

The Suspicious Activity Report

DECEMBER/JANUARY 2021

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 Iain Chapman. 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. It is the result of a review of AML/CFT legislation and aims to assist in detecting and deterring money laundering, contributing to public confidence in the financial system and achieving 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 headquarters group.

Financial Intelligence Unit

The Financial Intelligence Unit is led by Detective Inspector Christiaan Barnard and has been operational 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 is led by Detective Inspector Craig Hamilton and was established in December 2009 specifically 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 (ARUs), based in Whangarei, Auckland, Waikato/Bay of Plenty, Wellington, and Christchurch.

Money Laundering Team

The Money Laundering Team (MLT), led by Acting Senior Sergeant Benjamin McLaughlin, 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 investigate 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.

FINANCIAL INTELLIGENCE UNIT UPDATE

Notes from the Head of FIU

Detective Inspector Christiaan Barnard



The nearly two-year process for the Mutual Evaluation is coming to a close with the FATF plenary occurring in the last week of February. The final report will not be released until May 2021, but I can say that it is a well written report that fairly reflects the state of the AML/CFT landscape in New Zealand and it provides a number of pragmatic recommendations on how we can improve the framework, which in turn will harden the environment for organised crime.

This serves as a reminder that New Zealand is not in a bubble and in addition to demonstrating our commitment to the international community, our approach recognises the importance of international partnerships. The FIU has a range of active international partnerships that we use to ensure that relevant financial intelligence is shared, assists us with understanding strategic risk, and enables us to assist with capacity building where appropriate.

Outside of the standard-setting bodies (the [FATF](#) and the [APG](#)), the [Egmont Group](#) of FIUs is our key international partnership. With 166 FIU members (and growing) it provides the forum for international engagement and the ability to securely exchange financial intelligence. Between 2016 and 2019 the FIU has responded to over 380 requests for assistance from foreign countries and has sent more than 180 requests. During this same period, approximately 500 intelligence reports were shared with international partners.

The FIU is also an active member in the Financial Intelligence Consultative Group (FICG), which holds the [Counter-Terrorism Financing Summit](#). FICG is comprised of the 12 member countries' members of Australia, New Zealand and the Association of Southeast Asian Nations ([ASEAN](#)). In addition to holding five international CTF Summits, this group has collaborated to produce several strategic products on topics such as [corruption](#) and the [TF risk for non-profit organisations](#).

An exciting development is the newly created Pacific Financial Intelligence Community (PFIC). The foundation members of this group are Australia, New Zealand, Papua New Guinea, and Fiji with the co-chairs for the first two years being Australia ([AUSTRAC](#)) and Papua New Guinea ([FASU](#)). The group aspires to increase its membership and its focus is to identify, develop, and operationalise strategies to combat money laundering and terrorist financing matters in the Pacific. The first PFIC meeting was held in February 2021 and with the goodwill already shown, it will become an important element of our international engagement at a regional level.

Despite being geographically isolated, New Zealand is very well connected to the rest of the world and works to support our international partners while hardening our own economy against abuse by organised crime.

FIU News

Operation Gandolf selected to be included in the BECA Book II

In 2017, the FIU submitted [Operation Gandolf](#) to the Best in Egmont Cases Awards (BECA) and has recently been notified that the operation was chosen to be included in the BECA Book II, scheduled to be published in mid-2021.

Operation Gandolf was a multi-agency investigation into the importation of methamphetamine. The investigation was led by the Organised and Financial Crime Agency of New Zealand (OFCANZ, now New Zealand Police's National Organised Crime Group) and supported by New Zealand Customs Service (Customs), the Department of Corrections (Corrections) and the New Zealand Police Financial Intelligence Unit (FIU).

The primary target of Operation Gandolf was Egyptian national Mohamed Soliman Hussain Atta, who was at the centre of an organised crime group that orchestrated imports and distribution of methamphetamine throughout New Zealand. At the time, Atta was incarcerated at Rimutaka Prison for importation of cocaine and aggravated robbery. The investigation was sparked by two STRs, one each received from a bank and an international money remitter.

Starting in April 2014, initial FIU analysis established that between February and April 2014, eight New Zealand-based persons residing in four different regions had facilitated 20 separate transactions to five Thai-based persons to a total value of NZ\$178k. The FIU also found links to active New Zealand Police and Customs operations, identified associations with New Zealand gangs, and to individuals incarcerated in New Zealand prisons. They also identified individuals with historical criminal convictions including drug-related offending.

During the analysis stage, a total of 23 intelligence products were produced by the FIU, supported by 69 STRs containing 486 individual transactions received from Reporting Entities. All these intelligence products were used by investigators from OFCANZ, Customs, Corrections and the Asset Recovery Unit.

The results of Operation Gandolf included 15 defendants being charged with a variety of offences. Thirteen of the defendants have been sentenced to 48 years imprisonment combined. Atta was sentenced in 2016 to 13 years and two months imprisonment.



Indicators/Red Flags

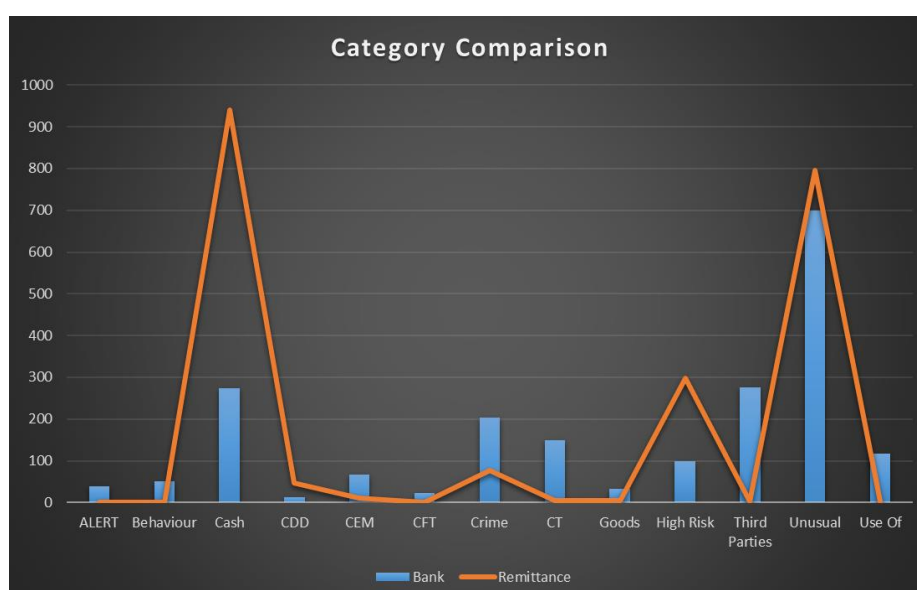
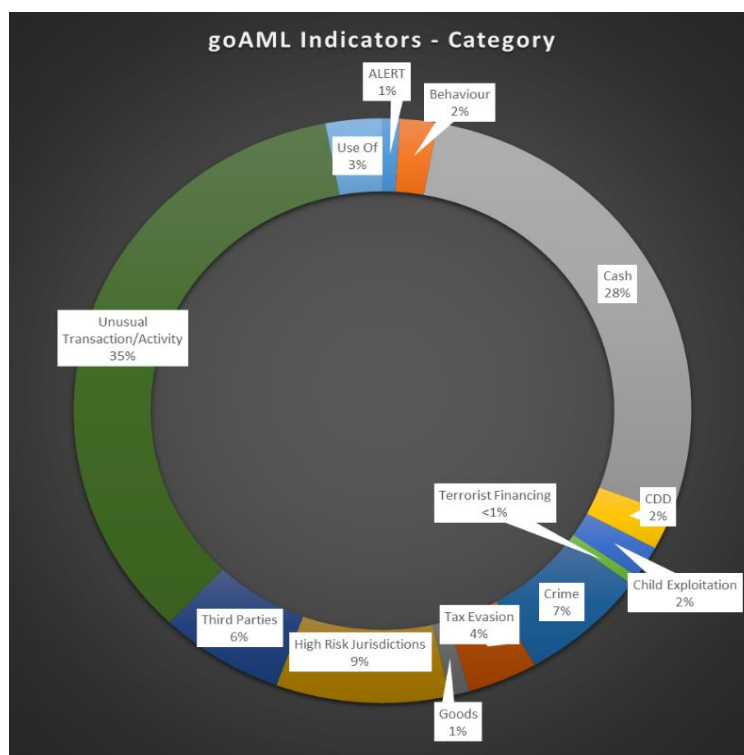
- Large cash transactions with a rapid movement of funds
- Unusual transactional behaviour – out of character with historic account transactional activity
- Smurfing – multiple persons making payments to a receiver rather than one larger transaction
- Structuring – splitting transactions into separate amounts under AU\$10k to avoid the transaction reporting requirements of the Australian FTR Act and New Zealand AML/CTF Act.

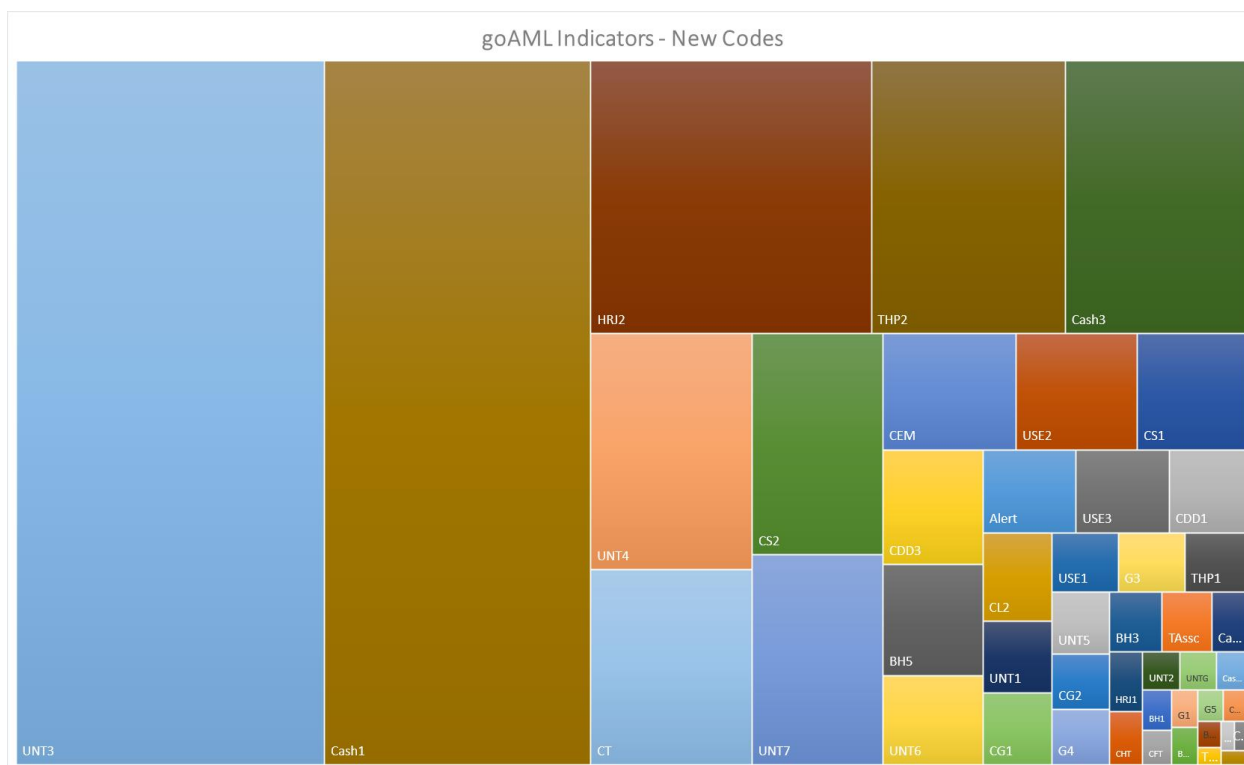
Suspicious Activity Reporting to the FIU with New Indicators

The new goAML indicators were uploaded in December 2020 and by the end of January 2021, nearly 100% of the Suspicious Activity Reports and Suspicious Transaction Reports (together, 'SARs') were submitted with at least one behaviour indicator selected. As seen in prior periods, the majority of SARs received in December 2020 and January 2021 were submitted by banks and other financial institutions (46%) and remittance companies (50%).

The first chart below shows the percentage of SARs by category received in January 2021 from all reporting entities. For better visibility, the categories of Child Exploitation and Tax Evasion have been split out from the new general Crime category, and the Use of (Casinos or Professional Services) category has been carved out of the Unusual Transaction/Activity grouping.

The second chart highlights the categories reported by the two largest reporting entity types.

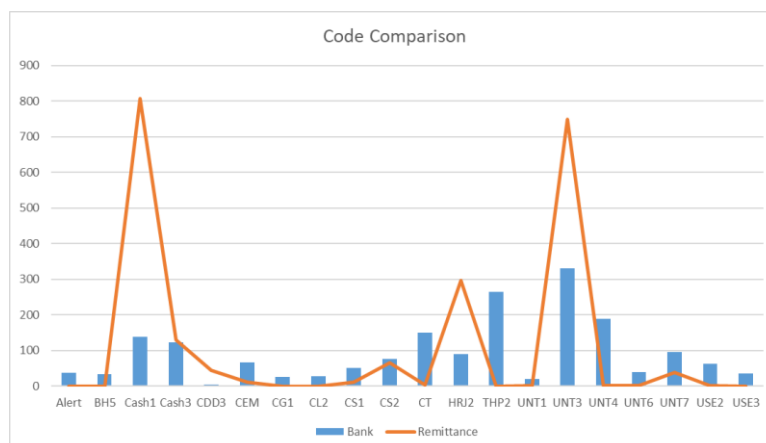




The Treemap above reveals the top five of the 49 new indicator codes as reported in January 2021 by all reporting entities were:

1. UNT3 – Unusual Transaction – Financial profile or activity changes or is different than what is expected.
2. Cash1 – Large deposits from one person to multiple accounts, or from multiple people to one account
3. HRJ2 – High Risk Jurisdiction – Transaction/activity involves high risk or sanctioned jurisdiction(s)
4. THP2 – Third Party – Inward/Outward payment from/to unrelated party
5. Cash3 – Cash/Location – multiple cash deposits at different locations within a short time frame.

The comparison graph below of the indicators selected by banks and remitters in January 2021 highlights the differences in the suspicious activity and transactions they encountered:



The greatly improved indicator selection will allow the FIU to better analyse and understand the AML/CFT risks in New Zealand, as well as help inform the National Risk Assessment.

News from our Partners

[FMA reminds Chinese New Zealanders how to spot investment scams](#)



Chinese New Zealanders are urged to be aware of investment scams in the current economic climate, and to report any investment scams to the Financial Markets Authority (FMA). In 2020, the FMA received only a handful of complaints of scams from Chinese New Zealanders, despite a 2020 FMA survey finding around one in five

Chinese New Zealanders had been approached about a potential investment scam. The FMA's Chinese-speaking staff are dedicated to investigating scams, and its call centre uses interpreters to help complainants when English is not their first language.

[AUSTRAC Junket Tour Operations in Australia Risk Assessment](#)

In December 2020, the Australian Transaction Reports and Analysis Centre (AUSTRAC) published a risk assessment of gambling junket tour operations based on financial data and intelligence gathered between April 2018 and March 2019. During that period, eight out of 13 casinos conducted junket programs, although one has since stopped such operations. AUSTRAC found the junket sector faced multiple criminal threats, with the overall risk of money laundering and terrorism financing to be high.



[United Kingdom National Risk Assessment](#)



The United Kingdom's National Risk Assessment of Money Laundering and Terrorist Financing 2020 report, compiled by the Treasury and the Home Office, was published in December 2020. The report found there is now a high likelihood of buyers using UK real estate to disguise illegal activity, up from a medium risk in 2017. The findings also upgraded the risk level for the estate agency sector from low to medium, due to law enforcement agencies observing increased overseas buyers and overseas cash flows into the UK property market. Red flags included clients seeking anonymity by buying property through complex corporate structures based in 'secrecy jurisdictions', clients buying property without a mortgage and no "verifiable source of income" and transactions involving multiple law firms.

[Project CRAAFT & RUSI: Financing Right-Wing Extremism and Terrorism briefing](#)

Project CRAAFT is an academic research and community-building initiative designed to build stronger, more coordinated counter-terrorist financing capacity across the EU. It is funded by the EU's Internal Security Fund-Police and implemented by a Consortium led by RUSI Europe. Project CRAAFT have published a briefing paper and webinar that analyses trends in the financial activities of right-wing extremists and terrorists around the world. The impact of the global pandemic on the present and future of right-wing extremist financing is also discussed.



INTERNATIONAL AML/CFT NEWS

China

[Campaign against fraud bars the use of other people's phone and bank cards](#)

Chinese authorities recently conducted a nationwide “Card Breaking Campaign”, an operation to crack down on illicit bank card transactions and bank card sales to combat telecommunications fraud and cross-border online gambling. This new type of crime has created an illegitimate industry employing 5 million to 6 million people and involving information technology, payment settlements and operations. The complex payments and money laundering system utilises small individual players who loan or lease financial credentials to offshore criminal groups, which then help illegal gamblers hide money from authorities, often using Tether’s USDT cryptocurrency.

Israel

[Cash and carry](#)

In December 2020, the Israel Tax Authority Committee for imposing Financial Sanctions published 96 cases it had ruled on in 2018. The Israel Tax Authority imposed NIS 2.4m [NZ\$1.02m] in fines, with 72% of the violations taking place at land borders, and 28% at airports. The cases included a Russian billionaire, a mystery package, and cash in the belly of a fish.



Under the terms of the Prohibition on Money Laundering Law, Israelis are obliged to report to the authorities when they cross the border with more than NIS 50,000 [NZ\$21,000] via airports, or NIS 12,000 [NZ\$5,100] at land border crossings. One man was apprehended at Ben Gurion Airport when he informed authorities that he had hidden US\$40,000 [NIS 130,000] in cash in the belly of a frozen fish in his luggage when faced with the destruction of the fish; it is prohibited to bring meat and fish products into Israel.

Netherlands

[Criminals use potato exports to launder money](#)

The Fiscal Information and Investigation Service (FIOD) has recently released their [2020 annual report](#). In an interview, FIOD chief Bert Langerak stated that Dutch criminals are increasingly using exports to Africa to launder money, which is subsequently invested in diamonds and gold from the continent. FIOD investigations found criminals ‘exported’ at least €150m [NZ\$251m] worth of produce, particularly potatoes, to Africa in the last five years.

FIOD investigators also found that over €120m [NZ\$201m] had been laundered via the export of lease cars in 2020. Langerak noted that “the perception of the car trade is that there is a lot of cash floating around there but that is not true. Most of the cash is probably criminal cash”.

Switzerland

[Credit Suisse charged over Bulgarian wrestler's cocaine smuggling ring](#)

A Bulgarian wrestler was able to launder CHF 35m [NZ\$54m] from a European cocaine trafficking ring through Switzerland, allegedly aided by a (now former) employee of Credit Suisse who set up 'special finance transactions' involving real estate and other deals through which the drug money was laundered. The case has been under investigation since the early 2000s, when authorities began tracking the wrestler, who cannot be named due to Swiss law.

United Kingdom

[Millions seized after 'pay per view' entertainment money laundering racket smashed](#)

An investigation by the Greater Manchester Police's (GMP) Economic Crime Unit, a specialised unit within GMP's Serious Organised Crime Group, recovered more than £5m [NZ\$9.6m] from fraudulent companies who used adult entertainment websites as part of an international money laundering racket. The investigation involved three Manchester-based companies that were linked to adult entertainment websites offering 'pay per view' services. Enquiries established that criminals had taken advantage of the websites' third-party payment process and were not offering the services advertised.

United States

[Woman defrauded hundreds of immigrants](#)

A Florida woman, Laura Torres, pleaded guilty in December 2020 to immigration fraud, laundering government money and making false statements to the US Department of Agriculture.

Torres offered to help undocumented immigrants for a fee, but instead filed fraudulent asylum applications and coached immigrants who made it to the interview stage on how to lie to authorities. She also stole the identities of those who received work permits and filed fraudulent income tax returns, using an address she controlled. The tax refunds were deposited into the bank accounts of an immigration lawyer, who received a 10% cut to receive the money and transfer it back to Torres. Torres laundered the money by purchasing real estate in Florida over the course of several years.

[Russian pleads guilty to money laundering in international cybercrime investigation](#)

A Russian national, Maksim Boiko, has pleaded guilty to one count of conspiracy to launder money. He is among 20 Eastern Europeans accused in Pittsburgh, Pennsylvania as part of an investigation into QQAazz, an organized crime group that provides money laundering services for cybercriminals worldwide. The network opened and maintained hundreds of corporate and personal bank accounts at financial institutions around the world to receive money stolen by cybercriminals. The funds were then transferred to QQAazz-controlled accounts or converted to crypto currency.

PEPs

[Firm for 'ultra-rich' fined for money laundering breaches](#)



Malta's Financial Intelligence Analysis Unit (FIAU) announced in December 2020 that Insignia, a luxury lifestyle management group, has been fined over several anti-money laundering compliance breaches. A politically exposed Russian with alleged ties to the mafia had been flagged by the FIAU after using a membership-only credit card service company. An onsite

inspection of Insignia revealed how the firm had failed to file a STR about its Russian client despite open source media reports on his ties with the Russian mafia and other red flags.

Sanctions

[Money laundered through Middle East, Africa to dodge Iran sanctions](#)

Two brothers have been charged with conspiracy to violate sanctions and smuggling. The men, Iranian citizens living in Ontario, Canada, are accused of routing financial transactions through the UAE, Uganda, China, Turkey and Canada, in what US prosecutors allege was money laundering. According to the recently unsealed indictments, the men purchased equipment in the US and Spain, and arranged to ship it via the UAE while hiding that the end destination was Iran.

Countering the Financing of Terrorism

[Government of Canada lists 13 groups as terrorist entities, including the Proud Boys](#)

The Government of Canada has placed 13 new groups on the *Criminal Code* list of terrorist entities, including four ideologically motivated extremist groups: Atomwaffen Division, the Base, [the Proud Boys](#) and Russian Imperial Movement. The *Criminal Code* mandates severe penalties for people and organizations that deal with property or finances of a listed entity.

[FBI probing if foreign governments, groups funded extremists](#)

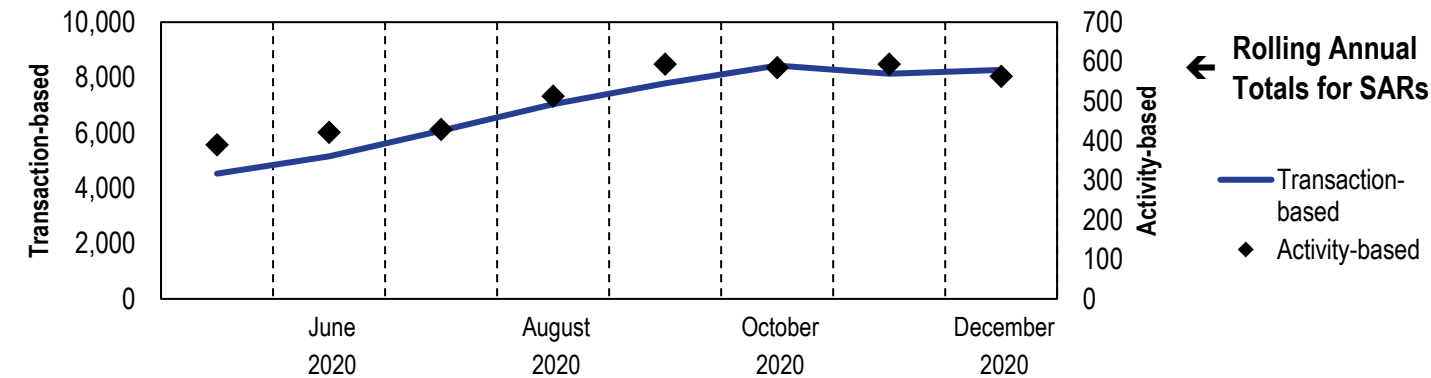
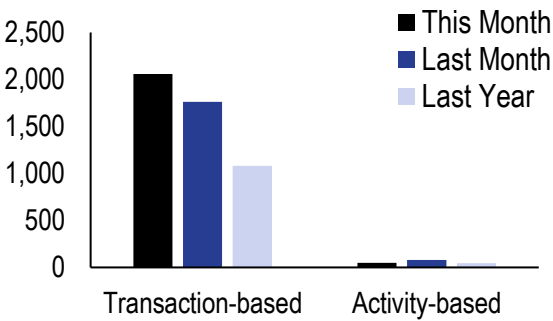
The FBI is investigating whether foreign governments, organisations or individuals provided funding to those who helped plan and execute the insurrection at the US Capitol on 6 January 2021. Part of the investigation will examine bitcoin payments made to key figures and groups a month before the attack, as documented by Chainalysis. At a news briefing, Michael Sherwin, the US attorney in Washington DC stated, "We're looking at and treating this just like a significant international counterterrorism or counterintelligence operation. We're looking at everything: money, travel records, looking at disposition, movement, communication records."

Chainalysis, a New York-based enterprise specialising in countering money laundering and fraud in digital currency, detailed in a January 2021 [blog post](#) that a French donor made payments in bitcoin worth more than US\$500,000 [NZ\$692,000] to 22 different virtual wallets in a single transaction. Many of the wallets belong to far-right activists and internet personalities, including some present at the US Capitol insurrection on 6 January 2021. The payments were made on December 8, 2020, although it is not certain the donations directly funded the insurrection or any associated activity.

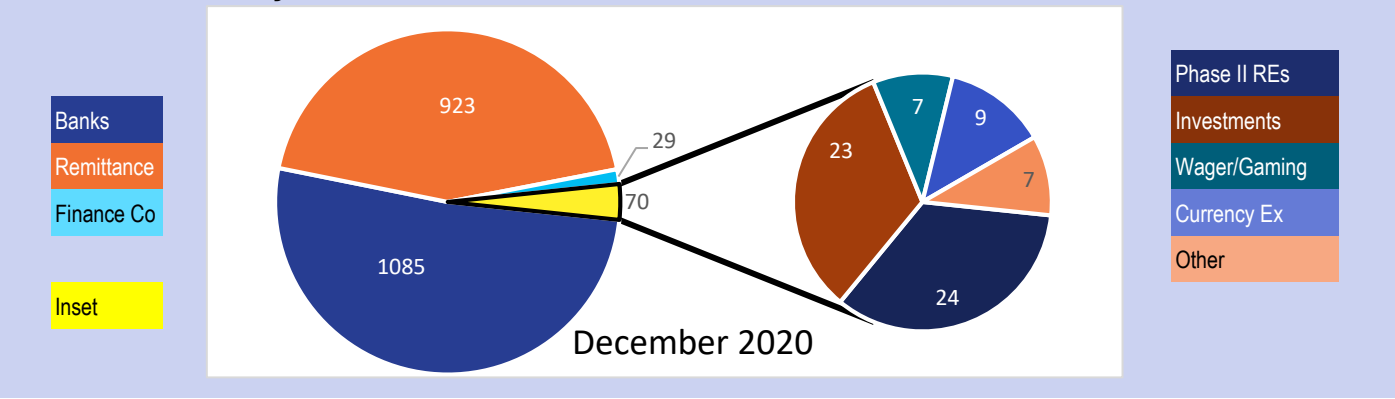
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This Month	Last Month	Last Year
	December	November	December
	2020	2020	2019
Transaction-based	2,059	1,761	1,080
Activity-based	48	79	46
Total	2,107	1,840	1,126

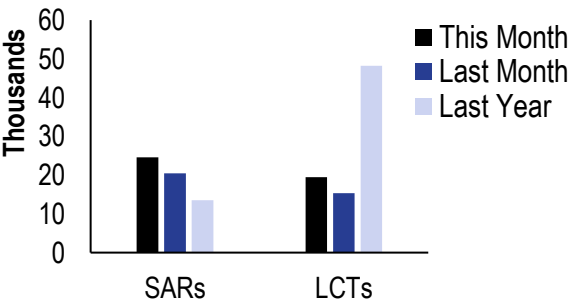


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

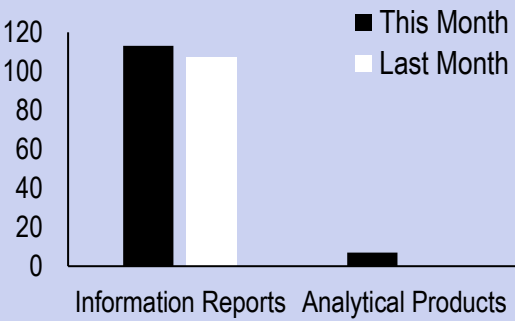
	This Month	Last Month	Last Year
	December	November	December
	2020	2020	2019
SARs	24,596	20,426	13,521
IFTs	465,046	403,735	459,663
LCTs	19,488	15,301	48,233



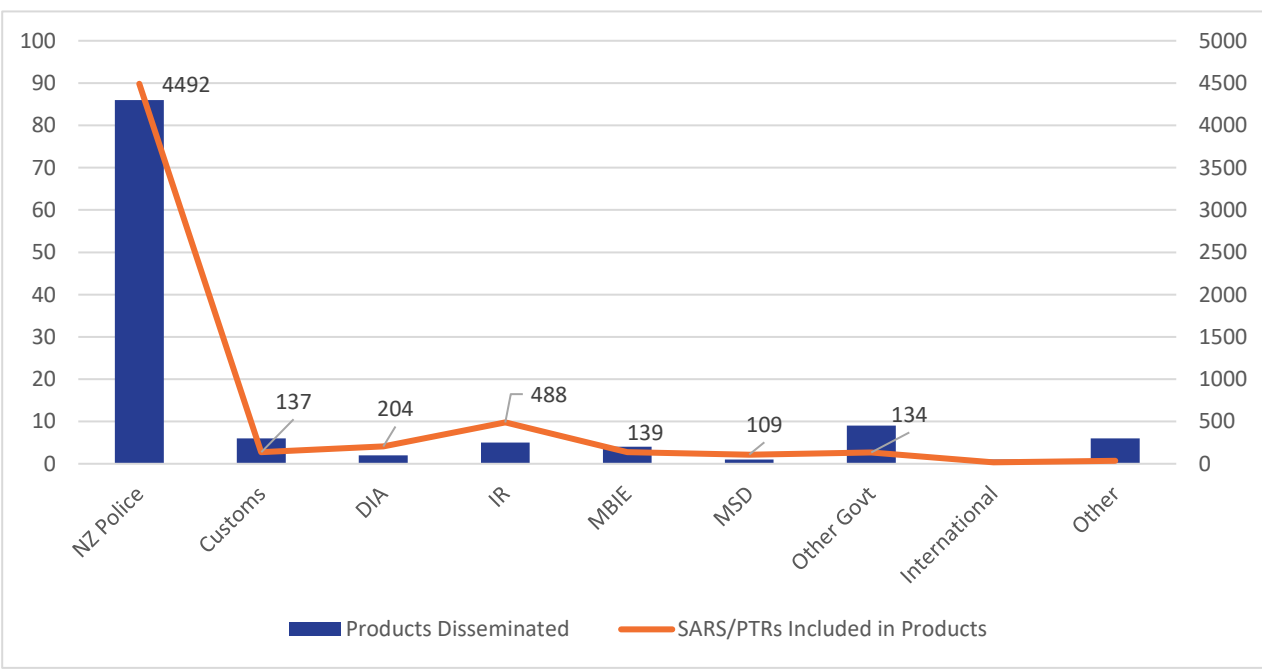
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

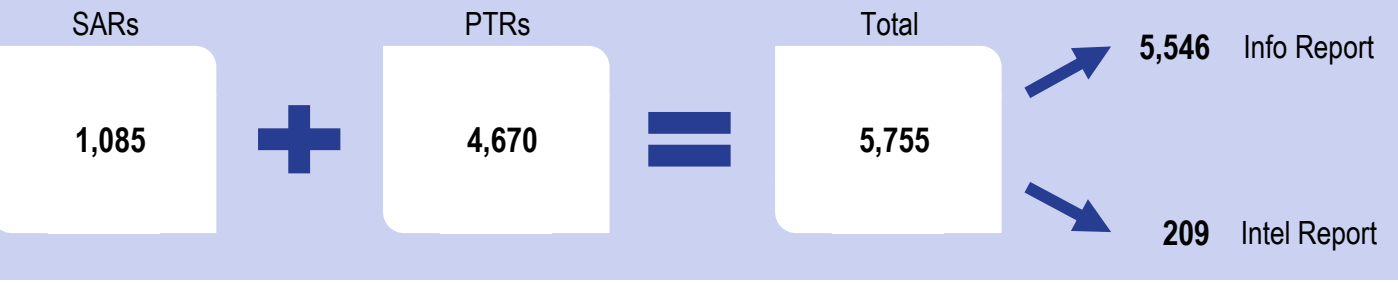
	This Month	Last Month
	December	November
	2020	2020
Information Reports	113	107
Analytical Products	7	0
Total Products	120	107



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*

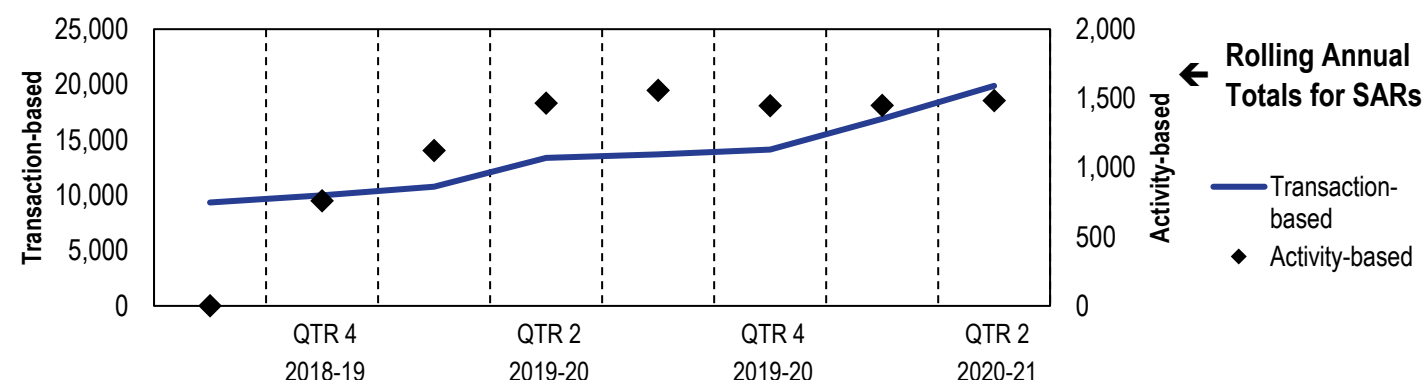
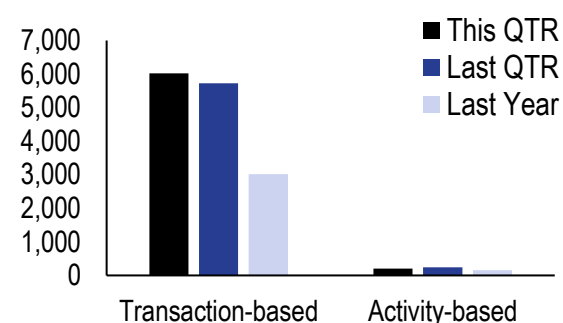
NEW ZEALAND POLICE FINANCIAL INTELLIGENCE UNIT

QTR 2 | 2020-21

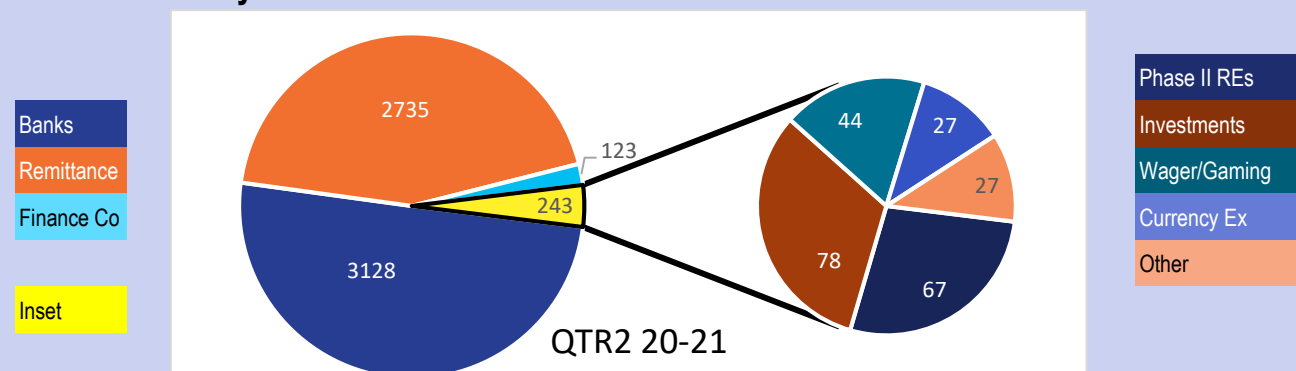
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This QTR	Last QTR	Last Year
	QTR 2	QTR 1	QTR 2
	2020-21	2020-21	2019-20
Transaction-based	6,024	5,722	3,020
Activity-based	205	240	159
Total	6,229	5,962	3,179

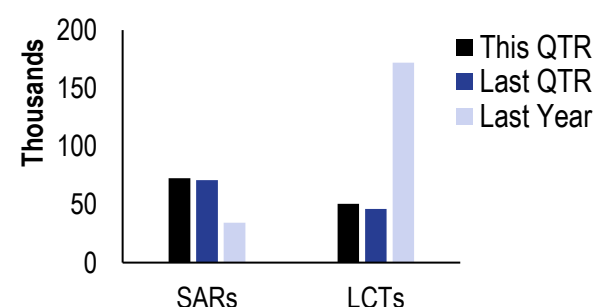


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

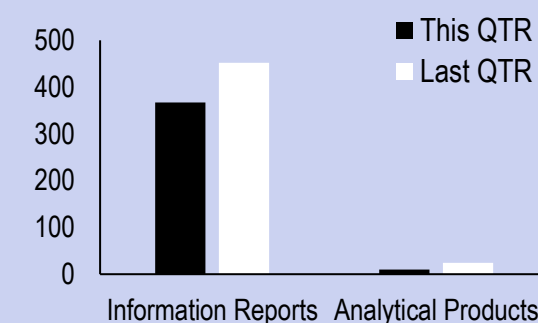
	This QTR	Last QTR	Last Year
	QTR 2	QTR 1	QTR 2
	2020-21	2020-21	2019-20
SARs	72,669	70,986	34,348
IFTs	1,293,591	1,290,544	1,353,315
LCTs	50,658	46,150	171,895



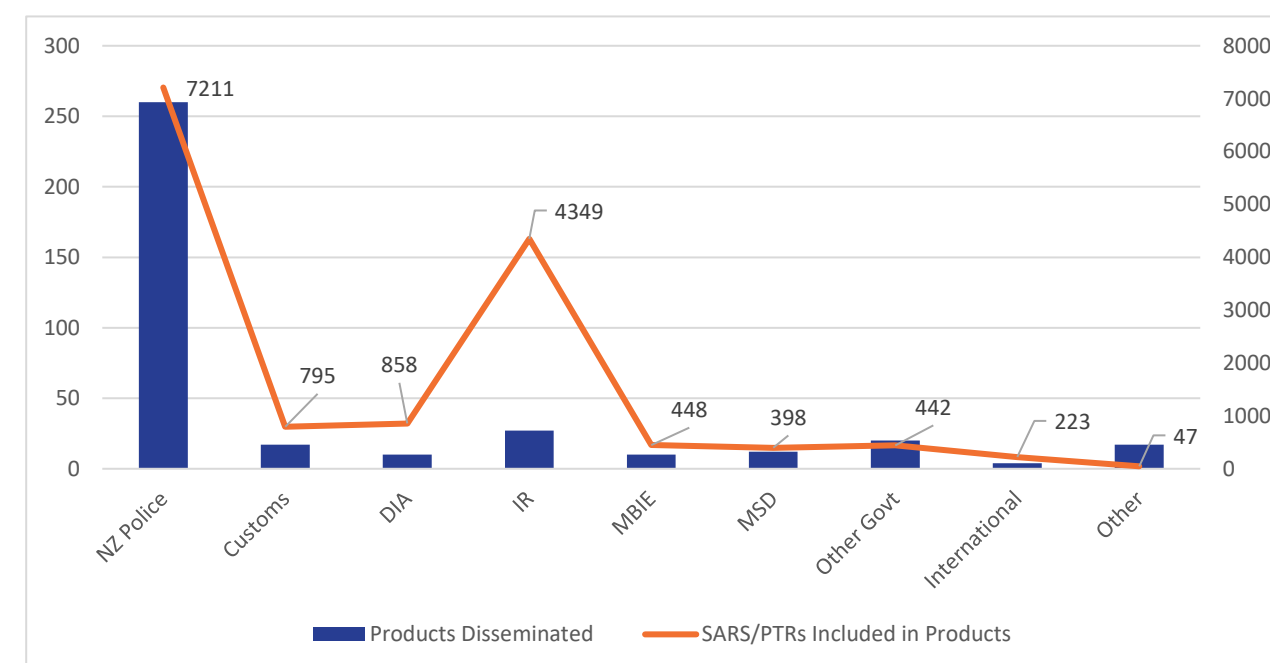
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

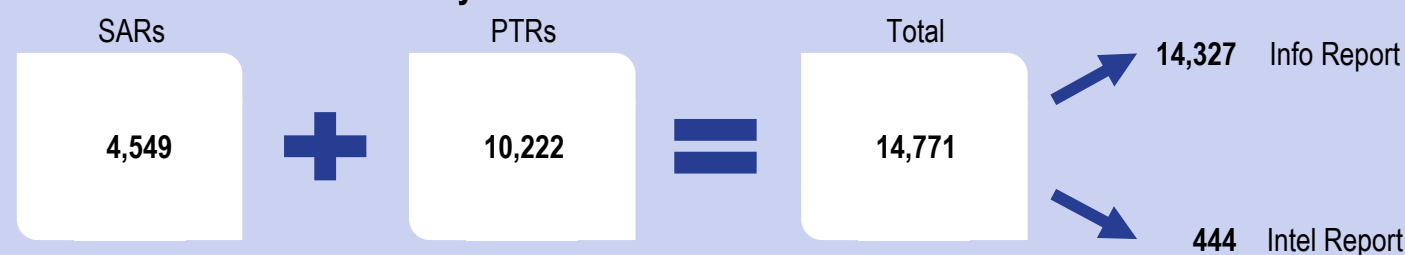
	This QTR	Last QTR
	QTR 2	QTR 1
	2020-21	2020-21
Information Reports	367	452
Analytical Products	10	24
Total Products	377	476



Disseminations of Products by Recipient



Disseminations of Products by Included SARs and PTRs

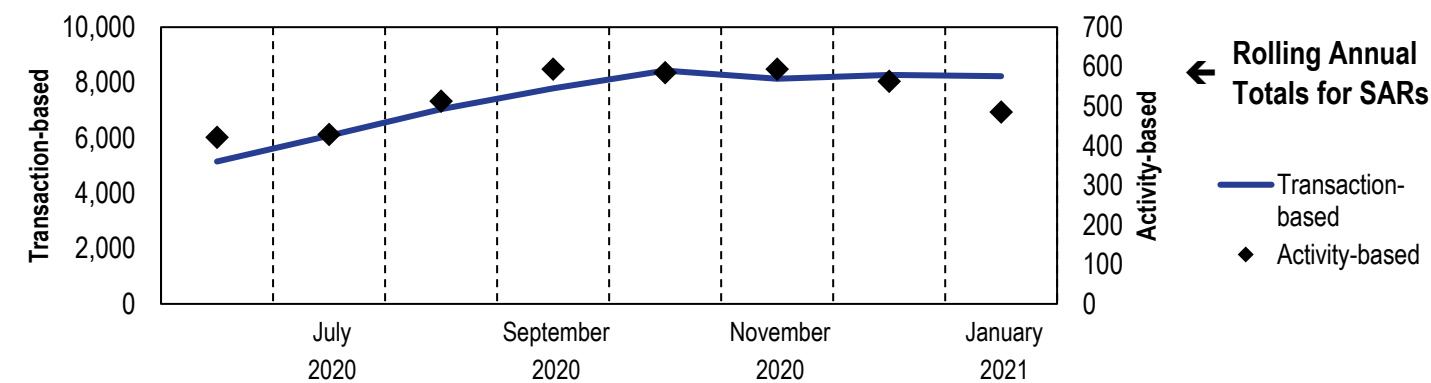
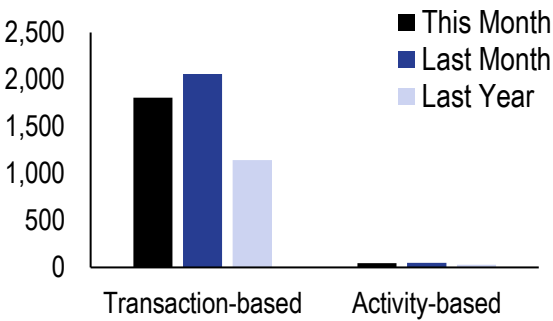


*Statistical data for transaction reporting and intelligence products may be updated as new information is processed, and so there may be minor discrepancies between the statistical figures contained in this report and subsequent reports.

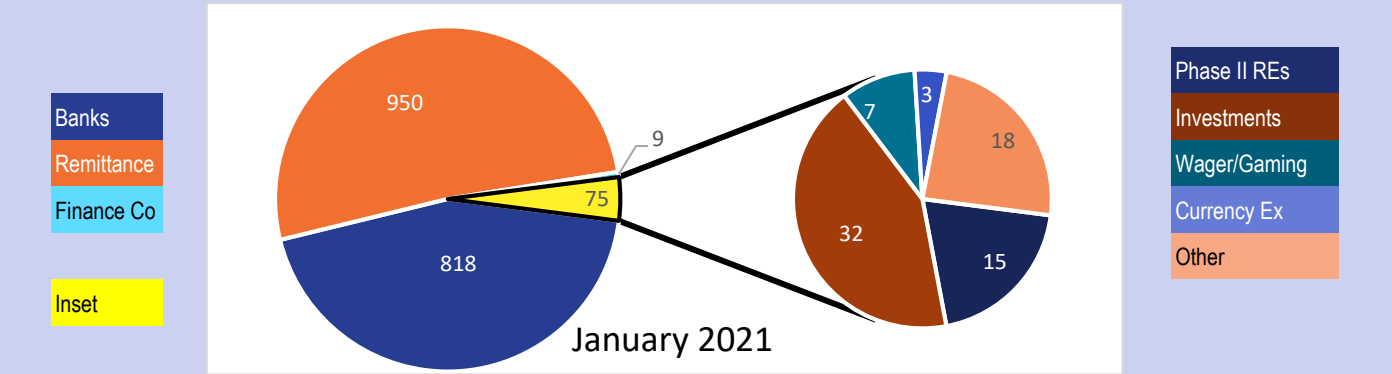
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This Month	Last Month	Last Year
	January	December	January
	2021	2020	2020
Transaction-based	1,806	2,059	1,142
Activity-based	46	48	29
Total	1,852	2,107	1,171

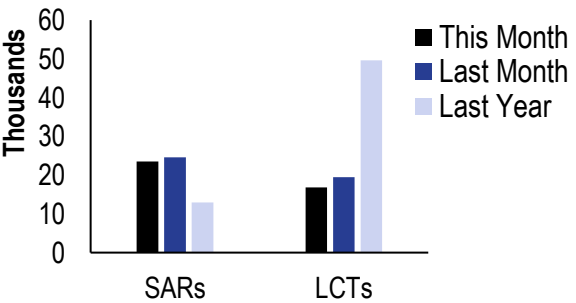


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

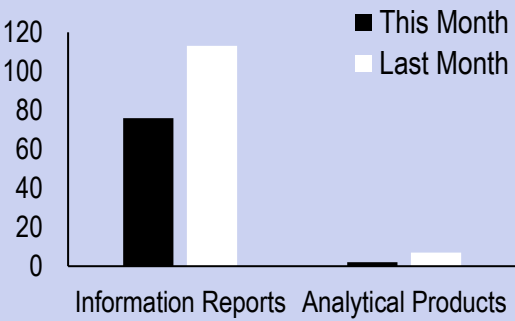
	This Month	Last Month	Last Year
	January	December	January
	2021	2020	2020
SARs	23,529	24,596	12,911
IFTs	389,412	465,046	428,699
LCTs	16,787	19,488	49,629



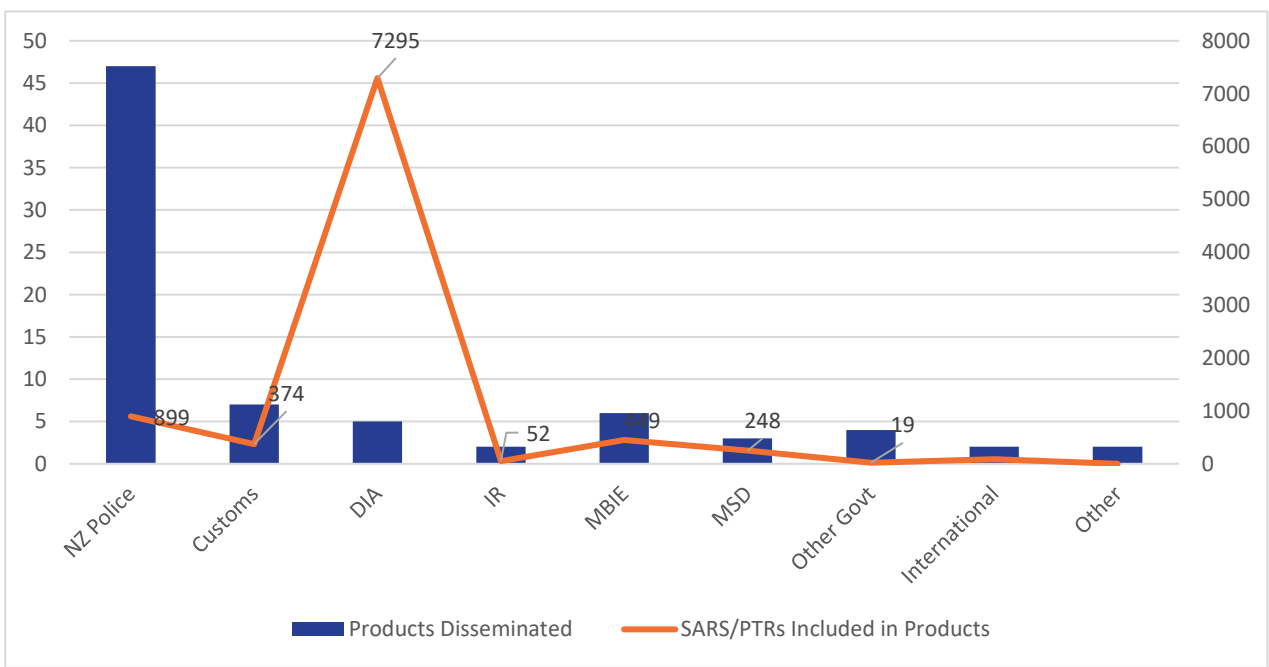
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

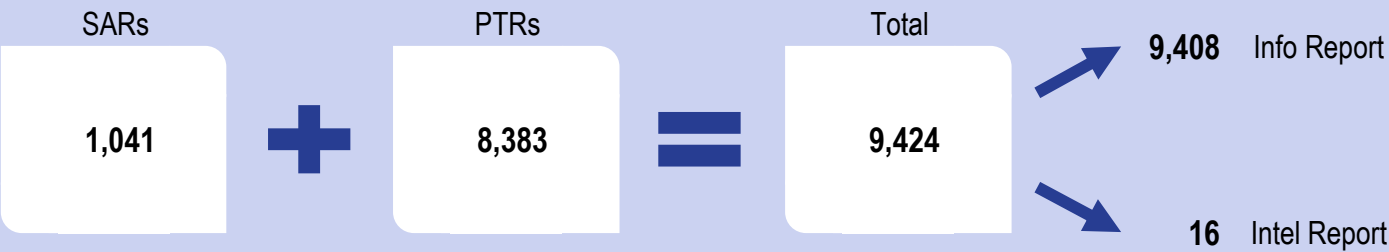
	This Month	Last Month
	January	December
	2021	2020
Information Reports	76	113
Analytical Products	2	7
Total Products	78	120



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.

