

The Suspicious Activity Report

SEPTEMBER 2020

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 Asset Recovery Unit, the Money Laundering Team, a headquarters group, and the Financial Intelligence Unit.

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 four Asset Recovery Units (ARUs), based in Auckland, Waikato/Bay of Plenty, Wellington, and Christchurch, with a fifth being established in Whangārei.

Money Laundering Team

The Money Laundering Team (MLT), led by Detective Inspector Lloyd Schmid, 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 DNFBPs and other third parties such as money remitters.

Message from the National Manager, Financial Crime Group

Detective Superintendent Iain Chapman



Organised crime is at its core a profit-making activity – they are a criminal business. If we focus or get distracted by anything else, be it the brand or the commodity that the group trade in, we fail to see the ways in which to combat it.

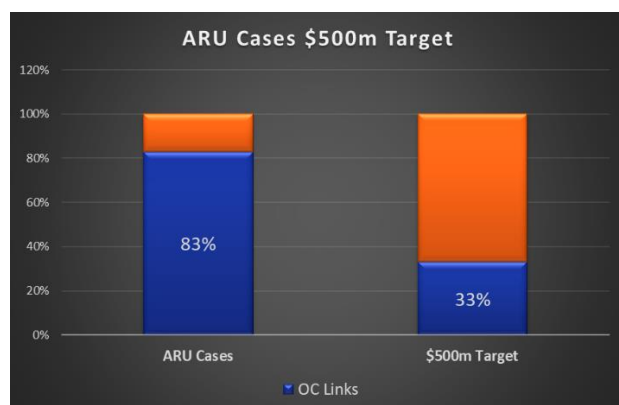
An import/export business would never conduct trades without a degree of confidence of the product to be shipped, its destination, and once there, its sale and distribution. The same can be said about the drug trade. Large shipments of drugs require certainty of payment, distribution and profit.

This is where enablers come in, and the levers we must pull to put NZ in the best possible position to identify, intercept and disrupt the illegal trade.

The AML/CFT Act is at its heart, one of those key levers.

The reporting and subsequent analytics that go on are heavily relied upon by law enforcement. The success of the system is demonstrable every time a major organised crime operation is taken apart, assets seized, and key figures left standing in the dock. By analysing your parts of the system, be it the legal, asset management, or financial sector, and identifying those parts that can be vulnerable to abuse by organised crime groups, you are placing your business, and New Zealand in the best possible position to be resilient against the success of organised crime groups.

Organised and transnational crime is a corrupting influence worldwide, undermining community wellbeing, economic development, and national security. The devastation that criminal groups and gangs have on communities is wide-reaching and its victims are not limited to any one demographic.



Since 1 July 2017, New Zealand Police have been working towards restraining \$500 million in cash and assets from gangs and organised crime groups by 30 June 2021. Police's adoption of this target acknowledges the fact that at its core, organised crime is profit driven.

The target provides an opportunity to pro-actively respond to wealth accrued

from criminality and reduce the negative impact criminality has on our communities. The \$500m target measures a prevention approach to expose criminals and strip them of their ill-gotten assets to discourage and prevent re-investment in crime. Organised crime has been linked to 83% of the asset recovery case files that have contributed to the performance against the \$500m target, and 33% of the value of assets restrained.

FINANCIAL INTELLIGENCE UNIT UPDATE

Notes from the Head of FIU

Detective Inspector Christiaan Barnard

‘Money Feeds the Beast’ is the theme of the 2020 FIU ACAMS Conference which is being held in November and if you have not done so already you can register on the [FIU website](#) before 23 October. In addition to the usual on-site conference, there is an option of remote access to the presentations. While it will be held again at Te Papa, to allow for some social distancing there will only be 300 on-site spaces, which is down from 430 from last year. Despite the challenges presented by COVID, we have endeavoured to bring to the conference a broad range of speakers from both New Zealand and by video-link from around the world. I am very excited by this year’s line-up, who will be covering a range of topics including human trafficking, wildlife trafficking, sanctions, and several case studies. The spots are disappearing fast, so register now.



Sanctions is recognised as being a challenging part of the AML/CFT framework, but it is important for reporting entities to understand their obligations and the risks posed. The terrorism designation of the Christchurch mosque shooter by the Prime Minister is a timely reminder for reporting entities to review their processes, confirm that they have not currently (or previously) provided him with a financial service or hold any assets on his behalf, and to report any business relationship you had or have with him. If you identify any current or proposed activity, you should immediately submit a SAR and you should seek legal advice before taking further action. In addition to the SAR, [section 43](#) of the Terrorism Suppression Act 2002 sets out the requirements in relation Suspicious Property Reports. The Christchurch mosque shooter has since been [designated](#) as a terrorist by the Australian Government which triggers the need to ensure that reporting entities are screening international funds transfers in accordance with their international sanctions obligations. The FIU is working with the Sector Supervisors to develop formal guidance on this issue and I hope that this will be published in the coming weeks.

If you want to stay well-informed of news and developments, please follow the official NZFIU twitter feed @nzfiu and remember – know the risk, ask the questions, and report your suspicions to the #nzfiu.

2020 AML/CFT Conference

Hosted by the FIU and ACAMS, the 2020 AML/CFT Conference programme contains over 15 sessions presented by domestic and international speakers from government agencies and the private sector, centred on the theme of 'Organised Crime – Money Feeds the Beast'. The presentations will focus on how money is the key motivator for a range of criminal offending, with the keynote speakers Archana Kotecha from Liberty Asia and Tom Keatinge from RUSI speaking about human trafficking and sanctions, respectively.

Notable sessions on Day 1 include a Case Study on Operation Woburn by Detective Senior Sergeant Wayne Gray (FCG Money Laundering Team), and a presentation on Operation Deans-Christchurch Terror Attack by District Commander Corrie Parnell and Forensic Accountant Andy Hugill.



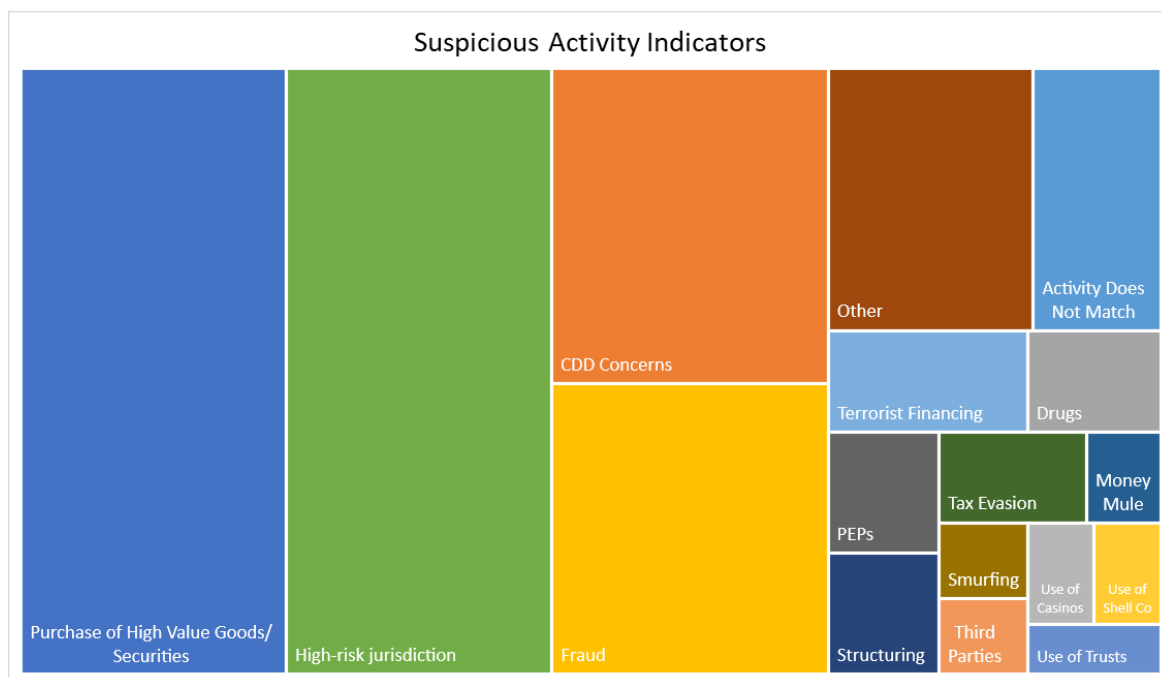
Day 2 highlights include the Sector Supervisors update from Damian Henry (RBNZ), Andrew Holmes (DIA) and Brandt Botha (FMA), presentations/case studies on three Operations (Nero, Hermes and Venezuela), and a session on New and Emerging Risks in relation to the Covid-19 Pandemic.

The 2020 AML/CFT Conference will be held on Tuesday, 10 November and Wednesday, 11 November at the Museum of New Zealand Te Papa Tongarewa in Wellington, New Zealand. Sector Supervisor workshops will be held Monday, 9 November at the Harbourside Function Venue also in Wellington, where each Supervisor will address key topics related to reporting entities in their sectors. This year's conference will be a hybrid event: along with the on-site attendance, there will be virtual access to the full conference. Workshops content will also be available.

Registration for the Conference closes on 23 October – no registrations will be accepted after this date. On-site attendance is limited to 300 attendees. Please [click here](#) to register.

Suspicious Activity Reporting to the FIU

This month, the FIU has analysed the indicators selected on SARs received in September to identify the trends of suspicion that led to reporting. While the Act does not distinguish between suspicious *activity* reporting from suspicious *transaction* reporting, the software (goAML) utilised by the FIU requires reporting entities to select SAR or STR when submitting a report. Just over 100 SARs were reported in September, a 60% increase from August and double the number reported in September 2019.



As shown in the treemap above, suspicions were mainly formed around attempted purchases of high value assets and securities, attempted transactions with high-risk jurisdictions and customers who avoided or refused to complete Customer Due Diligence (CDD). Reports indicated as fraud often contained a suspicion or confirmation of ID theft.

The FIU is encouraged to see an overall trend of increased reporting of SARs and STRs. While the number of STRs reported dipped slightly from August, reports nearly doubled compared to September 2019; the number of transactions reported also doubled between the two periods.

September also saw first-time reporting from five reporting entities, and a further seven reporting entities submit reports after a hiatus of several months or years.

This led, helpfully, to an increase in FIU disseminations. Products disseminated in September increased by 44% from the month before, and the number of PTRs and SARs included in those intelligence products more than doubled (125%) between the two periods.

A review of the quarters showed an increase in reporting received by the FIU – for the period ended 30 September 2020, overall reporting increased by 61% over the previous quarter, and 81% from Q1 2019-20. Disseminations of intelligence products increased nearly 40% between quarters in both products and reports included in those products.

The monthly and quarterly statistics showing the number of reports submitted to the FIU by reporting entities and the number of products disseminated by the FIU is attached to the end of this Report.

INTERNATIONAL AML/CFT NEWS

Spotlight on Crypto

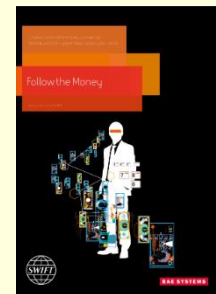
[FATF Report on Virtual Assets Red Flag Indicators](#)



The FATF has prepared this brief report on ML/TF red flag indicators associated with virtual assets to assist reporting entities. The red flag indicators included in this report are based on case studies contributed by jurisdictions from 2017-2020, the findings of the *Confidential FATF Report on Financial Investigations Involving Virtual Assets* (June 2019) and the published *FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014), as well as information on the misuse of virtual assets available in the public domain.

[Understanding the money laundering techniques that support large-scale cyber-heists](#)

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) commissioned BAE Systems to research and write this report. The aim of the report is to highlight the tactics and techniques used by cyber criminals to cash out so that the SWIFT community can better protect itself. The report notes that although the use of cryptocurrencies to launder funds is relatively rare, some criminal groups launder potentially identifiable cryptocurrency funds by blending it with large amounts of other funds.



[How North Korean hackers turn billions in cryptocurrency into cash](#)

Once the North Korean hacking team known as the Lazarus Group has successfully hacked a target and taken control of the money, the group attempts to cover its trail to throw off investigators. These tactics typically involve moving coins to different wallets and currencies. One new tactic, known as “peel chain”, moves money in rapid and automated transactions from one Bitcoin wallet to new addresses through hundreds or thousands of transactions in a way that both hides the source of the money and lessens the risk of setting off red flags.

[South African man charged in US Court for fraud involving US\\$28m in Bitcoin and Forex](#)

A South African man has been charged with fraud for allegedly scamming US\$28m (NZ\$42m) from over 1,000 investors. Since 2017, the man targeted church-going African immigrants, promising them guaranteed returns on his purported bitcoin and foreign currency investment pool. However, none of the money was invested in bitcoin or foreign currency.

[Racing officials probe horse racing outfit over cryptocurrency scam](#)



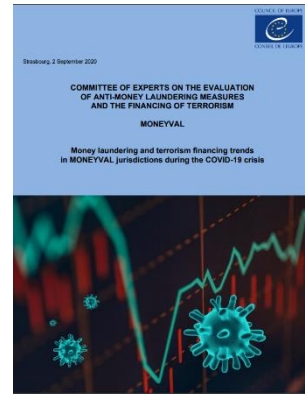
Racing NSW confirmed it is investigating Phoenix Thoroughbreds after its owner was accused in a US court of being involved in an international money-laundering scheme. Phoenix Thoroughbreds was banned from racing in France in August after a prosecution witness alleged that Phoenix’s Dubai-based owner had stolen US\$161m (NZ\$244m) in the OneCoin cryptocurrency scheme. Phoenix owns more than 100 horses in Australia.

MONEYVAL

[Money laundering and terrorism financing trends during the COVID-19 crisis](#)

The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism ([MONEYVAL](#)) has issued a report with the goal of providing an overview of the impact of the COVID-19 crisis on AML/CFT systems from a regional perspective, the measures taken by jurisdictions to mitigate this impact, and possible recommendations.

One of the findings of the report was that the urgent need to acquire specialised medical equipment and supplies created vulnerabilities for fraud, corruption, and subsequent money laundering. Other findings of the report are relevant for the general public as a source of information against potential criminal schemes, such as phishing emails and social engineering.



China

[E-Commerce schemes involving empty boxes linked to gambling and money laundering](#)



Police in the city of Wuxi, China recently uncovered an operation that used an 'empty package scheme' to launder illegal cross-border gambling money. Police say the scheme they discovered involves gambling platforms using third-party payment providers to transfer their gains and make it look like someone purchased an item online.

The investigation was opened after a man made a complaint regarding an iPhone purchased over WeChat that never arrived. The Police subsequently discovered 2,700 websites involved in empty package schemes and three criminal organisations. Suspects allegedly used empty package delivery services to create false online shopping and delivery records to disguise illegal transactions; often, physical packages were never sent. Police have arrested 40 people, some of whom were employees of legitimate delivery services.

Ireland

[170 vehicles seized in money laundering investigation](#)

Gardaí and British police have seized 170 cars and trucks as part of an investigation into a UK-based transnational organised crime group that laundered money through the Irish motor trade. The 85 vehicles seized in Ireland included Range Rovers, BMWs, Audis, Volvos and Skodas, along with two flatbed trucks and a car transporter. The Criminal Assets Bureau said the UK-based gang, with members from Pakistan and Lithuania, was stealing money from UK businesses through CEO impersonation and invoice redirect fraud and laundering it through the motor trade.

Countering Financing of Terrorism

[Suspected arms dealers moved millions in Somali money transfers](#)



Somali money transfer companies moved more than US\$3.7m (NZ\$5.6m) in cash between suspected weapons traffickers in recent years, including to a Yemeni under US sanctions for alleged militant links, according to a report seen by Reuters.

[The Global Initiative](#) analysed nearly six years of transaction records from the city of Bossaso, matching them with mobile phone records provided

by security sources and database searches. The report noted instances where individuals were able to make transfers using multiple names and numbers; one man used 24 names between the four companies, the report said.

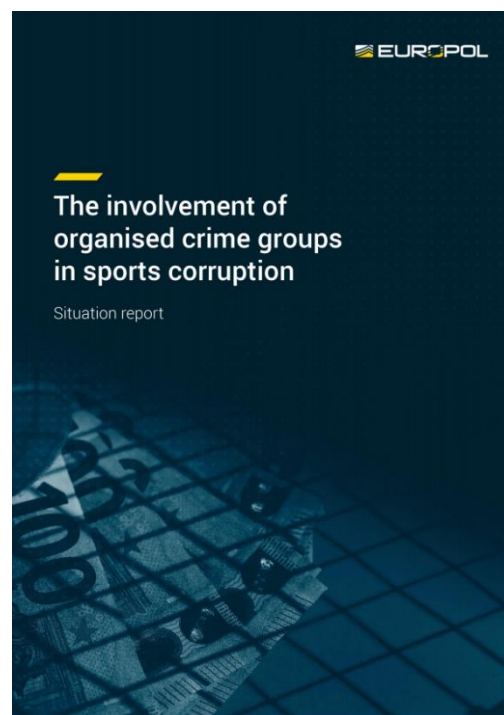
Gambling

[Football is money laundering paradise for organised crime groups](#)

According to a recent Europol report, match-fixing in sports is increasingly being used by organised crime groups to launder large sums of dirty money. [The situation report](#) released in August 2020 highlights the link between sports corruption and organised crime and examines the different types of match-fixing as the most prominent form of sports corruption monitored by Europol.

The report warns that sports corruption is often addressed only from the perspective of sports integrity because practitioners lack awareness on the involvement of organised crime. Europol's analysis identified links between the individuals involved in the manipulation of sports competitions at a lower level for merely financial gain, and other more sophisticated criminal networks behind the scenes; the criminal structures are multi-layered with the financiers sitting at the top of the pyramid.

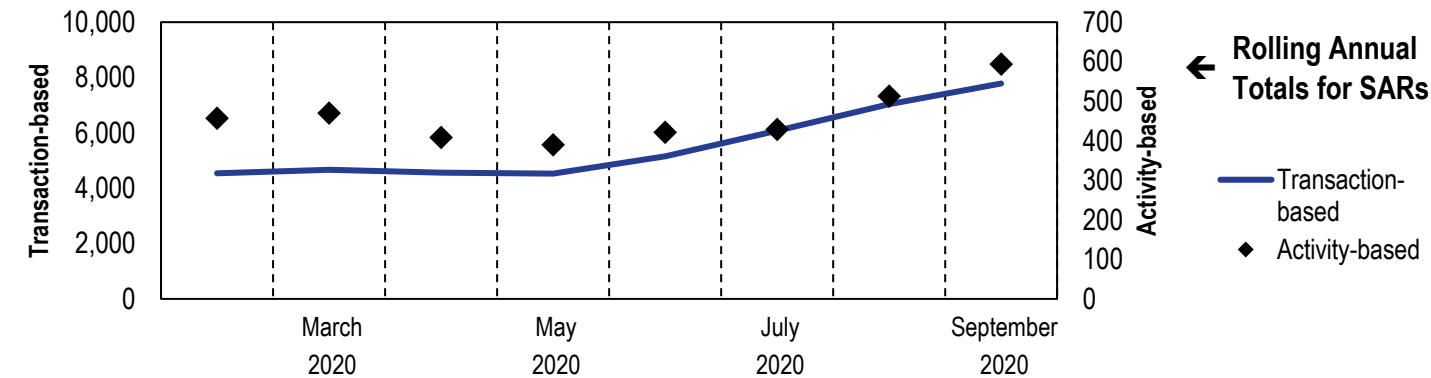
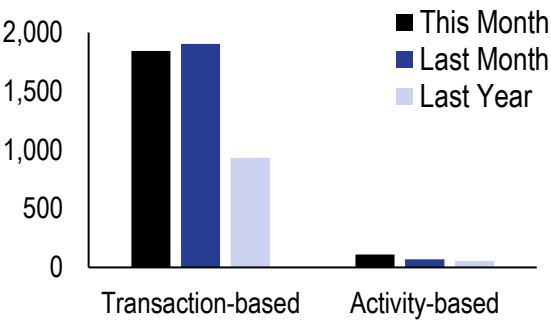
Europol said the more 'professional' method used by certain crime groups was to buy a club or sponsor it to an extent of gaining effective control over the team with the sole purpose of fixing matches and laundering money. Often, these organisations use established legal businesses to move their money through the sports world.



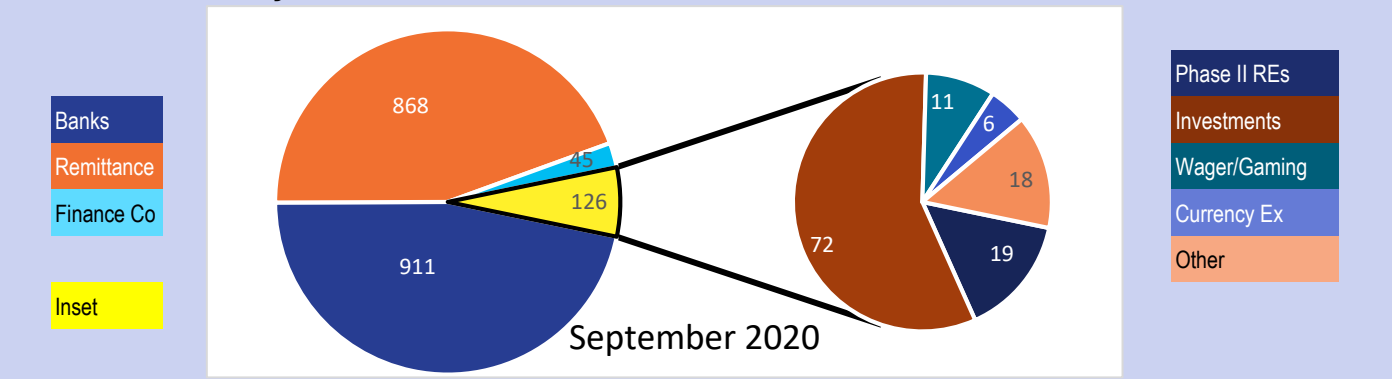
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This Month	Last Month	Last Year
	September	August	September
	2020	2020	2019
Transaction-based	1,842	1,902	934
Activity-based	109	68	54
Total	1,951	1,970	988

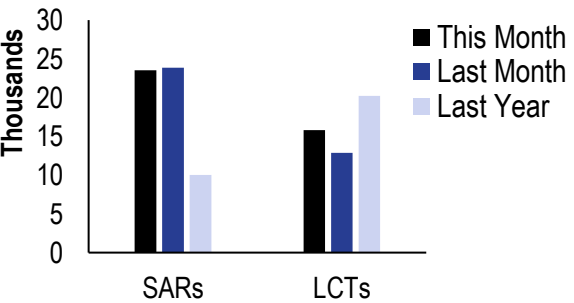


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

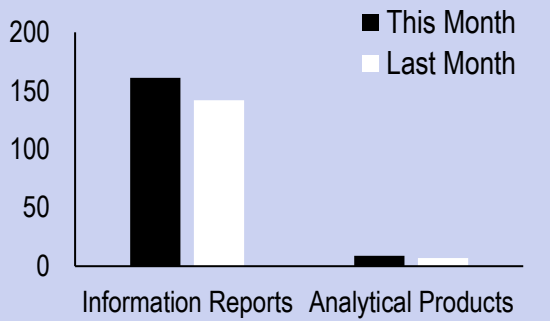
	This Month	Last Month	Last Year
	September	August	September
	2020	2020	2019
SARs	23,544	23,844	10,028
IFTs	418,771	404,743	402,475
LCTs	15,806	12,867	20,219



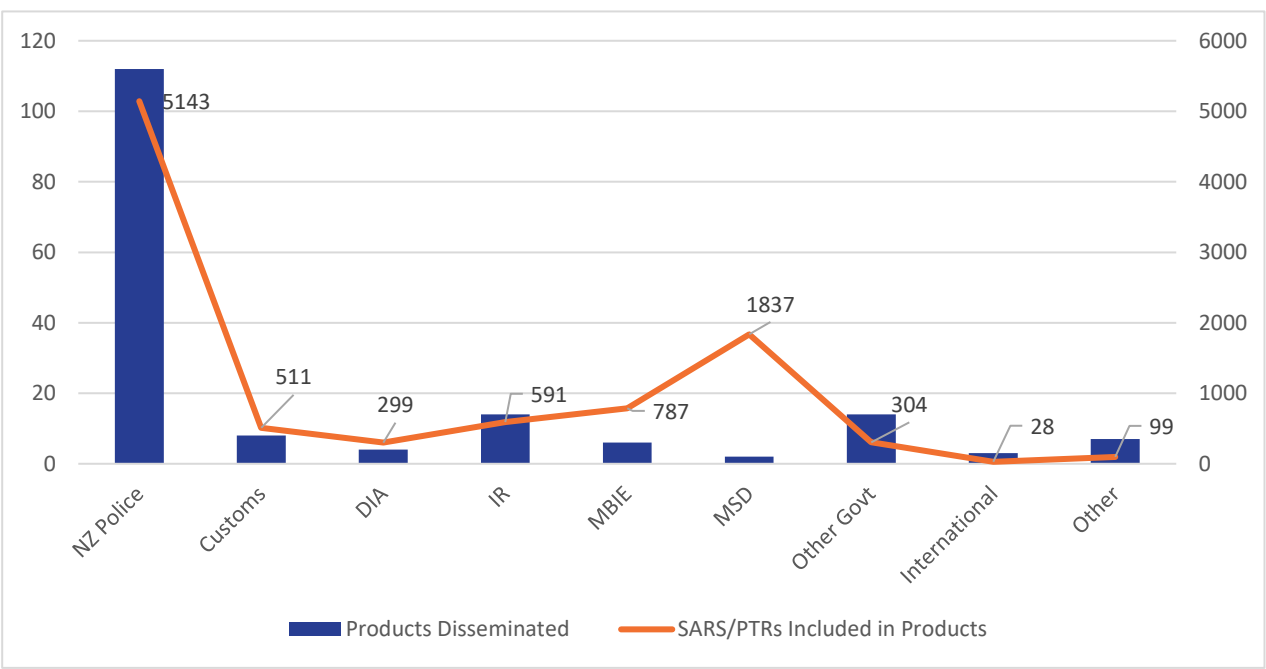
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

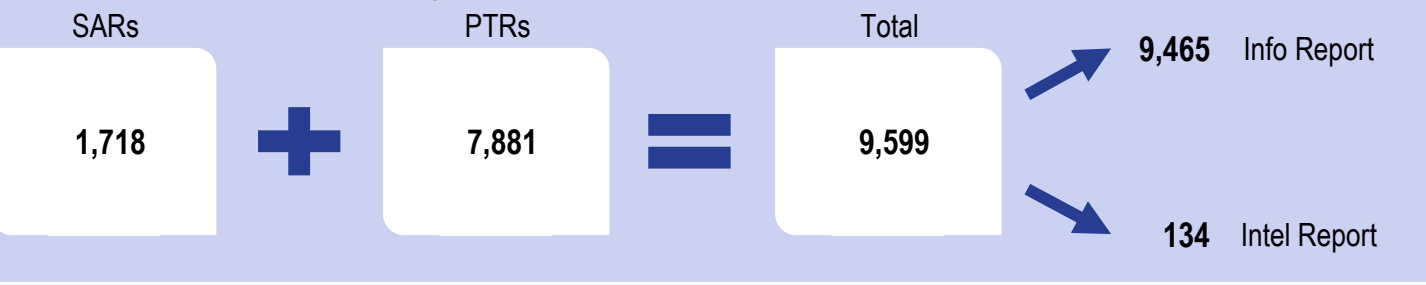
	This Month	Last Month
	September	August
	2020	2020
Information Reports	161	142
Analytical Products	9	7
Total Products	170	149



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*

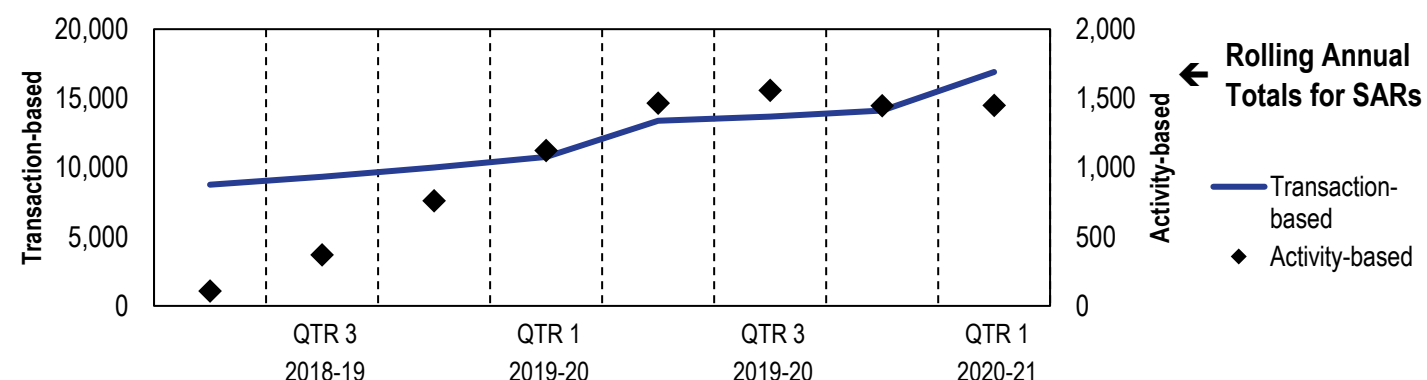
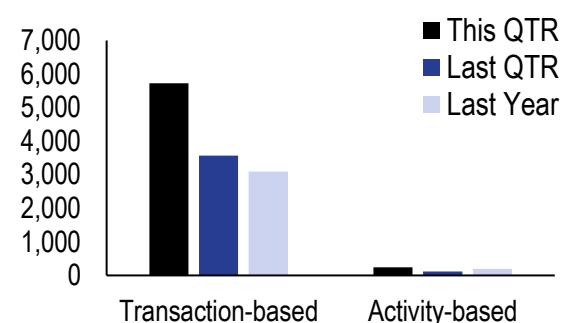
NEW ZEALAND POLICE FINANCIAL INTELLIGENCE UNIT

QTR 1 | 2020-21

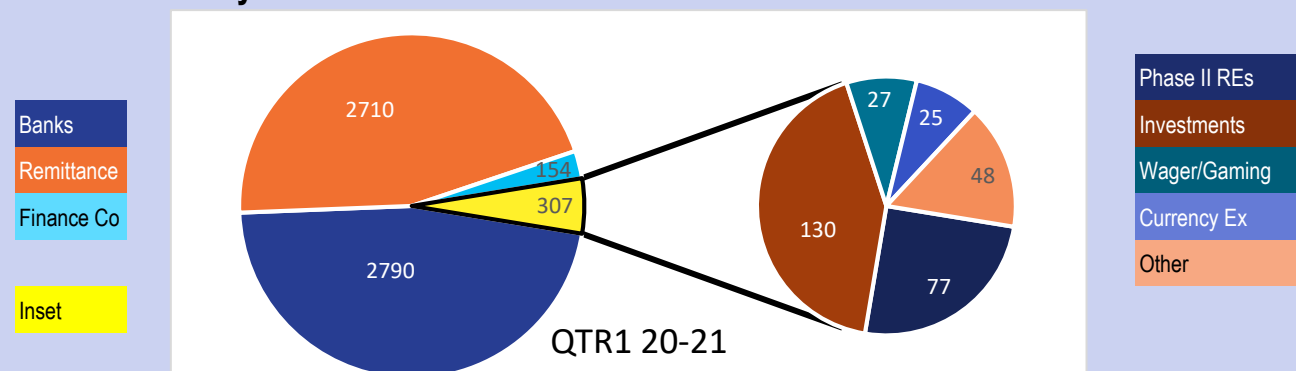
SUBMITTED REPORTS to the FIU*

Processed Suspicious Activity Reports (SARs)

	This QTR	Last QTR	Last Year
	QTR 1	QTR 4	QTR 1
	2020-21	2019-20	2019-20
Transaction-based	5,722	3,568	3,090
Activity-based	240	122	190
Total	5,962	3,690	3,280

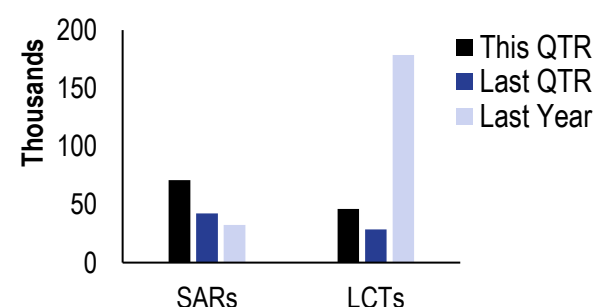


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

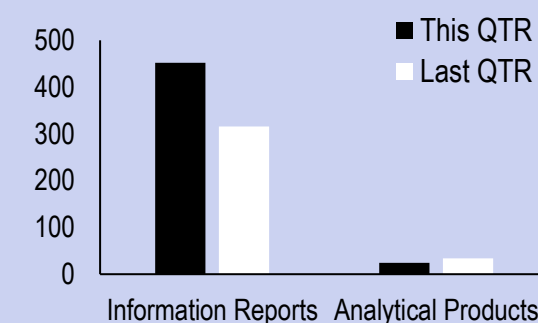
	This QTR	Last QTR	Last Year
	QTR 1	QTR 4	QTR 1
	2020-21	2019-20	2019-20
SARs	70,986	42,291	32,517
IFTs	1,290,544	1,135,471	1,300,113
LCTs	46,150	28,472	178,670



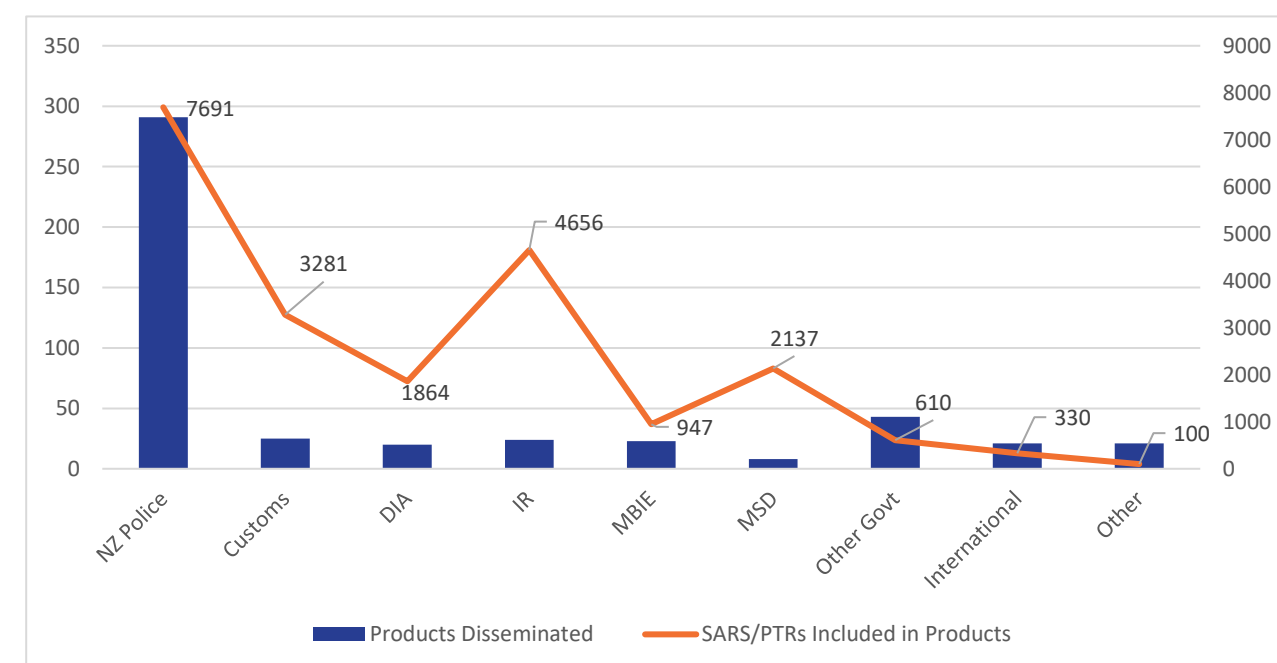
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

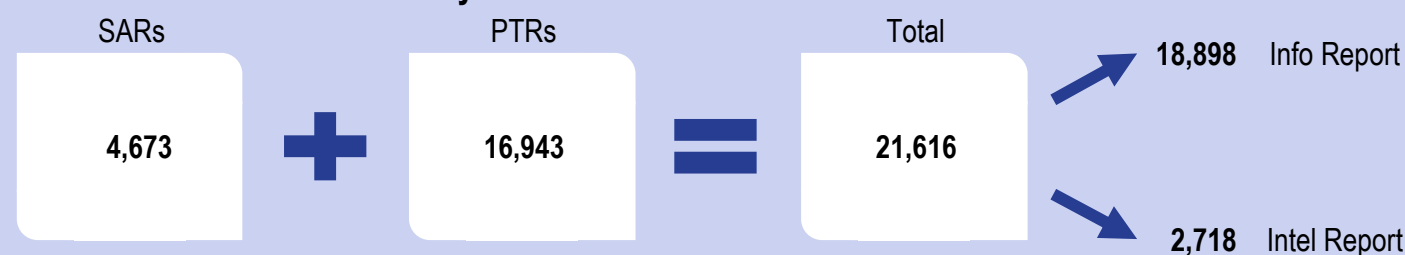
	This QTR	Last QTR
	QTR 1	QTR 4
	2020-21	2019-20
Information Reports	452	316
Analytical Products	24	34
Total Products	476	350



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.