

The Suspicious Activity Report

SEPTEMBER 2022

New Zealand Financial Intelligence Unit

INTRODUCTION

The Suspicious Activity Report is produced by the Financial Intelligence Unit (FIU), part of the New Zealand Police Financial Crime Group, led by Detective Superintendent David Lynch. This report is comprised of FIU holdings and open-source media reporting collected within the last month.

Background

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. It seeks to achieve this through compliance with the Financial Action Task Force (FATF) recommendations. The Financial Intelligence Unit produces this monthly report as part of its obligations under section 142(b)(i) and section 143(b) of the AML/CFT Act 2009. The Financial Crime Group is made up of the Financial Intelligence Unit, Asset Recovery Unit, the Money Laundering Team, and a group at Police National Headquarters.

Financial Intelligence Unit

The Financial Intelligence Unit (FIU), led by Detective Inspector Christiaan Barnard, has been in operation since 1996. Its core function is to receive, collate, analyse, and disseminate information contained in Suspicious Transaction Reports, Prescribed Transaction Reports, and Border Cash Reports. It develops and produces a number of financial intelligence products, training packages and policy advice. The FIU participates in the AML/CFT National Coordination Committee chaired by the Ministry of Justice, and chairs the Financial Crime Prevention Network (FCPN). It is a contributing member to international bodies such as the Egmont Group of Financial Intelligence Units and the Asia/Pacific Group on Money Laundering.

Asset Recovery Unit

The New Zealand Police Asset Recovery Unit (ARU) is led by Detective Inspector Craig Hamilton and was established in December 2009 to implement the Criminal Proceeds (Recovery) Act 2009 (CPRA). The ARU is the successor to the Proceeds of Crime Units, which were established in 1991, and was combined with the FIU to create the Financial Crime Group. The CPRA expanded the regime for the forfeiture of property that has been directly or indirectly acquired or derived from significant criminal behaviour. It is intended to reduce the possibilities for individuals or groups to profit from criminal behaviour, to reduce the opportunities they have to expand their criminal enterprises, and act as a deterrent for criminal activity. There are five Asset Recovery Units, based in Whangarei, Auckland, Waikato/Bay of Plenty, Wellington, and Christchurch.

Money Laundering Team

The Money Laundering Team (MLT), led by Detective Senior Sergeant Andy Dunhill, is the newest element of the FCG and was established in 2017 to target money laundering risks and reduce the investigative gap for financial investigations in organised crime. The MLT investigates criminal offenders moving the proceeds of predicate offending. The focus of the team is on disrupting and dismantling facilitators assisting organised criminal groups to hide illicit funds, including complicit Designated Non-Financial Business and Professions (DNFBPs) and other third parties such as money remitters.

Notes from the Director of the National Organised Crime Group

Detective Superintendent Greg Williams



The wholesale rate of methamphetamine (meth) continues to tumble across the globe as manufacturing ramps up. This is not a good news story for New Zealand because our users pay some of the highest retail prices in the world for meth.

It is estimated that the meth trade alone generates around \$300 million a year in New Zealand, and if other illicit products are considered, around \$750 million is generated annually.

The majority of these sales are still primarily cash at the gate. While some of the cash is consumed within communities, a substantial amount must be introduced into the licit financial system for it to be available or transferable. Significant amounts have to be deposited to pay for new products offshore as well.

Transnational crime groups are also targeting New Zealand and inserting their own cells here. In the last five years NZ Police have identified and disrupted 24 of these cells. On each occasion, after setting up supply lines in New Zealand and bringing the product in, they seek New Zealand-based money launderers to get the illicit cash into the financial system. This is done primarily through banks or casinos, so it can be moved offshore back to them.

The professional facilitators who provide money laundering can act as individual entities, on occasion as accountants, or in a number of recent cases, as money remitters. These crime groups are employing people to undertake cash depositing. Auckland features heavily in the cash depositing and these deposits are usually at the teller and most often into third party accounts. The cumulative amounts are surprising, as some deposits can be very small but could also range upwards of well over NZ\$100,000.

This is happening every day. This simple practice of getting illicit cash into the banking system is probably one of the biggest enablers of transnational crime and perpetuates massive social harm across our communities through addiction. It is also one of the simplest levers to pull to seriously impact both transnational and national organised crime groups, because if they can't get cash into the system they cannot function.

Disrupting these crime groups by targeting illicit cash deposits aligns perfectly with the 'Transnational Organised Crime Strategy' vision of making New Zealand the hardest place in the world for organised criminal groups and networks to do business.

NEW ZEALAND AML/CFT NEWS

FIU News

Updates to goAML

[GoAML](#) is a key tool for financial intelligence, as it holds information received from reporting entities to be used in the prevention, identification, and prosecution of financial and associated crimes.

In 2017 goAML began accepting a range of new report types, which significantly increased the amount of data being ingested into the system. While this is hugely beneficial in terms of the data available for analysis, the number of errors increased as the volume of reports increased. To ensure this vital system continues to offer accurate information, additional measures are being implemented to manage quality assurance for this ever-increasing flow of submissions.

Earlier in 2022, the FIU began a project to improve data quality within goAML.

The Data Quality Project aims to amend systems and processes to improve the overall quality and reliability of data held within goAML. This will ensure all reports submitted are complete and correct before the data is integrated into the system.

Upcoming changes will introduce a series of automated rules into the existing system, where any submitted reports that do not fulfil the rule requirements are flagged for further analysis. Rules will include checks for a range of details, including errors in account attribution, and correct usage of SWIFT codes. Flagged reports will be manually reviewed by the FIU Compliance Team, and reporting entities will be notified should any report they have submitted be rejected.

This combined automated and manual system will aim to provide streamlined management of reports entering the system and, over time, minimise the number of rejected reports while protecting the integrity of data within goAML.

Rules will be added to the system in the coming weeks, with additional rules being added over time. This change will occur in the background and will not affect reporting entities' ability to submit reports and use goAML.

This is an exciting progression for this integral system and will benefit everyone involved in the reporting of suspicious activity and prescribed transaction reports, strengthening New Zealand's ability to intercept and prevent financial crimes. The FIU looks forward to the progression of these changes and the positive outcomes these system improvements will bring.

AML/CFT Media Library

PODCASTS



[*Fraud Talk: The Insane, Real-Life Story of Crazy Eddie Antar*](#)

The author of *Retail Gangster: The Insane, Real-Life Story of Crazy Eddie* discusses the wide-ranging fraud case and ultimate unravelling with Association of Certified Fraud Examiners Chief Training Officer John Gill.



[*The Perfect Scam: Why Gift Cards are Gold Mines for Scammers*](#)

The podcast produced by the American Association of Retired Persons (AARP) has recently released this two-part series on gift cards, featuring three people who share their experiences with scams involving gift card payments.



[*Planet Money: Wake Up and Smell the Fraud*](#)

This podcast episode by National Public Radio (NPR) delves into a case of a fast-growing new fraud scheme: triangulation fraud.

DOCUMENTARY



[*Crime: Need vs Greed*](#)

Private investigator and former police detective Tim McKinnel explores New Zealand 'white collar crime' in this documentary, available on TVNZ+

YOUTUBE



[*QQAAZZ Group: How Cybercriminals Built a ML Empire*](#)

This video presents a real-life case involving an online darkweb gang, QQAAZZ. It explores how they laundered money, and how their love of Instagram clout ultimately led to its downfall.

MONEY MULES

Background

Money mule networks are a global issue and are used to move vast sums of illicit money between accounts, facilitating a range of criminal and terrorist activities.

Although it is difficult to assess the scale of money mule activity, the 2021 EUROPOL Money Mule Action ([EMMA 7](#)) resulted in 18,351 money mules and 324 mule recruiters identified across 26 countries. This is a marked increase from the previous EMMA 6 operation, which identified 4,031 money mules and 227 recruiters. The EUROPOL Money Mule Action revealed that money mules are being used to launder money for a wide array of online scams such as sim-swapping, man in the middle attacks, e-commerce fraud, and phishing.

In New Zealand, government cybersecurity department [CERT NZ](#) says scams have cost New Zealanders nearly \$70 million since March 2017, but that number is believed to be much higher due to the number going unreported as a result of shame or embarrassment. According to the Banking Ombudsman Scheme's [latest annual report](#), fraud and scam complaints increased by 63% in the 2021-2022 year.

What is a Money Mule?

A money mule is someone who transfers or moves illegally acquired money on behalf of someone else or allows someone to take control of their account. Criminals recruit money mules to help launder proceeds derived from online scams and frauds or other serious crimes by using the mules' bank accounts. The strategy is a way for criminals to conceal their identities and the source of their illegal funds and evade the customer due diligence (CDD) measures that would otherwise raise red flags. The use of money mules also allows criminals to create layers of distance between them and their victims, making it more difficult for law enforcement to accurately trace money trails.

There are three categories of money mules: unwitting, witting, or complicit.

Unwitting mules are unaware they are part of a larger scheme and may be victims of a romance scam or employment scam. They trust their contact when asked to use their bank account to move funds and are motivated by that trust, believing in the actual existence of their romance or employment.

Witting mules ignore obvious red flags or are wilfully blind to their involvement in illicit activity. Witting mules often receive a cut for the use of their accounts or for opening multiple bank accounts and are motivated by financial gain or an unwillingness to acknowledge their role.

Types of money mules



Unknowing individuals

are unaware they are part of a laundering scheme. These could be victims of online romance schemes or fake job offers.



Witting individuals

willfully ignore red flags or turn a blind eye to their money-laundering activity. They usually get paid.



Complicit individuals

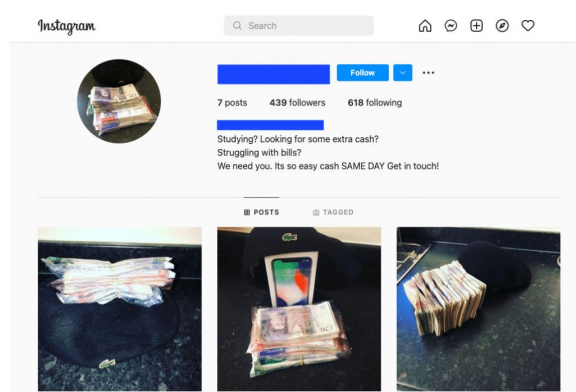
are professional money mules who are trained to subvert financial institutions and law enforcement.

Complicit mules are fully aware of their role and actively participate in the offending. They serially open bank accounts to receive money from a variety of unknown individuals or businesses for criminal reasons, keeping a percentage of the money they move, may also advertise their services, and recruit other money mules. They are motivated by financial gain or loyalty to a known criminal group.

Recruitment

Money mules may be recruited from a range of background, age, and gender groups, the categories of people most often targeted for money muling include those in economic hardship, new migrants, the elderly, and young people – especially university students.

Criminals exploit those with financial difficulties by approaching them via social media or unsolicited emails or instant messages with offers of easy cash. These ‘recruiters’ will use the promise of earning money quickly to convince unwitting money mules to provide their bank details and transfer funds received to another account, allowing them to keep some of the cash for themselves.



Instagram account of a person who recruits potential mules. Source: sumsub.com

Recruiters can lure unwitting money mules by creating job advertisements that appear like legitimate offers on job websites or social media, using terms such as “money transfer agents” or “local processors”.

To lure young people into becoming money mules, recruiters may also create profiles on social media platforms, infiltrate popular groups or special interest pages, and post images of a luxurious lifestyle, including large sums of money.

Romance scams are also a common recruiting tool; the criminal adopts a false online identity to gain a victim’s trust and affection, then convinces them to receive deposits and transfer funds through their financial accounts.

Traditionally, criminals have focussed on recruiting mostly younger people and students as money mules. [According to Barclays](#), the money mule recruits of people under 21 more than tripled between 2016 and 2019, with 30% of all money mules reported to Barclays by victims and other banks in this age group.

However, recent research from CIFAS and [Lloyds Banking Group](#) show that money mules are getting older. The [latest research from CIFAS](#) has revealed that there is an increasing number of middle-aged money mules and businesses being recruited to launder money, with data from the (UK) National Fraud Database revealing a 34% increase since 2017 in the number of accounts belonging to 40-60 year olds bearing the hallmarks of money mule activity. Mule recruiters are likely to be targeting this age group on the belief that larger transactions typically made by this age group may be less likely to appear suspicious.

Criminals may also perceive the movement of large sums in business accounts as appearing to be less suspicious. Data from the National Fraud Database also revealed a rise in the number of business accounts bearing the hallmarks of money mule activity. In 2020, there was a 26% increase in the number of business accounts involved compared to the previous year.

According to new [data from Lloyds Bank](#), there has been a sharp increase in those over the age of 40 caught moving fraudulent funds through their bank accounts over the last year. A surge of cases amongst older groups has been observed over the last 12 months, with a 26% increase in those aged 31 to 39 and a 29% increase in those aged over 40. Further, research conducted by Lloyds Bank on the British adult general population revealed that fewer than half (43%) realise that being asked to move money through their account on behalf of someone else could be the sign of a scam, or an attempt to disguise the original source of stolen funds.

Risk-Based AML/CFT Measures

The threat posed by money mules means that banks and other reporting entities must understand how mules operate as part of money laundering schemes and ensure that their AML/CFT compliance programs are set up to detect and prevent the relevant methodologies. While money mules have historically been used to transfer physical amounts of cash between locations, in a modern financial context, they are generally used to open and manage bank accounts to facilitate the deposit, transfer, and withdrawal of illegal funds.

Reporting entities must ensure that their AML/CFT program can detect when customers are being used as mules.

Know Your Customer

The process of establishing and verifying a customer's identity and the nature of their business is a cornerstone of a risk-based AML/CFT program. Robust CDD is vital to the detection of money mules that are opening accounts on behalf of third parties, and proper due diligence should be conducted for all age groups, even for elderly customers who look the least suspicious.


Money mules may be acting on behalf of politically exposed persons (PEPs) or other high-risk individuals. PEP and sanctions screening measures should be implemented to help reporting entities expose customers' connections to high-risk individuals.

Transaction Monitoring

Reporting entities should monitor customer accounts for suspicious transaction patterns. Money mule accounts may be used to facilitate an unusual volume or frequency of transactions or may engage in unusual transaction patterns. Money mule activities may only become apparent after a series of transactions, rather than an isolated payment. Mules are likely to engage in multiple transactions that do not fit their customer risk profile, have no obvious purpose, or involve transfers of funds into and out of high-risk jurisdictions.

To spot suspicious transaction patterns, reporting entities should implement ongoing monitoring measures that capture not only transaction characteristics but also the surrounding context, including recipients and destinations.

Mule accounts are most often unused accounts that previously belonged to genuine holders, who sell them on to criminals, or existing accounts operated normally for a period of time, before being used to receive the proceeds of scams.

 Transaction Indicators of a Potential Mule Account		
Transferred funds were recalled by originating bank under suspicion of scam/fraud through SWIFT.	Complaint on money mule account holder lodged by victim via contact centre or email.	When account is reviewed for a specific retrospective period, high account turnover is observed.
Low account balance.	Account is only active when wire transfer is received, followed by withdrawals.	Suspicious cash deposits, interbank fund transfers that are not consistent with client's profile (e.g. international student).
Police report received by the bank on possible money mule scam.	Adverse news or law enforcement production order.	Forged document provided by account holder to justify account transactions.
Small ATM cash withdrawals or small outward interbank fund transfer to third parties.	Fictional debit narrative on the incoming wire transfer (e.g. "family aid", "financial support", "loan", "prize winnings").	Outward wire transfer to high-risk countries associated with cybercrime.
User behaviour inconsistent over time, including geo location, activities.	IP location hidden.	Hundreds/thousands of small sums paid in and withdrawn in bulk.

Worldwide Actions

Australia

From July 2022, the Australian Communications and Media Authority (ACMA) registered new rules to require telecommunications providers to identify, trace, and block text message scams. Under the rules, telcos must also publish information to assist their customers to proactively manage and report text scams, share information about scam messages with other providers, and report identified scams to authorities.

These new rules complement ACMA rules that came into force on 30 June 2022 that require telcos to use multi-factor ID checks for customer transactions that are commonly targeted by scammers, including SIM swap requests and account changes.

Combatting text and identity theft phone scams are a compliance priority for the ACMA and telcos will face penalties up to \$250,000 if they fail to comply with the new rules.

Singapore

The [Anti-Scam Command \(ASCom\)](#) was implemented on 22 March 2022 to achieve better cooperation between various scam-fighting units within the Singapore Police Force (SPF) by integrating scam investigation, incident response, intervention, and enforcement under one group.

The ASCom partners with more than 80 institutions in the fight against scams. These include local and foreign banks, non-bank financial institutions, Fintech and cryptocurrency companies, and remittance service providers in Singapore.

As part of the collaboration in combating scams, the ASCom and the Monetary Authority of Singapore worked with the banks to co-locate their staff within ASCom premises. Since July 2022, six banks have come onboard to enhance real-time coordination with the Police in investigative efforts, tracing the flow of funds, and freezing bank accounts suspected to be involved in scammers' operations.

United Kingdom

Since December 2021, [Lloyds Banking Group](#) has joined forces with City of London Police to launch the industry's first pilot scheme using proceeds of crime to fund a series of fraud fighting and victim support programmes across the UK. The pilot schemes initiative is beneficial for the National Economic Crime Victim Care Unit (NECVCU) led by London Police, as it provides one-to-one phone support, tips, and aftercare to fraud victims.

One of the bank's biggest successes in freezing funds from the proceeds of crime has been through the 2018 creation of an innovative 'mule-hunting team' to stop the movement of money from scams. The frozen cash will be invested in several projects to tackle fraud as well as increasing education and awareness to help keep more people safe by stopping scams from happening in the first place.

Additional Resources



[Take Five](#) – a UK public/private national campaign that offers [straight-forward advice](#) to help everyone protect themselves from preventable financial fraud.



[Money Mules Fact Sheet](#) – a UK publication aimed at teenagers.



[Money Mules](#) – a booklet outlining how New Zealanders can unwittingly become money mules for international fraudsters. Produced by [Te Ara Ahunga Ora Retirement Commission](#) and the NZ Police, the booklet details how Kiwis can protect themselves and what to do if they think they've been used as a money mule.

INTERNATIONAL AML/CFT NEWS

Australia

[Foreign call centre raided over alleged links to scam tricking Australians out of their superannuation](#)

A call centre located in the Philippines recently raided by the Philippine National Police Anti-Cybercrime Group is allegedly linked to sophisticated multi-million-dollar scams that targeted Australians.

According to Australian cyber-crime investigator Ken Gamble, who accompanied the Philippine Police during the raid, staff at the centre were pretending to be calling from Melbourne, Australia. The raid was triggered by Mr Gamble's firm IFW Global lodging a criminal complaint in the Philippines on behalf of six Australian victims.

Nigeria

[Nigerian authorities raid cybercrime training centres](#)

Nigerian authorities raided several schools specialised in teaching internet fraud and arrested two owners and seven students, according to the country's Economic and Financial Crimes Commission (EFCC). It is unknown how widespread such schools are but at least three similar facilities have been detected since 2019.

The most common types of cybercrime practiced in Nigeria include romance scams, phishing, impersonation, and crypto fraud.

United States

[Mastercard pushes deeper into crypto with new tool for combating fraud](#)

Mastercard has debuted a new piece of software that helps banks identify and cut off transactions from fraud-prone crypto exchanges. The system relies on data from the blockchain and uses artificial intelligence algorithms to determine the risk of crime associated with crypto exchanges on the Mastercard payment network.

On the Crypto Secure platform, banks and other card issuers are shown a dashboard with colour-coded ratings representing the risk of suspicious activity, with severity of risk ranging from red for "high" to green for "low". Crypto Secure doesn't make a judgement call on whether to turn away a specific crypto merchant; that decision is left to the card issuer.

Wales

[Santander expert's warning on new twist to 'Hi mum' and 'Hi dad' text message scam](#)

A fraud expert at a major Wales bank is warning of a recent pick-up in fake messages purporting to be from relatives, with some involving requests to transfer money to a friend or family member before it is sent on to the scammer. Similar scams have also appeared on WhatsApp in recent months.

Corruption

[Zambia: Auditors expose 9,800 ghost workers in government ministries](#)

The audit of government payroll by Zambia's Office of the Auditor General published recently reveals a series of grave misuse of public money including that between 2017 and 2021, ministries paid more than US\$45 million (NZ\$77m) in regular salaries to 9,800 apparently non-existent individuals.

Among other instances of embezzlement, the auditors detected 87 individuals who were diverting funds reserved for salary payments to private accounts outside the civil service, and some officials had been paid for periods up to 14 years despite being suspended.

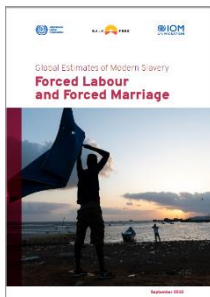
Illegal Fishing

[South Australian scientists are tracking the origins of seafood to fight illegal fishing and fraudulent labelling](#)

A new technology developed by South Australian scientists is tracking the origins of seafood in a bid to combat fraudulent labelling and improve sustainability. University of South Australia marine ecologist Zoe Doubleday and her team have developed technology to find the source of seafood by testing bones and shells of marine creatures for oxygen isotopes.

The isotopes are compared in a database to locate the origins of seafood by ocean temperature; the method is universal and can test for many marine species. The next challenge for researchers is to determine how far east or west a fish is from, allowing regulators to pinpoint the exact origin of that catch.

Modern Slavery



[Global Estimates of Modern Slavery: Forced Labour and Forced Marriage](#)

According to the latest Global Estimates of Modern Slavery report by the International Labour Organization (ILO), 50 million people were living in modern slavery in 2021. Of these people, 27.6 million were in forced labour, including 3.3 million children, and 22 million were trapped in forced marriages.

The report notes most cases of forced labour (86%) are found in the private sector, with state-imposed forced labour accounting for 14 percent, and that slavery is not confined to poor countries, with more than half of all forced labour occurring in wealthier countries in the upper-middle or high-income bracket.

Russia Sanctions

[US charges British man with helping Russian oligarch evade sanctions](#)

A British businessman was arrested in the United Kingdom on charges of helping Russian oligarch Oleg Deripaska evade sanctions imposed by the United States. The businessman is accused of

wiring more than US\$1 million (NZ\$1.7m) to cover the upkeep of three homes belong to Deripaska in the United States. The indictment against him also states that he used his own credit card to pay over US\$12,000 (NZ\$21k) to move Deripaska's artwork from New York to London, and planned to bill Deripaska afterward.

Wildlife Trafficking

[Malaysian extradited to US for alleged rhinoceros horn smuggling](#)

An alleged wildlife trafficker from Malaysia has been extradited to the United States on charges of participating in a conspiracy to traffic more than 70kg of rhinoceros horns valued at more than US\$725,000 (NZ\$1.2m).

The US Department of Justice alleged that the trafficker had specialised in the smuggling of rhino horns from poaching operations in Africa to customers primarily in Asia, though he also claimed to be able to ship the horns to the US. The US Treasury Department also announced sanctions on the trafficker, his alleged transnational criminal organisation, and a Malaysian firm for alleged "cruel trafficking" and trading in the "products of brutal poaching."

Basel Institute on Governance



[The Basel AML Index](#)

The Basel AML Index is a leading independent ranking of money laundering and terrorist financing (ML/TF) risks around the world. The index provides risk scores based on data from 18 publicly available sources such as the Financial Action Task Force (FATF), Transparency International, the World Bank and the World Economic Forum.

The risk scores cover five domains considered to contribute to a high risk of ML/TF: Quality of AML/CFT Framework; Bribery and Corruption; Financial Transparency and Standards; Public Transparency and Accountability; Legal and Political Risks.

Royal United Services Institute (RUSI)



[The Illicit Finance Threat to Democracies: A Transatlantic Response](#)

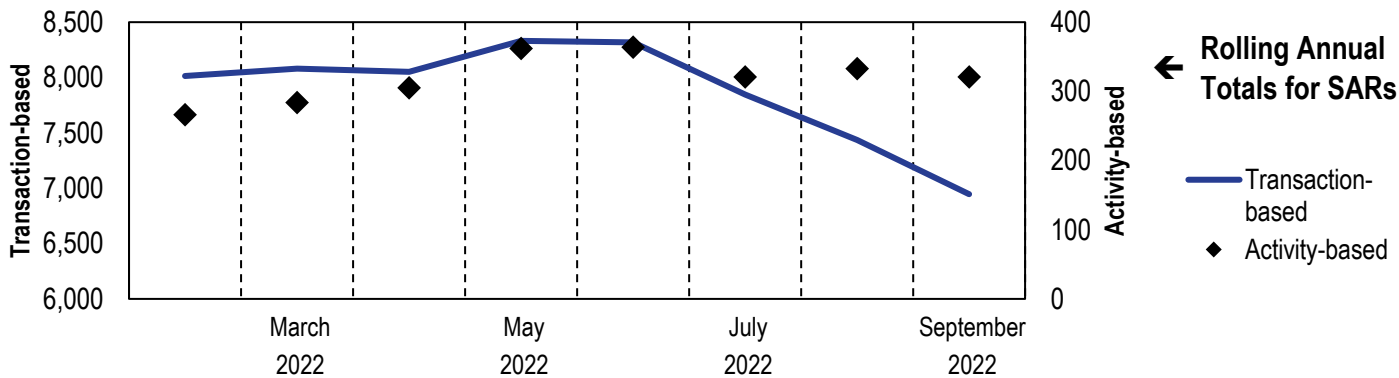
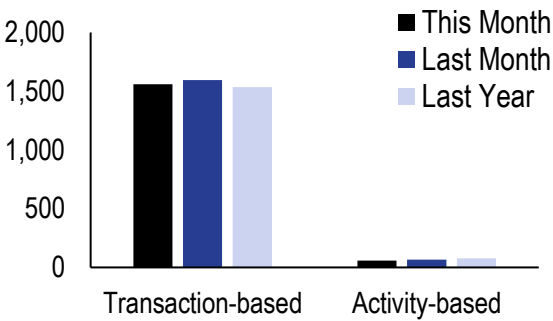
This Policy Brief draws its recommendations from the Taskforce on Transatlantic Response to Illicit Finance (TARIF), which was established in July 2021 by the Centre for Financial Crime and Security Studies at RUSI in response to the growing acknowledgement of the illicit finance threats posed by kleptocratic and corrupt actors to democratic societies, specifically those of the United States and the United Kingdom.

This Policy Brief explores how the US and the UK are exposed to and should respond to the illicit finance that undermines democratic societies. These two countries – as global leaders, financial hubs, and favoured destinations of illicit financial flows – are in a unique position to take on international leadership in responding to this threat.

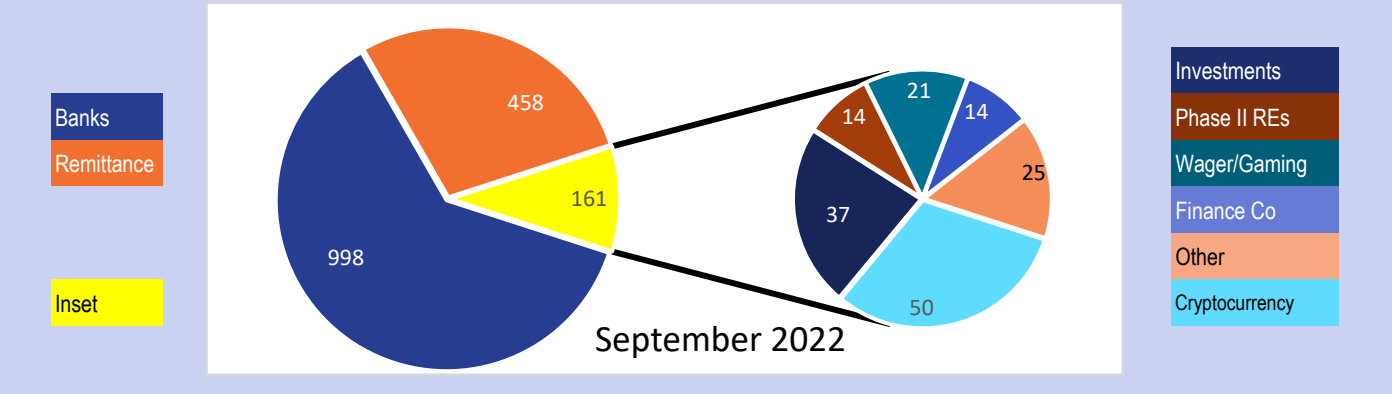
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This Month	Last Month	Last Year
	September	August	September
	2022	2022	2021
Transaction-based	1,559	1,595	1,536
Activity-based	59	65	78
Total	1,618	1,660	1,614

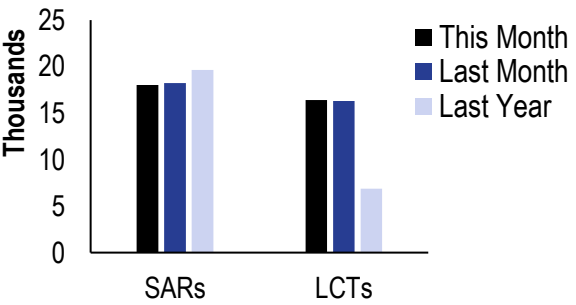


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

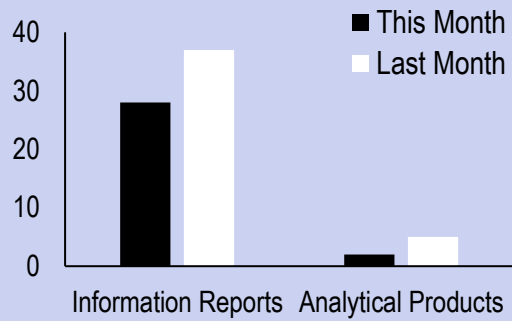
	This Month	Last Month	Last Year
	September	August	September
	2022	2022	2021
SARs	18,007	18,230	19,653
IFTs	426,165	518,952	424,206
LCTs	16,401	16,291	6,867



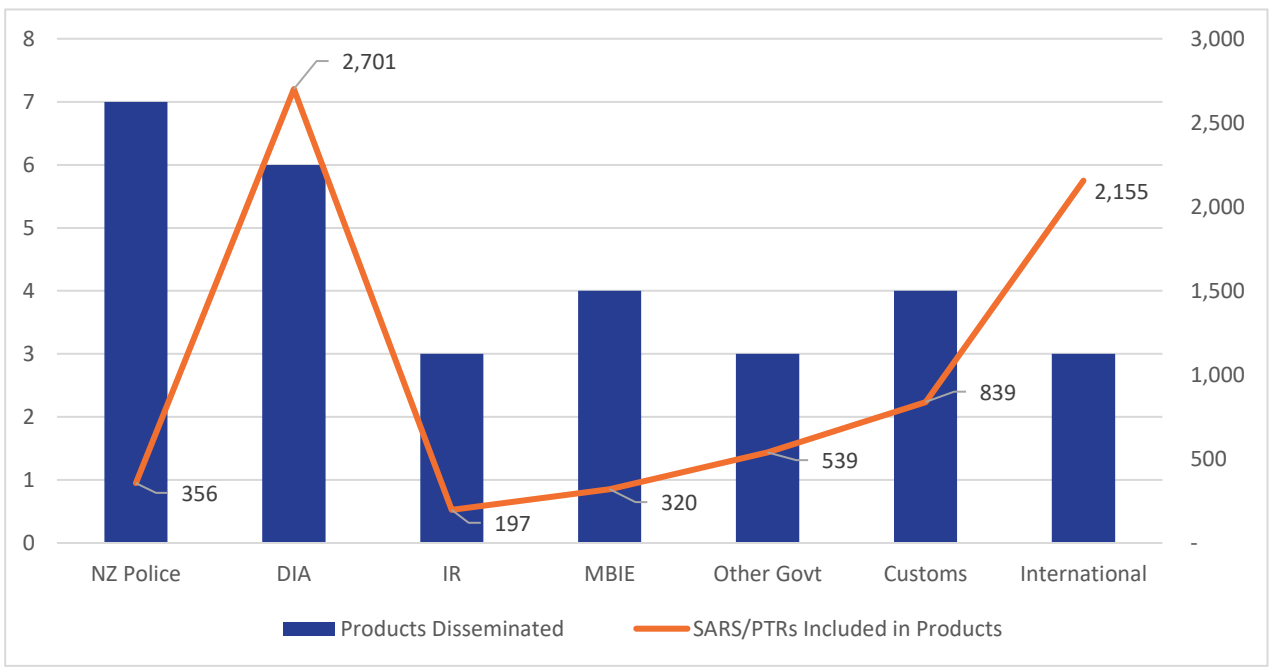
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

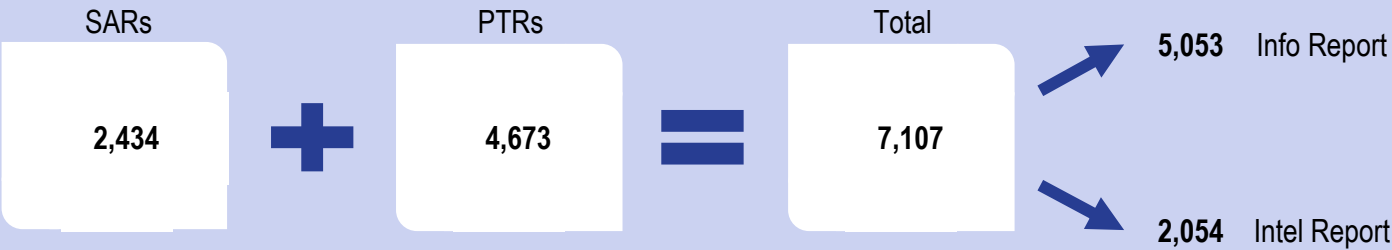
	This Month	Last Month
	September	August
	2022	2022
Information Reports	28	37
Analytical Products	2	5
Total Products	30	42



Disseminations of Products by Recipient



Disseminations of Products by Included SARs and PTRs



*Statistical data for transaction reporting and intelligence products may be updated as new information is processed, and so there may be minor discrepancies between the statistical figures contained in this report and subsequent reports.

QUARTERLY STATISTICS*

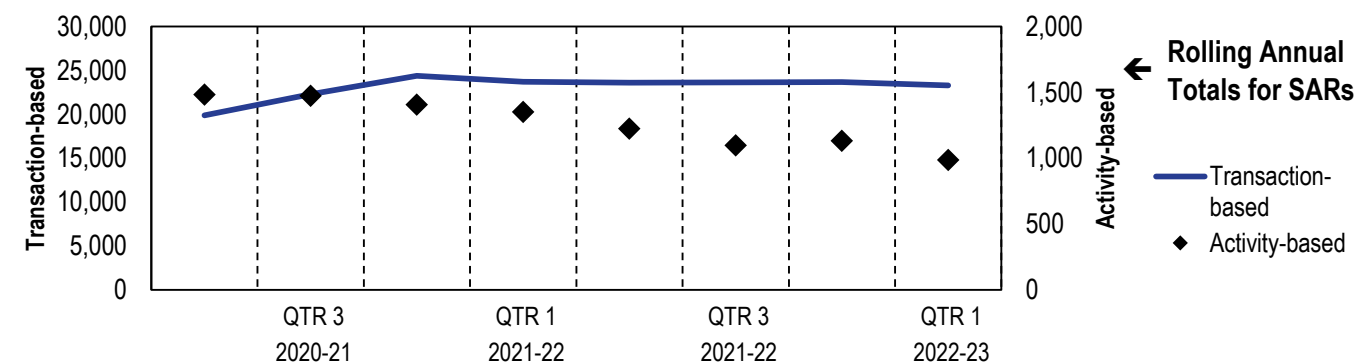
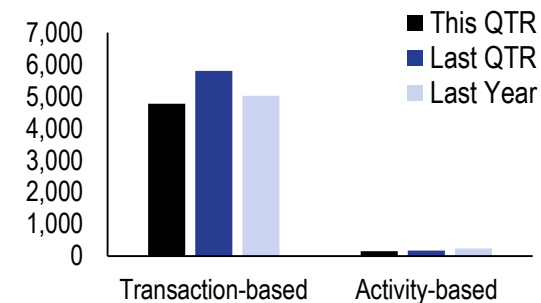
NEW ZEALAND POLICE FINANCIAL INTELLIGENCE UNIT

QTR 1 | 2022-23

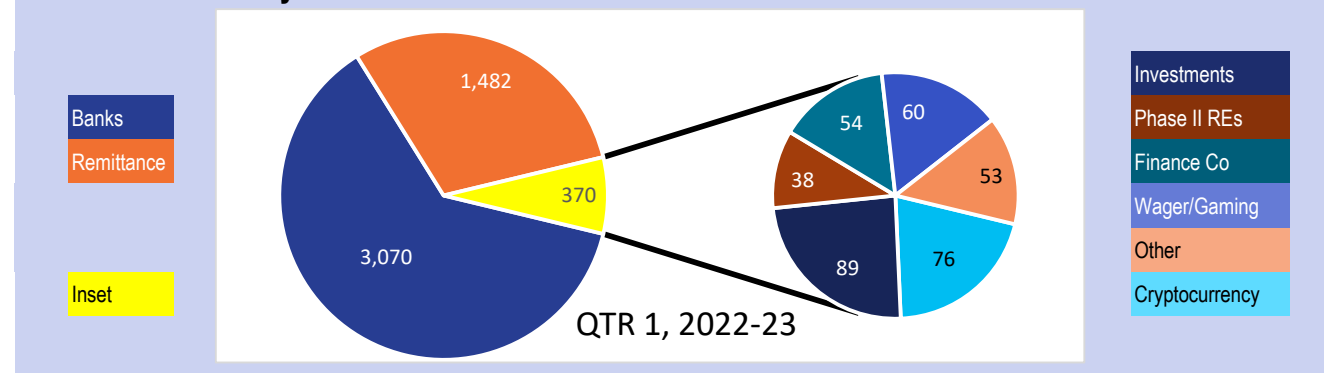
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This QTR	Last QTR	Last Year
	QTR 1	QTR 4	QTR 1
	2022-23	2021-22	2021-22
Transaction-based	4,768	5,802	5,015
Activity-based	157	169	240
Total	4,925	5,971	5,255

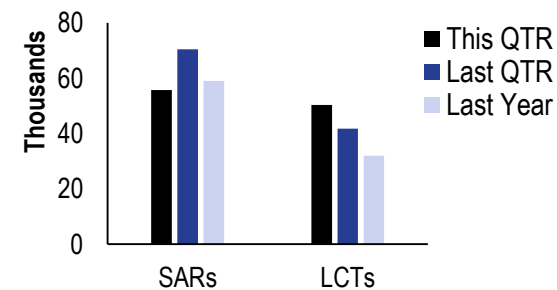


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

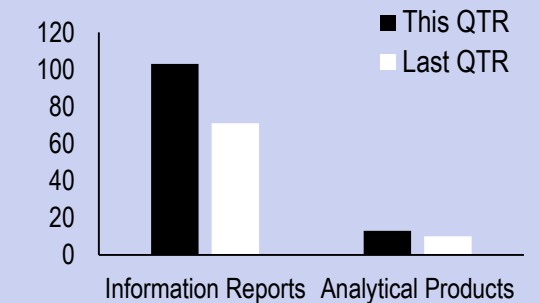
	This QTR	Last QTR	Last Year
	QTR 1	QTR 4	QTR 1
	2022-23	2021-22	2021-22
SARs	55,731	70,423	59,050
IFTs	1,447,788	1,812,675	1,308,474
LCTs	50,329	41,747	31,925



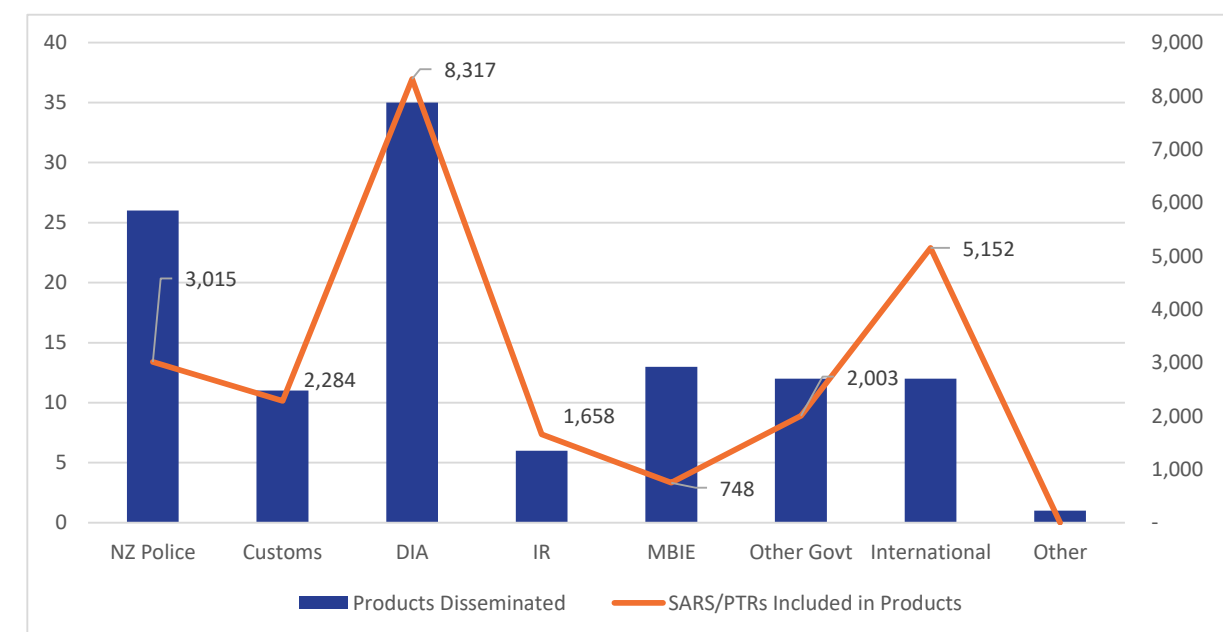
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

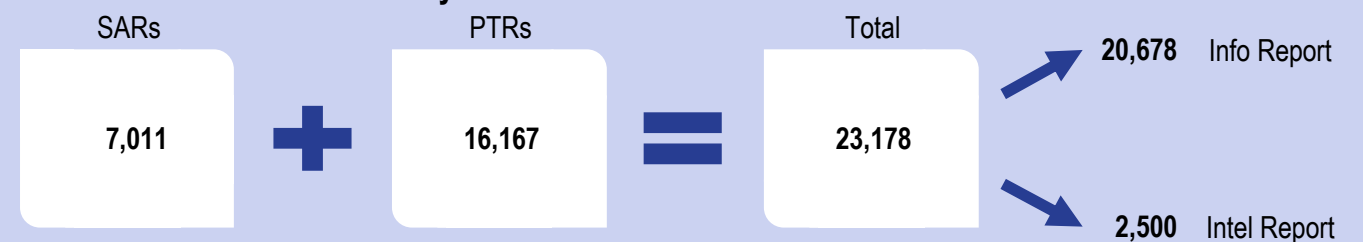
	This QTR	Last QTR
	QTR 1	QTR 4
	2022-23	2021-22
Information Reports	103	71
Analytical Products	13	10
Total Products	116	81



Disseminations of Products by Recipient



Disseminations of Products by Included SARs and PTRs



*Statistical data for transaction reporting and intelligence products may be updated as new information is processed, and so there may be minor discrepancies between the statistical figures contained in this report and subsequent reports.

