The Suspicious Activity Report

MARCH 2021

New Zealand Financial Intelligence Unit

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

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 Inspector Craig Hamilton. 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 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 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 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

This month features an article on what a good suspicious activity/transaction report looks like. SARS are the life blood of any FIU – but the concept of GIGO is entirely apt in our setting. The FIU receives a mixture in the quality of SARS – some are excellent, while others are not as good. We want to encourage high-quality, lower-volume SAR reporting. A key issue for reporting entities is the confusion caused by the concept of 'suspicion'. Its misinterpretation can lead reporting entities to apply a threshold for reporting that is too low.

The article goes into much more depth, but I wanted to reinforce some key points. Forming a suspicion is the start of a journey of investigation for a reporting entity. This stage is simply speculation, that does not (except for limited circumstances) reach the required threshold to report. A reporting entity must make inquiries to either negate the speculation or to increase the level of belief to having a *reasonable grounds to suspect*. This month's article provides a helpful four stage process for reporting entities to apply to this journey of determining whether there are reasonable grounds to suspect.

What is *reasonable grounds to suspect*? It comes down to understanding the difference between speculation and what is likely. In practise it means that the proposition (i.e. the suspicion that the behaviour is relevant to an offence) is regarded as inherently likely. For example, if a customer behaves in accordance with a money laundering typology, this will form a suspicion, but in the absence of any other information this is speculation and is not reasonable grounds to suspect. There must be additional inquiries conducted to raise the level of belief to a point where the submitter of the SAR believes that it is likely the customer behaviour is relevant to crime.

The threshold of reasonable grounds to suspect is an objective test. This means that any other reasonable person reviewing your inquiries would arrive at the same conclusion – that it is inherently likely that the transaction or activity is relevant to the investigation or prosecution of an offence. These types of objective thresholds are regularly tested in our courts through the exercise of emergency powers by Police and the application for orders such as search warrants and production orders.

The FIU expects that reports are thorough and reflect the various inquiries undertaken, so that it clearly conveys both the reasonable grounds to suspect and further tactical information that will assist the FIU with analysing the report.

Keep up the good work with the SARs and strive for innovation and excellence in your detection and reporting. Remember, – know the risk, ask the questions, and report your (reasonable grounds for) suspicion to the #nzfiu.

REPORTING ENTITIES' FAQ

Q: What is Suspicion?

Suspicious activity is defined in the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) as an activity undertaken where the reporting entity has "*reasonable grounds to suspect*" that a transaction, service, or inquiry may be relevant to the investigation, enforcement or prosecution of a crime. Whilst goAML separates reporting by transaction (STR) or activity (SAR), the collective term for suspicious reporting in the AML/CFT Act is 'SARs'. The following guidance will also refer to STRs and SARs collectively as 'SARs' and is focussed on the 'Reason for Suspicion' free text field.

Reasonable grounds to suspect

Suspicious Activity Reporting is based on an objective test applied to *reasonable grounds for suspicion*. In the 2017 ruling of Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd, paragraph 64 notes "where an objective observer would conclude that reasonable grounds for suspicion were known to the reporting entity, it is no defence that the reporting entity did not actually consider the transaction to be suspicious." The test for a SAR is not a subjective test; if a person in your circumstances should have inferred knowledge or formed a suspicion, then a report must be submitted.

Forming suspicion

When deciding whether a matter needs to be reported, reporting entities must ensure reasonable grounds for suspicion exist. It is important reporting entities do not engage in defensive reporting as this practice is not in line with the intentions of the Act and may lead to the reporting entity breaching other obligations.

In practice, the FIU expects that reporting entities will need to conduct enquiries to gather information to establish reasonable grounds for suspicion once an unusual event occurs or is flagged by account monitoring. A transaction may have many factors that, considered individually, do not raise suspicion, but when considered collectively, suggest criminal activity.

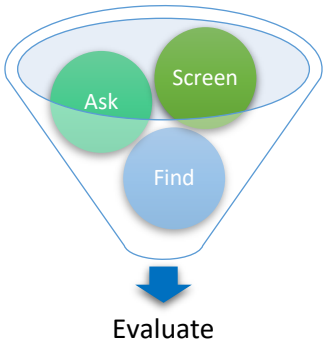
In most situations, we expect a SAR would be filed within three business days of the reporting entity ***gathering sufficient verifying information*** *for reasonable grounds to crystallise suspicion, rather than three days from an initial event.*

On defining *reasonable grounds for suspicion*, there is a significant amount of case law, which can be summarised as 'an activity and/or transaction that is **inherently likely** to be relevant to the investigation, prosecution of any person for a money laundering offence (or the enforcement of the specified Acts)'. Circumstances giving rise to speculation or concern are **not** enough to constitute reasonable suspicion. In Westlaw NZ's commentary on the Search and Surveillance Act 2012 S S6.10 (Reasonable Grounds to Suspect), they noted whether such grounds exist is to be determined objectively by considering all the relevant factors cumulatively and not in terms of the personal belief of the person submitting the report.

Only once *reasonable grounds for suspicion* exist, the legal obligation is triggered for a reporting entity to submit a SAR to the FIU as soon as practicable, but no later than three working days.

SAFE Method [from HK JFIU]

Our colleagues at the Hong Kong Joint Financial Intelligence Unit recommend the 'SAFE' approach as an effective systematic approach to identify suspicious activity.



Often, reporting entities submit a SAR simply because a suspicious activity indicator has been recognised. This is only step (1) of the systematic approach, however, leaving out steps (2), (3) and (4). This can lead to a lower quality of SARs. SAFE provides a robust methodological framework to ensure reporting entities consider a range of factors when reviewing potentially suspicious activity and deciding whether to submit a SAR.

SAFE stands for: Screen, Ask, Find, Evaluate.

Screen

Screen for suspicious activity indicators.

The recognition of one or more indicator(s) of suspicious activity is the first step in the suspicious activity identification system. The FIU has recently updated our indicators, but some common indicators include:

- Large or frequent transactions (deposits or withdrawals)
- Involvement of one or more of the following entities: shell companies, companies registered in known tax havens, money remitter, casinos
- Customer refuses or is unwilling to provide an explanation of financial activity
- Activity is not as expected from the customer considering the information already held on that customer

Ask

The reporting entity should start with asking the customer the appropriate questions. This may be required as part of an enhanced customer due diligence (ECDD) process.

In carrying out an activity or transaction for a customer, if one or more suspicious activity indicators is observed, the customer should be questioned on the reason for conducting the transaction or activity, the source of funds, the ultimate beneficiary of the money being transacted and/or the beneficial owner of any money or assets involved. This is a requirement of the Act and is not considered 'tipping off'. While tipping off will be covered in more detail in a future edition of this Report, tipping off by a reporting entity relates to the disclosure to a customer the existence of a SAR or their intention to submit a SAR.

Find

Find information from the customer's records: review information already held on the customer.

Reporting entities hold various pieces of information on their customers which can be useful when considering if the customer's financial activity is to be expected or is unusual. In this

step, reporting entities should review the information already known about the customer and their previous transactions and consider this information to decide whether the financial activity is legitimate and to be expected, or if the activity is unusual.

This step is often accomplished during 'ongoing due diligence and account monitoring', as set out in the AML/CFT Act. Open source internet searches and subscription-based data services can also be checked during this stage.

While 'Find' is listed as the third stage, a reporting entity can conduct this stage before or concurrently with the 'Ask' step. Reporting entities should also consider that they may uncover information that causes suspicion to dissipate. If this occurs, no further action is required.

Evaluate

Evaluate all the above information - is the transaction or activity objectively suspicious? Consider whether the customer's explanation, the enhanced CDD verification undertaken, the information held, and any open source searches support a reasonable and legitimate explanation of the activity observed. Are there **reasonable grounds to suspect** (i.e. is it likely) that the activity or transaction will be relevant to the investigation or prosecution of money laundering, or the enforcement of the Acts specified in s. 39A of the AML/CFT Act?

As a general rule, all inquiries should be completed before an evaluation is completed; once the evaluation is made and there are reasonable grounds to suspect, the three-day submission rule is triggered.

Submitted SARs will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker. If, having considered all the circumstances, the activity is found to be genuinely suspicious (applying an objective test), then a SAR should be submitted.

Reporting entities are therefore encouraged to submit SARs based on the SAFE approach, even if they do not know a specific crime or type of crime that may be connected to the suspicious transaction or activity.

A note on Enhanced Customer Due Diligence

Section 22A of the AML/CFT Act requires a reporting entity to conduct enhanced CDD if a SAR is submitted. The stages outlined above (Screen, Ask, Find, and Evaluate) are all consistent with conducting enhanced CDD, and it needs to be stressed that enhanced CDD can be triggered at any of these stages in accordance with the Act.

If a reporting entity is not able to complete enhanced CDD, they must not carry out any occasional transaction or activity for the individual(s) or entity(ies), nor establish a business relationship with them. If a reporting entity already has a business relationship with the customer, it must be terminated. The final outcome of enhanced CDD should form part of the grounds for suspicion.

For more information on conducting enhanced CDD, please refer to the triple branded (i.e. RBNZ, DIA, FMA) guidance on your Supervisor's website.

Example 1: Grounds for Suspicion Formed by Observation and Account Monitoring

Mr A was a member of a casino's loyalty programme and an occasional visitor to the casino. On 3 November, casino staff noticed Mr A was associating with people that had previously come to the attention of casino staff for suspicious activities [SCREEN]. At this point, there were not reasonable grounds for suspicion.

Mr A visited the casino again on 5 November and purchased a larger amount of chips than usual. When queried by casino staff, Mr A provided a vague response [ASK]. The matter was referred to their monitoring team who escalated the matter to enhanced CDD.

On 8 November, after examining Mr A's transactions, casino staff noticed Mr A's playing habits were changing – he was spending longer at the casino and increasing the size and frequency of his bets [FIND]. The casino formed a suspicion Mr A was engaged in money laundering or other illicit activity [EVALUATE] and submitted a SAR on 9 November (within the three business days timeframe).

Example 2: Grounds for Suspicion Detected on Initial Interaction

Ms B was an existing customer at the bank. On 3 March, she visited a branch of the bank with $20,000 in $20 notes. The bank's staff member noticed the money was damp and smelled of cannabis.

At this point, there were reasonable grounds to suspect that Ms B was engaged in money laundering or other illicit activity; no further investigation was required to corroborate the suspicious state of the cash. The matter was referred to the AML/CFT compliance team who submitted a SAR on 5 March (within the three business days timeframe).

Q: What does a good SAR look like?

The purpose of Suspicious Activity Reports (SARs) is to report known or suspected violations of law or suspicious activity detected by reporting entities subject to the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act).

In many instances, SARs have been instrumental in enabling law enforcement to initiate or supplement money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR submissions also presents the FIU with a method of identifying emerging trends and patterns associated with financial crimes.

It is critical that the information provided in a SAR is as accurate and complete as possible.

Reporting entities are required to submit SARs that are complete and timely. The failure to adequately describe the factors making the activity or transaction suspicious undermines the very purpose of the SAR and lessens its usefulness to law enforcement. Because the SAR 'reason' fields serve as the only free text area for summarising suspicions, it is essential that reporting entities write narratives that clearly describe how the suspicion was formed and are concise and thorough. That is, describing all relevant details but leaving out unnecessary or unhelpful information.

The form and content of a SAR is prescribed in Schedule 1 of the AML/CFT (Requirements and Compliance) Amendment Regulations 2017. A SAR submitted to the FIU must, as it relates to the matter giving rise to suspicion, contain:

- a statement of the reasonable grounds on which the reporting entity holds a suspicion;
- an indication of any supporting documents that may help the FIU to analyse the SAR;
- information the reporting entity lawfully holds on the timing, parties and accounts for transactions or services that are sought or provided;
- customer or other party details – names, addresses, business names and addresses – and other supporting identity information as available.

All SARs must also explain why the transaction or activity (or proposed transaction or activity) is suspicious. For example, stating that a personal or business transaction is suspicious simply because the transaction is large without any supporting information or explanation is not sufficient and does not satisfy the reasonable grounds element.

To be useful for analysis, the details provided in a SAR needs to be sufficient to connect a person(s) to a suspicious activity along with any information obtained through the account opening process and during subsequent customer due diligence obligations (as permitted by the legislation and regulations) that helps to show the cause for suspicion.

The narrative of the SAR should be concise and clear, provide a detailed description of the known or suspected predicate crime or suspicious activity, identify the essential elements of information (i.e. the 5 Ws), and be chronological and complete.

The 5 Ws and 1 H Framework

In general, a SAR narrative should identify the five essential elements of information – who? what? when? where? and why? – of the suspicious activity being reported. The method of operation (or how?) is also important and should be included in the narrative.

Who is conducting the suspicious activity?

Describe additional details about the person(s) of interest other than those provided earlier in the SAR form, including their employer/occupation information or other known source of funds or wealth and the manner and length of business relationship the reporting entity has with that person(s).

The 'Reason for suspicion' field should be used to describe the person or persons of interest. If more than one individual or business is involved in the suspicious activity, identify all of them and any known relationships amongst them. While detailed information may not always be available (e.g. in situations involving persons not in a business relationship), such information should be included to the maximum extent possible, including account numbers and account names.

Phone numbers and addresses are important; reporting entities should note not only the person's primary street addresses, but also other known addresses, including any post office box numbers and apartment numbers when applicable. Any identification numbers associated with the person(s) of interest other than those provided earlier are also beneficial, such as passport and driver's license numbers. If available, electronic data such as IP addresses, phone numbers and CCTV should be included.

What products or methods are being used to facilitate the suspicious activities?

Where the activity involves a service or inquiry, identify and describe the service or inquiry. Examples of this could include the creation of trusts and companies, management of client affairs, undertaking certain litigation, and setting up charities.

Where the activity involves a transaction, identify and describe the transactions that raised suspicion. For example, transactions could include cash deposits and/or withdrawals, wire or other electronic transfers, casino chips, cryptocurrency, and foreign currency translation.

Financial products or mechanisms that may be used in suspicious activity include but are not limited to, letters of credit and other trade instruments, correspondent accounts, casinos, structuring, shell companies, stocks, mutual funds, insurance policies, travellers cheques, credit/debit cards, stored value cards, and/or digital currency business services.

In addition, several different methods may be utilised to conduct transactions including internet banking, smart ATMs, or couriers. For legal structures, methods may include utilising legal arrangements with overly complex ownership structures or trusts and other entities where beneficial ownership is obscured.

If documenting the movement of funds, identify all account numbers at the financial institution affected by the suspicious activity and when possible, provide any account numbers held at other institutions and the names/locations of the other financial institutions, including money remitters and foreign institutions involved in the reported activity.

When did the suspicious activity take place?

If the suspicious activity is a one-time occurrence, identify the date. If a pattern of activity occurred over a span of time, state when the activity first initiated, when it was detected, and then describe the activity during the duration. If the suspicious activity isn't a pattern but still is spread over a period of time, indicate the date when the suspicious activity was first noticed, the duration of the activity, and if it is still continuing.

Where did the suspicious activity take place?

Where a financial transaction is involved, identify the branch/entity location or locations where the activity occurred, including the street address (including postcode). Identify all account numbers and types of accounts affected by the transactions/activity. Indicate if suspicious transactions involve other domestic or international banks or reporting entities and provide any available information on those, including locations and account numbers.

For other activities, identify if a customer or person may be acting in a high-risk jurisdiction, utilising an entity(ies) domiciled in a tax haven, or where a hired safe deposit box is located.

Why does the reporting entity think the activity is suspicious?

Describe concisely but fully why the reporting entity considers the activity as suspicious; consider the types of products and services offered by your industry, and the nature and normally expected activities of similar customers. Be sure to include any relevant information about suspicious customer activity that the reporting entity has in its files at the time the SAR is filed. If the SAR mentions a Production Order or Request for Information, include the PO/RFI File Number in the summary and/or attach a document with the details of the Investigating Officer; include Trust Deeds if a trust is mentioned in the SAR; and consider attaching copies of ID and/or CCTV images to support information provided in the SAR. Any open-source links related to the suspicious activity should also be included.

How did the suspicious activity occur?

Describe the method of operation of the subject conducting the suspicious activity. In a concise, accurate and logical manner, describe how the suspicious transaction or activity or pattern of transactions or activities were completed. Provide as completely as possible a full picture of the suspicious activity involved.

Narrative

When all applicable information is gathered, analysed, and documented and the reporting entity concludes that a SAR is required to be submitted, the information should be described in the 'Reason' field in a concise and chronological format. Include all elements of the '5 Ws and 1 H' set out above, as well as any other information that can assist law enforcement.

The suggested structure of the SAR narrative is Introduction, Body, Conclusion.

Introduction

The intro should provide:

1) A brief statement of the SAR's purpose;
2) How the suspicion was brought to the reporting entity's attention (i.e. automated reporting, manual monitoring).
3) Description of the known or suspected offence;
4) The date of any SARs previously filed on the person(s) of interest and the purpose of that SAR;
5) Any internal investigative numbers used by the filing institution to maintain records of the SAR.
6) The current status of enhanced customer due diligence and any intention to exit should be signalled.

Body

The body should provide the relevant facts about all parties facilitating the suspicious activity or transactions. Answers "who?"

Identify the involved accounts and transactions or other products or services being provided, including where the suspicious activity took place. Provide the particular date of a single activity or transaction or the period of time for a pattern of activities or transactions. Answers "what, where, when".

Explain in detail the reporting entity's position that the activity or transaction is illegal or suspicious. Detail the reporting entity's conclusions and how the reporting entity arrived at those conclusions. Answers "why".

Describe the method of operation of the subject – the way the activity or transactions were completed; any relationship to other transactions, accounts, individuals, etc; and subsequent results of the activity. Answers "how".

The body should also include all pertinent information that supports why the SAR was filed. This could include red flags observed, any factual observations or incriminating statements made by the person of interest, and any other relevant facts about the parties involved.

Conclusion

Summarise the report in the conclusion at the end of the Reason for Suspicion text box.

In the 'Action' text box, include any planned or completed follow-up actions by the reporting entity, such as intent to cease or cessation of the business relationship, and/or ongoing monitoring of activity.

Examples of Sufficient and Insufficient SAR Narratives

On the following pages, the FIU has provided examples of sanitised sufficient and insufficient SARs submitted from different types of industries for illustration. Each example is followed by brief commentary.

Example 1: Sufficient SAR Filed by a Financial Institution

Investigation case number: 987654. The customer, a bakery and its owner, are suspected of intentionally structuring cash deposits to circumvent reporting requirements. The customer is also engaged in activity indicative of an informal money remittance operation: deposits of bulk cash, third party transfers, and multiple IFTs to Dubai, UAE. The type and volume of activity observed is non-commensurate with the customer's expected business volume and deviates from the normal volume of similar types of businesses located in the same area as the customer. Investigative activities are continuing.

Joe Bloggs opened a personal transaction account, #12345-6789, in March 2006. Bloggs indicated that he was born in Yemen, presented a New Zealand driver's licence as identification, and claimed he was the self-employed owner of a bakery identified as Acme, Inc. A business transaction account, #23456-7891, was opened in January 2008 for Acme, Inc.

Between 17 January 2013, and 21 March 21 2013, Joe Bloggs was the originator of nine IFTs totalling NZ$225,000. The IFTs were always conducted at the end of each week in the amount of NZ$25,000. All of the IFTs were remitted to the Bank of Anan in Dubai, UAE, to benefit Kulkutta Building Supply Company, account #3489728.

Reviews covering the period between 2 January and 17 March 2013, revealed that 13 cash deposits totalling approximately $50,000 were posted to Bloggs' personal account. Individual amounts ranged between $1,500 and $9,500 and occurred on consecutive business days in several instances.

A review of deposit activity on the Acme, Inc. account covering the same period revealed 33 cash deposits totalling approximately $275,000. Individual amounts ranged between $4,446 and $9,729; however, 22 of 33 deposits ranged between $9,150 and $9,980. It was further noted that in nine of 13 instances in which cash deposits were made to both accounts on the same day, the combined cash deposits exceeded $10,000.

A search of the internet identified a website for Acme, Inc., which listed the company as a bakery that provides remittance services to countries in the Middle East including Iran. In addition, the DIA website did not list Acme as a licensed money wire transfer business. We have begun action to close this account due to the suspicious nature of the transactions being conducted by Joe Bloggs.

NOTES

This narrative is a well-written summary of all the suspicious activity and supports the stated purpose for filing the SAR. Furthermore, the narrative provides an internal reporting entity case number for the SAR that can be used by law enforcement should investigators wish to contact the reporting entity to discuss pertinent facts presented in the narrative. Specific information is also provided in the narrative that details the source and application of suspicious funds. The SAR also identifies other actions taken by the financial institution as part of its internal due diligence program and its efforts in detecting possible illegal activity being facilitated by the person of interest.

Example 2: Insufficient SAR Filed by a Financial Institution

Bob Smith was the originator of nine IFTs totalling $225,000. All of the transfers were remitted to a Dubai based company. During the same period of time, John Doe deposited cash into his account. See attachment.

NOTES

This SAR does not provide specific details on the application of the suspicious funds (the name, bank, and account number of the beneficiary, if identifiable). There is also no information about the relationship, if any, between the entity and the customer. Also, no specific transaction data is provided that identifies the dates and amounts of each wire transfer.

Example 3: Sufficient SAR Filed by a Money Remitter

For at least a year, beginning on 20 May 2012, two customers, John Smith and his son, Bob, have been using our money remittance service to send large amounts of cash to receivers named Jane Doe and Mary Doe located in Antigua. Funds are sent to the XYZ Caribbean Money Centre in St. Johns, Antigua. The amount of money presented each time by John and/or Bob Smith is usually $5,000 and the transmittals are sent bi-weekly.

During one particular incident earlier this month, on 12 June 2013, John Smith attempted to send $10,000 without proper identification. We refused to send the funds and Mr. Smith left the premises. He returned later in the afternoon with identification but only sent $5,000. All incidents/transactions have occurred at our store in Anytown. The office has copies of the driver's licences of both customers. Suspicion lies in the Smiths' occupation (lawyers), and the amount of money leading to the suspicion of possible tax evasion.

NOTES

This narrative provides enough details of the money remittance customers' frequent suspicious money transmittals to support the purpose of the SAR. Also, the beneficiary information, including beneficiary names and location, was included. The narrative identified the person(s) of interest by name and occupation and related that driver's license information was retained at the remitter's business location.

Example 4: Insufficient SAR Filed by a Money Remitter

An elderly male sent money to two different countries. These payments could be for a scam.

NOTES

There is no explanation given as to why the money remitter considers this activity suspicious, or how they concluded the remittance could be a scam. The reporting entity also did not provide any information about the purchaser or nature of the business and/or if this activity was normal or unusual for the purchaser or business.

Example 5: Sufficient SAR Filed by a Real Estate agent

We are filing this SAR as an offer placed on a property is substantially higher than the value of the property. The subject of this SAR also uses many aliases and has a history of tax fraud.

On 10 December 2019, Mr Bob Smith (aka Robert James Smith, Bob Jones, James Smith) made an offer to purchase a property at 123 Main Street, Anytown through sales agent Mary Anderson. Mr Smith is a man in his 40s with dark hair. The offer was $1.5m over the Rating Valuation.

The sales agent notified our AML compliance officer, Joe Blogg, of her suspicion. Joe searched the internet for Mr Smith and found that Mr Smith has a history of tax fraud (see attached link). Mr Smith also been the director of multiple companies that have been removed from the Companies Register. Joe searched independent databases for NZ property holdings for Mr Smith and his aliases, but did not find any current holdings.

NOTES

This narrative is a well-written summary of all the suspicious activity and supports the stated purpose for filing the SAR. Specific information is also provided in the narrative on the individual being reported. The SAR also identifies other actions taken by the reporting entity as part of its internal due diligence program and its efforts in detecting possible illegal activity being facilitated by the person of interest.

Example 6: Insufficient SAR Filed by a Real Estate agent

We have discovered that this individual is buying and selling several properties utilising multiple agencies in a short time frame. We have selected red flag indicators.

NOTES

This SAR does not provide specific details about the suspicious activity or why it is considered suspicious. The reporting entity also does not provide further information on the red flag indicators or why they were selected.

Example 7: Sufficient SAR Filed by a TCSP

We are filing this SAR as our client has been indicted in the UK for breaching the Bribery Act 2010.

Funds which may have been sourced from his UK transactions may have been deposited into the accounts of three New Zealand Limited Partnerships which we administer on behalf of John Smith.

Due to the indictment, we are now suspicious of the activities conducted through the Limited Partnerships. All funds received into the accounts of the three New Zealand Limited Partnerships in relation to these activities have been frozen and no payments will be made from these accounts until the resolution of this matter.

I have attached the following:

1) A list of involved parties.
2) A list of suspicious transactions.
3) A copy of the indictment.
4) Copies of John Smith's CDD documents.

NOTES

This narrative is a good summary of the reason for suspicion and supports the stated purpose for filing the SAR. Specific information is also provided in the attachment on the individual being reported. The SAR also identifies other actions taken by the financial institution as part of its internal due diligence program and its efforts in detecting possible illegal activity being facilitated by the person of interest.

Example 8: Insufficient SAR Filed by a TCSP

This person requested a private box to receive parcels on 8 September 2017, then cancelled two weeks later before providing AML/CFT documents or sending payment.

NOTES

This SAR lacks specific details about the activity or why it is considered suspicious. The reporting entity also did not detail any attempts to contact the individual being reported, if the reason for cancellation was due to their refusal to complete the required CDD documents, or if any other suspicious information was held on or discovered about the individual.

Example 9: Sufficient SAR Filed by an Accountant

We are filing this SAR because our client refuses to provide an explanation for a suspicious withdrawal of cash in the amount of $650,000, and we suspect he is committing tax evasion.

Acme Ltd has been a client for 7 years. The owner of the company, Bob Jones, asked us to provide accounting and tax services to a new entity he created, XYZ Ltd.

We asked for details on several occasions over the course of 4 months where the withdrawn funds had been deposited and if he was registered for GST, so that we could complete tax filings. A list of the email dates is attached. The client ignored all requests for information. We were then contacted by ABC Bookkeepers and told that Bob Jones had moved his business to them, and asked for his files.

NOTES

This narrative is a good summary of the reason for suspicion and supports the stated purpose for filing the SAR. Specific information is also provided in the attachment on the individual being reported and the attempts to gather information required.

Example 10: Insufficient SAR Filed by an Accountant

We reviewed our client's accounts and found an unusually large transaction. We decided that it was suspicious.

NOTES

This SAR does not provide any specific details about the large transaction or why it is considered suspicious. The reporting entity also did not provide details on any action taken to understand the transaction.

INTERNATIONAL AML/CFT NEWS

Netherlands

Criminality blooms around flower trade, according to new report

An investigation was conducted for a collective of stakeholders including the police, public prosecutors, and Royal Flora Holland growers' cooperative to examine how the flower transport industry is used to distribute drugs through the Netherlands. The report, published in March 2021, shows the entire sector is vulnerable to drug trafficking, money laundering and exploitation of workers due to its global network and relatively lax controls. The report is currently only published in Dutch; the NZ FIU has requested a copy in English.

Estonia

How shady clients from around the world moved billions through Estonia

The Organized Crime and Corruption Reporting Project, an investigative reporting platform for a worldwide network of independent media centres and journalists published an exposé in 2017 that revealed billions of dollars of dirty money flowed through Danske Bank's branch in Estonia. The original audit report written by the Estonian Financial Supervision Authority (FSA) has now been made public.

The FSA audit found that the relationship managers in the non-resident banking unit ignored obvious signs of money laundering. Contracts were often not collected as part of due diligence and implausible trades – such as one for US$1,000 paint cans – were not questioned.

United States

Fraudsters are laundering millions through online investment platforms

Tech-savvy fraudsters stealing from the US government's COVID pandemic relief programs to help businesses have allegedly been laundering the illicit funds via online investment funds, according to law enforcement officials.

The online investment funds suspected to have been used include Robinhood, TD Ameritrade, E-Trade and Fidelity. These accounts are relatively easy to sign up for, and provide relative anonymity compared with bank accounts, which may be appealing to criminals.

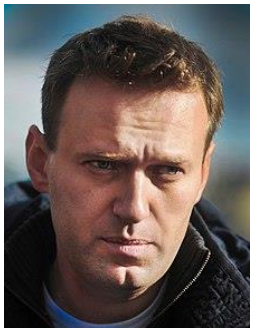
Visa moves to allow payment settlements using cryptocurrency

In March 2021, Visa announced that it will allow the use of the cryptocurrency USD Coin to settle transactions on its payment network. The USD Coin (USDC) is a stablecoin cryptocurrency whose value is pegged directly to the US dollar.

In an interview, Visa revealed to Reuters that they had launched the pilot program with payment and crypto platform Crypto.com and plan to offer the option to more partners later this year.

Corruption/Sanctions

US applies wide range of sanctions to Russian Officials and entities



Alexi Navalny (2011)

On 2 March 2021, the US Departments of Treasury, State and Commerce announced the coordinated imposition of sanctions and other restrictive measures on Russia and Russian officials and entities for the "poisoning and subsequent imprisonment of Russian opposition figure Alexei Navalny". The US Department of Commerce, Bureau of Industry and Security announced the addition of 14 entities located in Russia, Germany and Switzerland "based on their proliferation activities in support of Russia's weapons of mass destruction programs and chemical weapons activities" to its Entity List.

Also in March, the Biden Administration stated it was sanctioning a German chemicals company called Riol-Chemie because of its "activities in support of Russia's weapons of mass destruction programs." Investigative files compiled by the authorities in Lithuania show that Riol-Chemie received hundreds of thousands of dollars from a British Virgin Islands-registered company accused of laundering some of the stolen money that was uncovered by Magnitsky.

Countering Financing of Terrorism

Bangladesh militants use Bitcoins for laundering money to Kashmir

According to a senior police official, a Special Action Group of the Dhaka Metropolitan Police's counter-terrorism and Transnational Crime Unit arrested two Ansar Al Islam (AI) militants in September 2019. Through interrogation, police learned that AI and another militant group, Ansarullah Bangla Team (ABT) had been receiving funds through the Bitcoin system since 2014. The militant groups revealed that they had shifted from 'hundi' to Bitcoin, as it is an easier method to exchange illegal funds.

Three arrested in Spain for terrorist financing

The Spanish National Police supported by Europol, arrested three individuals for their suspected involvement in the facilitation of terrorist financing. The suspects are believed to have used humanitarian aid for Syrian orphans to finance the activities of Al-Qaeda affiliated militants.

Human Trafficking

Two people arrested for human trafficking, forced labour and money laundering

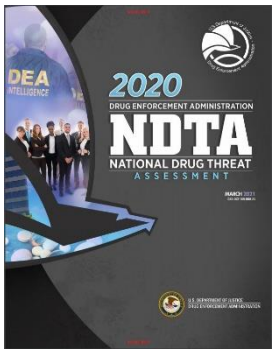
Two residents of the state of North Carolina were arrested relating to violations of conspiracy to smuggle, transport and harbour illegal residents for commercial advantage or private financial gain, conspiracy to commit forced labour, and money laundering.

In order to smuggle Honduran women into the US, those involved in the conspiracy wired thousands of dollars from locations in North Carolina to Honduras and Mexico to smugglers.

Once the women were in the US, they were taken to the residence of an individual in North Carolina where they were forced to provide labour and services by means of force, threat, physical restraint, or threats of physical restraint.

US Drug Enforcement Administration (DEA)

2020 National Drug Threat Assessment



The US Drug Enforcement Administration published its annual National Drug Threat Assessment (NDTA) in March. The report details Transnational Criminal Organisations from Mexico, Colombia, the Dominican Republic, as well as an overview of organisations based in Hong Kong, Macau and Taiwan that are linked to illicit drug smuggling in Australia and New Zealand. The report also details the methods criminals have used to move and launder the proceeds from illicit drug sales, including the use of digital currency ATMs and withdrawals of Bitcoin from dark web merchants.

European Banking Authority (EBA)

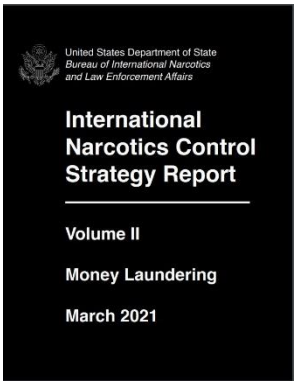
Biennial Opinion on Risks of ML/TF

The EBA is required to issue an Opinion on the risks of money laundering and terrorist financing affecting the European Union's financial sector every two years. The EBA published its third Opinion in March 2021. The ML/TF risks identified by the EBA include those that are applicable to the entire financial system (e.g. use of innovative financial services) while others affect specific sectors (e.g. de-risking). As a complement to this Opinion, the EBA has developed an interactive tool, which provides access in a user-friendly manner to all ML/TF risks covered in the Opinion.

US Department of State

International Narcotics Control Strategy Report Volume II

The 2021 edition of the Congressionally mandated International Narcotics Control Strategy Report (INCSR), Volume II: Money Laundering focuses on narcotics-related money laundering. The report reviews the anti-money laundering legal and institutional infrastructure of jurisdictions and highlights the most significant steps each has taken to improve its AML regime. It also describes key vulnerabilities and deficiencies of these regimes and identifies each jurisdiction's capacity to cooperate in international investigations.



In addition to identifying countries in relation to illicit narcotics, the INCSR is mandated to identify 'major money laundering countries'. The statute defines a major money laundering country as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking". The INCSR lists 80 "major" money laundering jurisdictions identified in 2020.

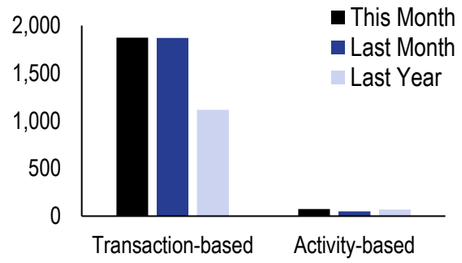
Inclusion in Volume II is not an indication that a jurisdiction is not making strong efforts to combat money laundering or that it has not fully met relevant international standards. The INCSR is not a "blacklist" of jurisdictions, nor are there sanctions associated with it.

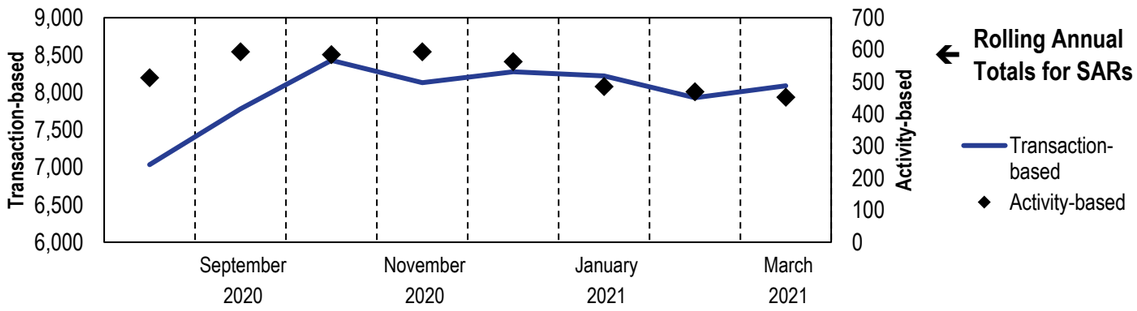
MONTHLY STATISTICS* | NEW ZEALAND POLICE **FINANCIAL INTELLIGENCE UNIT** March | 2021

SUBMITTED REPORTS to the FIU*

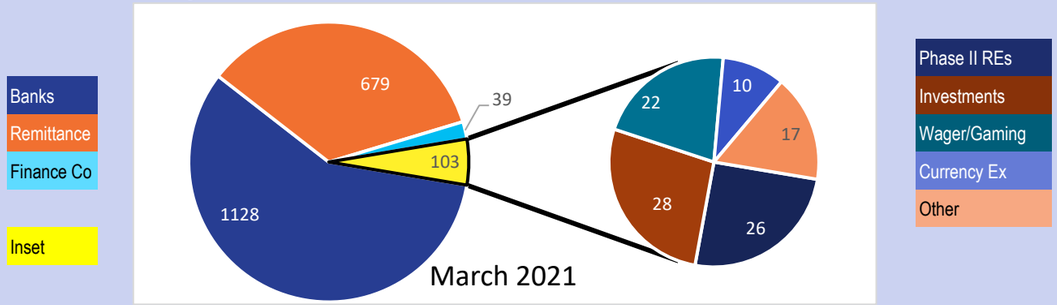
Processed Suspicious Activity Reports (SARs)

	This Month	*Last Month*	*Last Year*
	March 2021	**February** 2021	**March** 2020
Transaction-based	**1,874**	**1,869**	**1,115**
Activity-based	**75**	**51**	**69**
Total	**1,949**	**1,920**	**1,184**



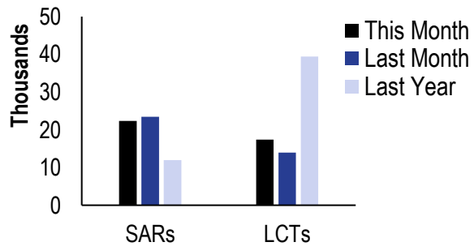


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

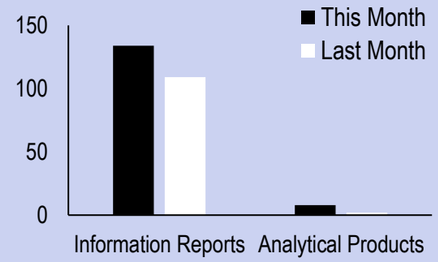
	This Month	*Last Month*	*Last Year*
	March 2021	**Feb** 2021	**March** 2020
SARs	**22,376**	**23,455**	**11,964**
IFTs	**435,513**	**386,474**	**440,647**
LCTs	**17,376**	**13,947**	**39,445**



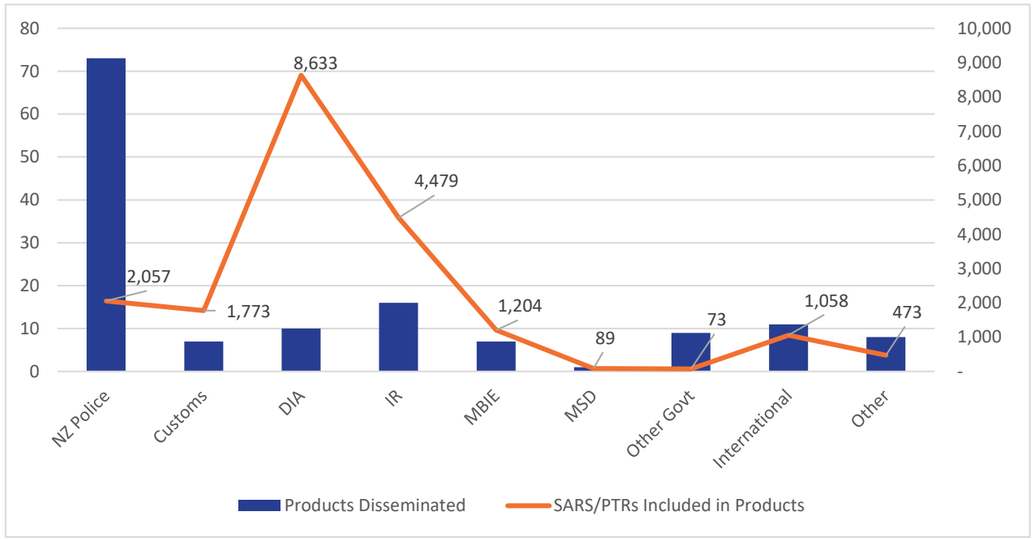
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

	This Month	*Last Month*
	March 2021	**February** 2021
Information Reports	**134**	**109**
Analytical Products	**8**	**2**
Total Products	**142**	**111**



Disseminations of Products by Recipient



Disseminations of Products by Included SARs and PTRs

SARs		PTRs		Total		
2,170	+	**17,669**	=	**19,839**	→ **18,958**	Info Report
					→ **881**	Intel Report

*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.

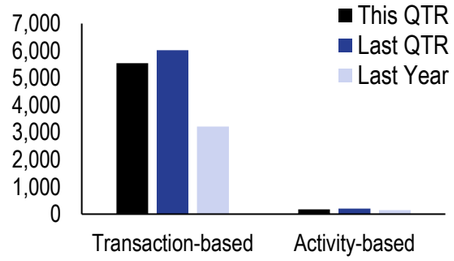
1 January 2021 - 31 March 2021

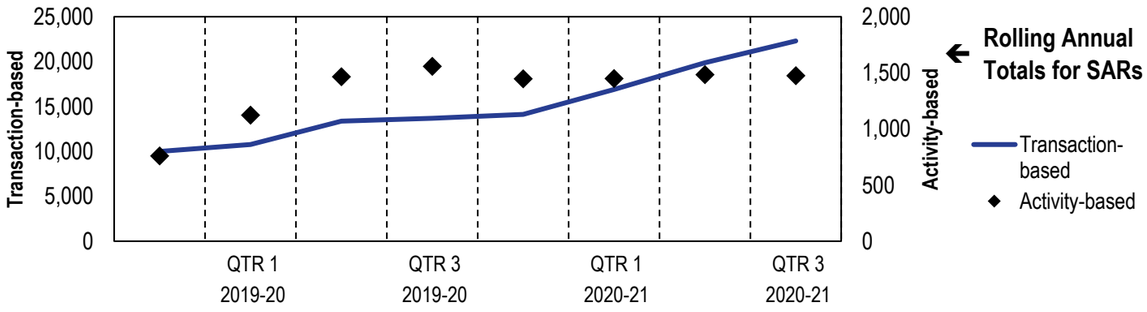
QUARTERLY STATISTICS* | NEW ZEALAND POLICE FINANCIAL INTELLIGENCE UNIT | QTR 3 | 2020-21

SUBMITTED REPORTS to the FIU*

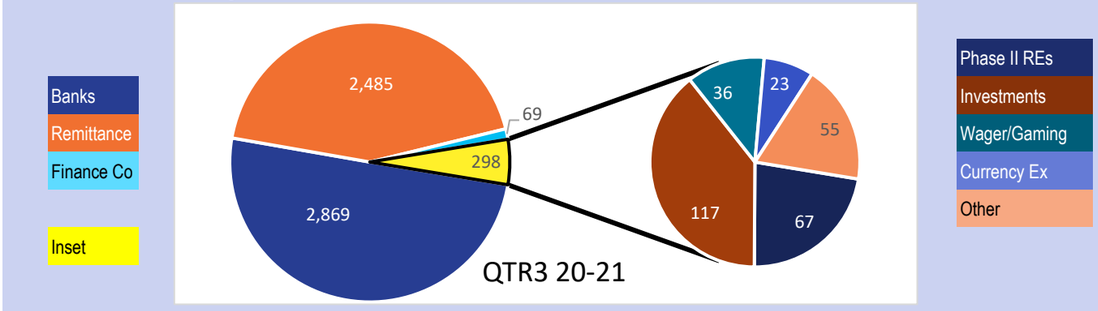
Processed Suspicious Activity Reports (SARs)

	This QTR	*Last QTR*	*Last Year*
	QTR 3 2020-21	QTR 2 2020-21	QTR 3 2019-20
Transaction-based	5,549	6,024	3,217
Activity-based	172	205	144
Total	5,721	6,229	3,361



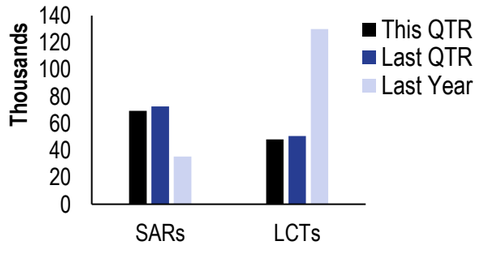


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

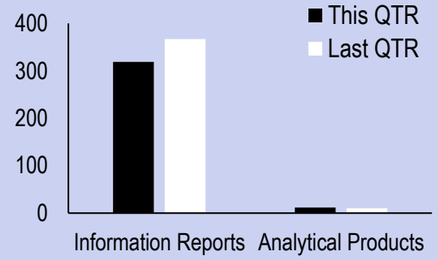
	This QTR	*Last QTR*	*Last Year*
	QTR 3 2020-21	QTR 2 2020-21	QTR 3 2019-20
SARs	69,360	72,669	35,330
IFTs	1,211,399	1,293,591	1,284,840
LCTs	48,110	50,658	130,091



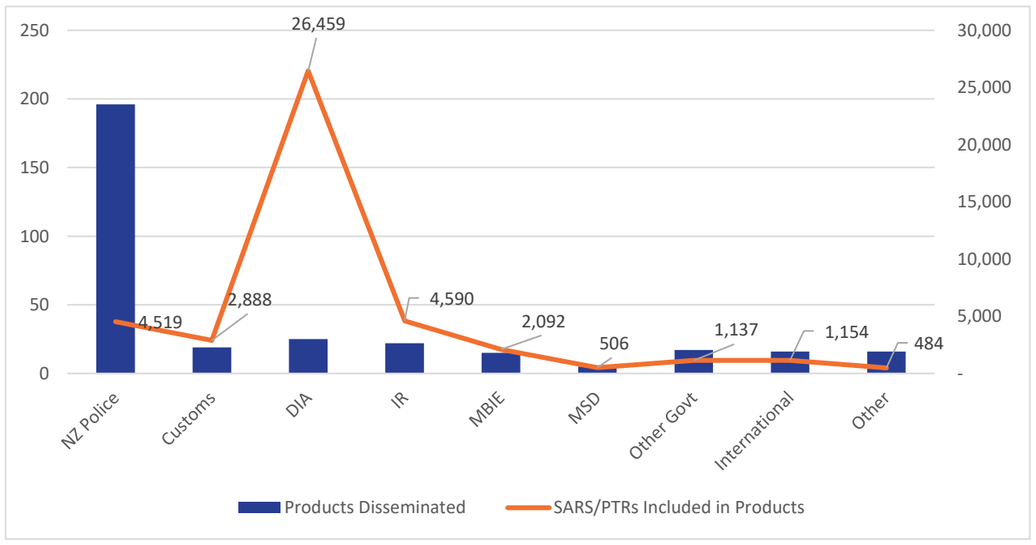
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

	This QTR	*Last QTR*
	QTR 3 2020-21	QTR 2 2020-21
Information Reports	319	367
Analytical Products	12	10
Total Products	331	377



Disseminations of Products by Recipient



Disseminations of Products by Included SARs and PTRs

SARs		PTRs		Total		
5,598	+	38,231	=	43,829	→ 42,916	Info Report
					→ 913	Intel Report

*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.

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

@NZFIU

www.police.govt.nz