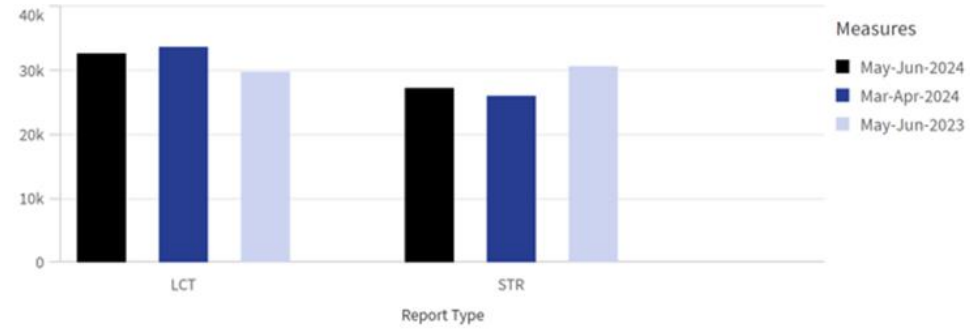
Relevance: *An increase in the proportion of females engaged in money mule activities can be transposed to the New Zealand context where women experienced a disproportionate fall in employment due to the negative economic effects of COVID-19. In theory, this could have created greater motivation for engaging in illegal activities. Reporting entities should consider how future shock events disproportionately impact different demographics and include these in their compliance monitoring systems, ensuring they are provided better assistance and guidance. The article also indirectly touches upon implications in setting intelligence targeting and profile parameters in response to unforeseen global events. It will interest MOH, law enforcement, sociologists, and sectors with money mule risks.*

Podcasts

	The 24 May episode of **The Suspicious Transaction Report**, released by the Centre for Finance and Security at the Royal United Services Institute, discusses the economic impact of sanctions against Russia. The guest, Vladimir Milov, an economist and energy expert, previously served as deputy minister of energy before leaving Russia after clashes with senior government and bureaucratic officials. Milov reveals the smoke and mirror tactics employed by the Russian state in presenting its economic figures and statistics. ➢ **Relevance:** *Difficulties securing import chains, alongside legitimate export channels, has led both Russian and some Western-based businesses to undertake sanction busting activity. As the analysis presented by Mr Milov shows, the negative effects of sanctions on the Russian economy will linger, leading to the continuation and likely expansion of existing underground and illicit business activities intended to skirt sanctions, the proceeds of which will need to be laundered.*
	On the 7 June episode of **AML Conversations**, John Byrnez, former ACAMS Executive Vice President and current RightSource Vice Chairman discusses the most recent AML/CFT news and current affairs. ➢ **Relevance:** *This podcast provides insights from a US-centred viewpoint for those who do not have the time to read more in-depth pieces. The hosts often raise points that deserve further consideration from reporting entities.*

	The 7 May episode of **The Dark Money Files** introduces Proliferation Financing, its risks, and reporting entity obligations within the UK. ➢ **Relevance:** *Although presented from a UK perspective, the proliferation financing regime is underpinned by UN Security Council Resolutions thereby applying a relatively rigid global standard. This episode has helpful information for New Zealand reporting entities wishing to know more about the subject.*

Processed Transaction Volumes



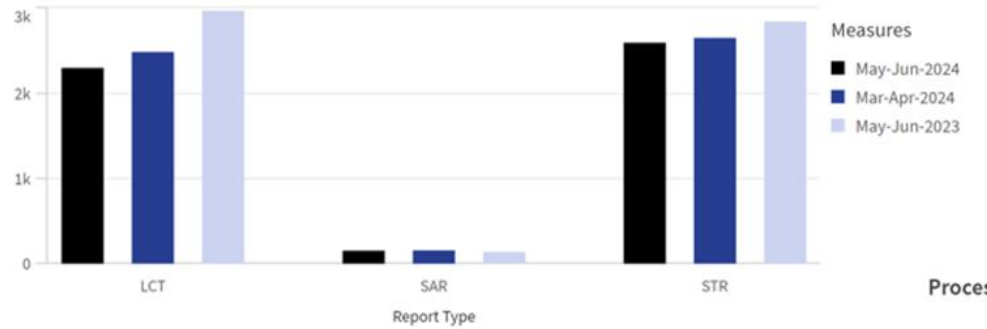
May-Jun-2024 Transactions
1.35M

May-Jun-2024 Reports
30.55k

Processed Report Volumes

Report Type	May-Jun-2024	Mar-Apr-2024	May-Jun-2023
IFT	25514	23320	25438
LCT	2296	2483	2966
SAR	153	156	138
STR	2592	2649	2840

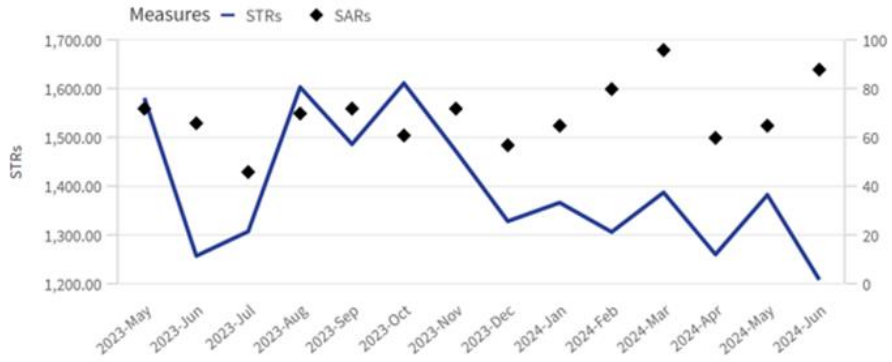
Processed Report Volumes



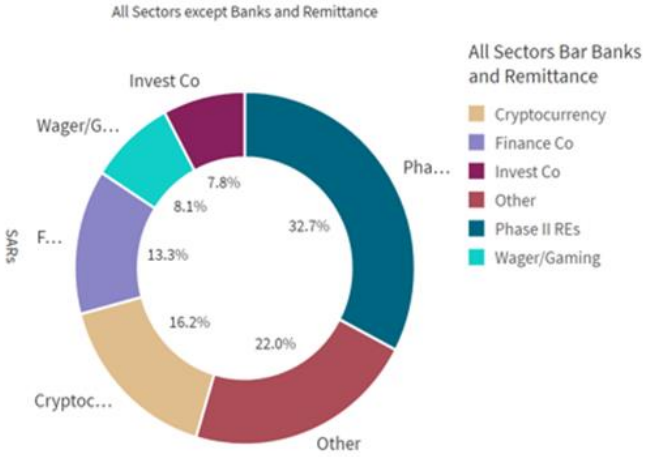
Processed Transaction Volumes

Report Type	May-Jun-2024	Mar-Apr-2024	May-Jun-2023
IFT	1292117	1206886	1108909
LCT	32673	33694	29790
STR	27265	26043	30661

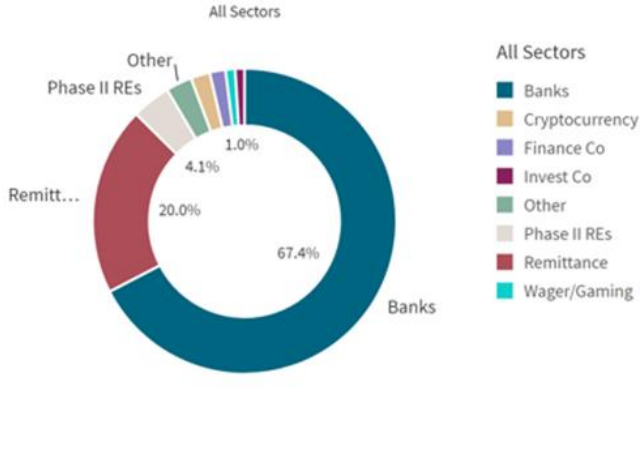
SAR/STR Volumes



Processed STRs & SARs



Processed STRs & SARs



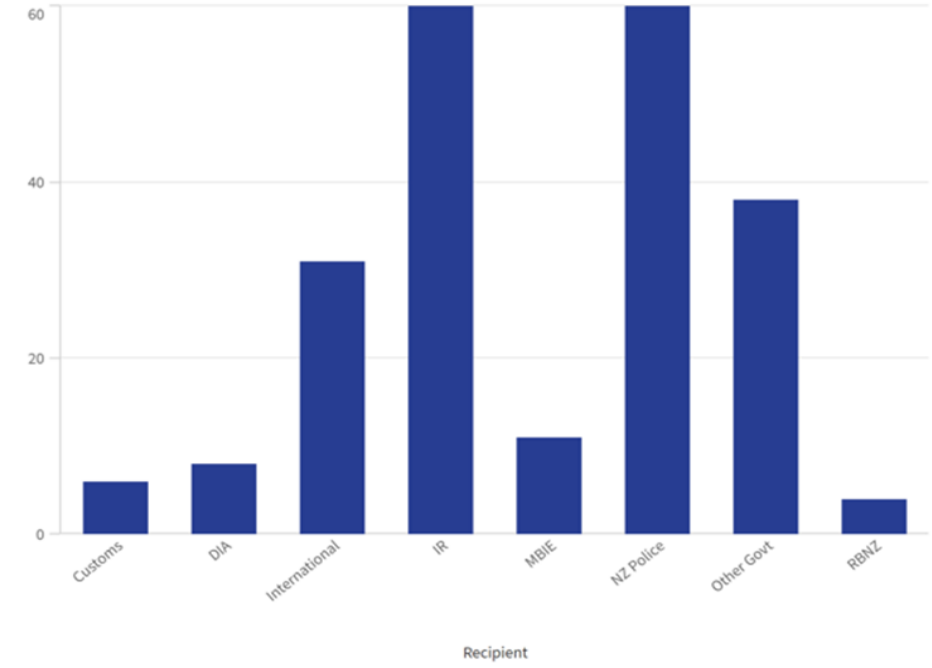
Disseminations of Products by Recipient

Recipient	May-Jun-2024	Mar-Apr-2024	May-Jun-2023
Customs	6	3	6
DIA	8	16	12
International	31	11	3
IR	60	35	6
MBIE	11	5	6
NZ Police	60	51	21
Other Govt	38	24	11
RBNZ	4	0	2

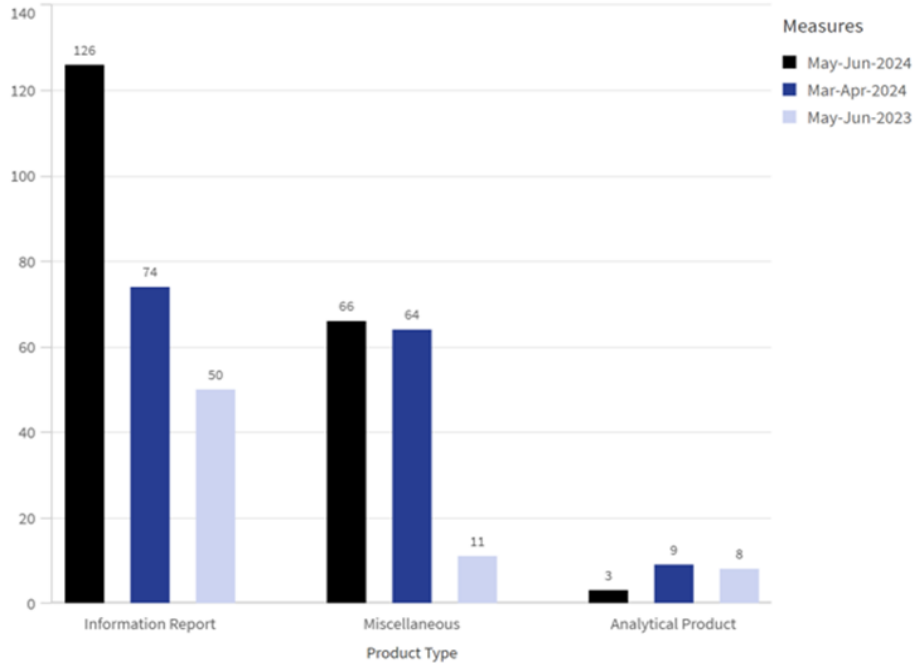
Disseminations of Products by Type

ReportGroup	May-Jun-2024	Mar-Apr-2024	May-Jun-2023
Analytical Product	3	9	8
Information Report	126	74	50
Miscellaneous	66	64	11

Disseminations of Products by Recipient



Disseminations of Products by Type



NEW ZEALAND
POLICE
Ngā Pirihimana o Aotearoa