The Suspicious Activity Report

OCTOBER / NOVEMBER 2022

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 Superintendent David Lynch. This report is comprised of FIU holdings and open-source media reporting collected within the last month.

Background

The Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act became law in October 2009. The Act's purpose is to detect and deter money laundering and contribute to public confidence in the financial system. It seeks to achieve this through compliance with the Financial Action Task Force (FATF) recommendations. The Financial Intelligence Unit produces this monthly report as part of its obligations under section 142(b)(i) and section 143(b) of the AML/CFT Act 2009. The Financial Crime Group is made up of the Financial Intelligence Unit, Asset Recovery Unit, the Money Laundering Team, and a group at Police National Headquarters.

Financial Intelligence Unit

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

Asset Recovery Unit

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

Money Laundering Team

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

Letter from the Editor

Dawn Logan, Senior Strategic Advisor (Acting)

Tēnā koutou.

I thought I'd come out from behind the curtain and introduce myself to everyone. It's been just over three years since I started with the FIU as the Research Analyst and though I've taken on more responsibilities as the years have passed, this newsletter has continued to be my favourite project.

My background is in numbers – accounting and tax – and it has been interesting to transition to a role steeped in researching and writing. Of course, there is overlap between my previous speciality and the world of anti-money laundering. Earlier this month, a colleague asked me if I'd heard about electronic sales suppression, a form of 'skimming', that can help a business lower their GST and income tax payable. This led me down a few rabbit holes until I had enough information to share it with you all (see page 7).

The FIU and our government agency partners have had another busy year, most notably the swift implementation of sanctions upon Russia at the beginning of the year in response to the Russian invasion of Ukraine. Led by the Ministry of Foreign Affairs and Trade (MFAT), this work has been ongoing as more and more individuals and entities are added to the designated persons list nearly every month. Reporting entities will be familiar with these new sanctions and the reporting required. Your efforts have been noted and appreciated.

This year also saw the completion of the AML/CFT Act review and beginning of the implementation work for the 200+ recommendations listed in the final report. Most, if not all, New Zealand government agencies were involved in this massive undertaking, with significant input and collaboration from the private sector. There is quite a lot of work to come, but it will ensure our Act is fit for purpose, New Zealand's international reputation is maintained, and the public continue to have confidence in the financial system.

The world opened up a bit in 2022, with conferences returning to in-person attendance. Christiaan Barnard, Manager of the FIU, had the opportunity to travel to Latvia for the Egmont Plenary in June (detailed in the July 2022 edition of *The Suspicious Activity Report*), as well as the Pacific Financial Intelligence Community Plenary in November. And our own FIU/ACAMS conference hosted over 300 participants and international speakers in person, providing opportunities to network and connect.

Looking towards 2023, my team has expanded to include a new Research Analyst, which means I'll be handing over the reins to *The Suspicious Activity Report*. Work has already begun on a feature article for the next edition!

I hope everyone is able to have some time out of the holiday break and spend some well-deserved time with friends and family.

Ngā mihi o te wā. Kia hūmārie to koutou haere i ngā wā whakatā.

NEW ZEALAND AML/CFT NEWS

New Zealand Security Intelligence Service | Te Pā Whakamarumaru

National Terrorism Threat Level revised from MEDIUM to LOW

New Zealand's National Terrorism Threat Level has been revised from Medium to Low as of 30 November 2022. This reflects a change in assessment of the likelihood of a terrorist attack, according to Director-General of Security, Rebecca Kitteridge.

The Threat Level and the assessment that underpins it enables relevant government agencies to ensure that they are appropriately placed to respond and to mitigate risk. Ms Kitteridge stated that the National Terrorism Threat Level is continually evaluated and could change at any time.

Kia mataara ki ngā tohu – Know the signs

NZSIS recently published a guide to raise awareness of indicators of violent extremism, to help New Zealanders identify some of the key warning signs. Violent extremism is often difficult to identify and can involve a range of behaviours.

NZSIS investigators have reviewed all cases of violent extremism in New Zealand since 2006 and have grouped the behaviours and activities that are of most concern under seven indicators. These indicators are a guide, rather than a checklist – the individual behaviours and activities listed in this guide are concerning when they occur alongside other activities, but on their own may not be considered signs of violent extremism.

Independent Police Conduct Authority | Mana Whanonga Pirihimana Motuhake

Review of Police management of fraud allegations

IPCA
Independent Police Conduct Authority
Mana Whanonga Pirihimana Motuhake

This Independent Police Conduct Authority (IPCA) report is the outcome of a review of Police investigative practices in relation to fraud, which was initiated following the receipt of a number of reports about the way Police handled fraud complaints.

The report makes a number of recommendations to reduce the prevalence of fraud in New Zealand and improve the experience of victims of fraud, including the suggestion that Police lead the development of a fraud prevention strategy with the support of other government agencies and the private sector.

FIU News

2022 AML/CFT Conference

Hosted by the FIU and ACAMS, the 2022 AML/CFT Conference centred on the theme of 'Money Laundering is Not a Victimless Crime'.

The conference began with a keynote presentation from the Honourable Nanaia Mahuta, Minister of Foreign Affairs, on the financial sanctions brought against Russia, followed by a panel discussion on how implementing international sanctions affects the private sector.

The International theme continued with a look at where, how, and why money laundering was happening in British Columbia, Canada and how it can be prevented. The Cullen Commission's findings and how they impact New Zealand and the Pacific were brought to the audience by Barrister Gary Hughes and Vancouver based Senior Commission Counsel, Patrick McGowan, who was part of the Commission's inquiry team.

Jarod Koopman, Executive Director, Cyber and Forensic Services IRS – Criminal Division informed conference participants on emerging trends and the use of the dark web and cryptocurrency in child exploitation investigations. Jarod also provided a case study on the value of partnering with the private sector (Coinbase) that resulted in 23 victims being identified, 338 offenders arrested, and 38 countries impacted.

Finishing the day, Eleanor Parkes, Director of Child Alert NZ, shared the lessons learned from child exploitation investigations, especially how those investigations impact New Zealand victims. Included in this session was a moving account from a person who had been trafficked as a young person.

The Honourable Tim Grosser started the second day of the conference with a very engaging account of the geopolitics of the Russia/Ukraine conflict and the influence this has on the way sanctions are implemented. This sobering presentation highlighted possible impacts of the conflict to New Zealand.

Ilze Znotina, former head of the Latvian FIU, travelled to New Zealand to attend the conference in person to share insights into how a major scandal like the ABVL Bank's involvement in money laundering can impact a small country and its compliance processes surrounding sanctions and money laundering.

In an afternoon session on the second day, Immigration New Zealand Investigation Manager, Carl Knight, stepped the audience through a case on modern day slavery and human trafficking in New Zealand. Operation Star began with an immigrant who had overstayed his visa, leading to an investigation into possible human trafficking. The operation uncovered multiple victims who had been trafficked to New Zealand over two decades. The offender was sentenced to 11 years prison after being convicted on 10 human trafficking charges and 13 slavery charges.

Pacific Financial Intelligence Community Plenary

The first annual Pacific Financial Intelligence Community (PFIC) Plenary was held in Port Moresby, Papua New Guinea over two days in November, hosted by the PNG Financial Analysis and Supervision Unit. The plenary was sponsored by New Zealand Police and the Australian Transaction Reports and Analysis Centre (AUSTRAC) and attended by 16 Pacific FIUs. Christiaan Barnard, Manager of NZ FIU, and Sarah Coddington-Lawson, FIU Analyst, attended on behalf of the New Zealand FIU.

The PFIC is a regional body, consisting of FIUs located in the Pacific region. It was established out of the need to deal with common challenges that confront the Pacific region. PFIC encourages multilateral and bilateral collaboration on issues of mutual priority through the regular dialogue and engagement between members that it provides.

During the plenary, Sarah provided an overview of Mobile Banking Platforms, which is the topic of a joint strategic paper that the New Zealand FIU is leading. Christiaan led a discussion on the strategic direction of PFIC looking forward over the next three years. The discussion included understanding shared capability and operational priorities; de-banking in the Pacific and the role PFIC could play; and the expansion of membership.

PFIC members agreed to focus on corruption in the Pacific region by developing a paper on regional financial indicators and red flags of corruption for use by private and public stakeholders, with New Zealand agreeing to take the lead on this paper. AUSTRAC agreed to lead the integration of corruption methodology and detection into financial intelligence training.

PFIC members also agreed to provide financial intelligence insights to mitigate de-banking in the region by producing a regional ML/TF risk assessment, led by AUSTRAC, and deliver a series of webinars to members on virtual assets to inform future PFIC considerations, led by Cook Islands.

ELECTRONIC SALES SUPPRESSION

What is electronic sales suppression?

Electronic sales suppression (ESS) is a method used by businesses to manipulate electronic sales records, either during or after the point of sale, in order to hide or reduce the value of individual transactions. ESS is undertaken to reduce the recorded turnover and corresponding tax liabilities of the business while providing what appears to be a credible and compliant audit trail.

Background

Sales suppression, also known as 'skimming' has always existed in one form or another to evade taxes. Skimming can be achieved through various basic techniques such as failing to ring cash sales into the cash register or diverting sales to a second cash register which was not accounted for in the business accounts. In some cases, businesses employing these methods keep two sets of books and records: one for the tax authorities and the other for the owner to obtain loans or to show potential buyers when looking to sell the business.

Modern cash registers in the retail sector operate as comprehensive sales and accounting systems, often using standard business software, and are relied on as effective business accounting tools for managing the enterprise. Such systems can be manipulated to permit skimming of cash receipts and when equipped with sales suppression software, can facilitate elaborate frauds.

How is it done?

Modern technology allows transactions to be under-reported through various means, even allowing a business owner to perform ESS at a convenient time, such as at the end of the business day. Automated sales suppression devices are typically used in conjunction with a point of sale (POS) or electronic cash register to alter business records, and include phantom-ware, zappers, and sales suppression as a service.

Phantom-ware

Phantom-ware is a software program already installed or embedded in the accounting application software of a modern point of sale system. The *phantom* in phantom-ware refers to the hidden nature of the software. The software is not easily accessible; investigators have seen a variety of access methods, including swipe-cards, hidden buttons on the screen, or a combination of keys that lead to a secret menu.

Operating in the background, the software will capture the transaction data before it is logged into the cash register. If sales are deleted, the tool can automatically adjust inventory details to avoid an apparent mismatch. Where accounting changes have been made it may also print out a log of the transactions deleted so the business owner can manage and/or track what has changed.

Phantom-ware can also manipulate sales after a transaction. The $50 sale may be logged as $30, allowing the owner to effectively skim $20 off the proceeds, lowering the GST due to be paid to IRD.

Zappers

Zappers are external software programs loaded on electronic media such as USB keys. They allow a business to 'zap' (delete) selected sales, then recalculate individual receipts and taxes due. The most sophisticated systems can reconcile differences with the business' other financial records to hide evidence of the fraud. Zappers are most effective when a sale is made in cash, due to the lack of corroborating records for the transaction.

Zappers are designed, sold, and maintained by those who develop industry-specific POS systems, but independent contractors have also developed these tools. Zappers operate similarly to phantom-ware but are more difficult to detect because of their sophisticated design and because the software is not typically connected during normal use of the POS.

Zappers can also be accessed remotely via the internet, connecting directly to the cash register. These are called 'sales suppression as a service'.

Sales suppression as a service

This method takes the software offsite and turns hard code on a system or USB drive into a subscription model service via the internet. Those who sell this service offer to provide erasing, deleting, or purging sales, as well as crashing or physically destroying a client's hard drive and replacing it. This subscription could easily be listed as a maintenance or support fee, paid to the POS installer.

Studies

United Kingdom

At (UK) Budget 2018, the government announced a commitment to hold a call for evidence on electronic sales suppression, which was open from 19 December 2018 to 20 March 2019. There were 11 responses in total from software sellers, EPOS system manufacturers, consultants and professional representative bodies.

EPOS industry stakeholders had a relatively good working knowledge of the different types of ESS, including abusing built-in features of POS software such as training mode or voiding sales and turning off the journal to ensure sales or refunds are not recorded.

One of the main themes from the responses was that some sectors appear to be higher risk than others, with respondents stating ESS is particularly evident in small independent retailers, takeaways and the hospitality sector. Respondents also indicated some businesses have explicitly asked EPOS providers, and software developers, to include ESS functionality in their till systems, with a primary driver being to keep the business's turnover below the VAT registration threshold.

USA

California's anti-zapper law came into effect 1 January 2014, making it a crime to knowingly purchase, install, use, transfer, or sell any "automated sales suppression device or zapper or phantom-ware" with the intent to defeat or evade the determination of California's sales or use taxes by falsifying records.

After the law came into effect, California state revenue authorities undertook an audit of 2,197 restaurants between 2014 and 2019. They found nearly one fifth of California restaurants had illegal software applications installed or attached.

International Solutions

OECD

The OECD released a study in 2013 to help all countries understand address the risk of electronic sales suppression. It describes some of the most common ESS techniques used by businesses to evade tax, and how these methods can be detected by tax auditors. The report makes several recommendations to countries' tax administrations for addressing ESS.

Many countries around the world have since introduced measures to identify, investigate and prosecute businesses using ESS to commit tax evasion. Strategies that countries have adopted include raising public awareness of the illegal activity, working with industry bodies to strengthen voluntary compliance, improving audit and investigation skills of tax auditors, developing and sharing intelligence between government agencies and countries, and the use of advanced technology to support traditional investigative techniques. Some jurisdictions have also criminalised the provision, possession, or use of ESS software.

Fiji

Fiji implemented a comprehensive digital invoice regime in 2018 with the goal of automatic, real-time, and encrypted reporting of all taxable transactions, business to business and business to consumer. Businesses captured under the regime are required to install, implement and operate accredited electronic fiscal devices (EFD) with each POS machine.

The regime intended to increase VAT compliance. Before implementation, Fiji first undertook a 40% reduction in the VAT rate (from 15% to 9%) on 1 January 2016.

From 1 January 2018, all supermarkets and pharmacies (Group 1) were required to comply with the new regime. Group 2, containing hardware companies, accounting firms, medical centres, travel agencies and law firms, came under the new regime in June 2018, with Group 3 following in July 2019.

A special feature of the EFD is the Proof of Audit function, which means any invoice must be approved by the tax administration server. The EFDs monitor each sales point and issues a digitally signed invoice; the process is very quick and does not affect the printing of receipts for customers. Taxpayers and customers can log onto the system to verify the receipt information by scanning the embedded QR code on the receipt with a smart phone.

Receipts are normally reported from every sales point operated by taxpayers in real-time, however some receipts may have gone missing due to internet failure, power outage etc, so some may have never been reported. The scan of the QR code by a customer contributes to the collection of audit data and in return, customers can win various rewards, such as phone top-ups.

New Zealand

A Regulatory Impact Statement on sales suppression software was published in June 2021 by The Treasury New Zealand. It noted Inland Revenue had been informed that overseas businesses may be selling sales suppression software to New Zealand businesses, and existing tax law appeared insufficient to deter the usage of ESS. Three options were provided to address the policy problem, with the preferred option being to establish an appropriate penalty regime, enforced by Inland Revenue.

Subsequently, Inland Revenue issued Revenue Alert RA 22/01 – "Consequences of acquiring, possessing or using electronic sales suppression tools" - in December 2022. The Alert advises of the new measures introduced to respond to the threat posed by ESS tools and outlines the Commissioner's current view on how the law should be applied.

A new civil penalty and two new criminal offences related to the use of ESS tools were introduced into the Tax Administration Act in April 2022. The acquisition or possession of a suppression tool now attracts a civil penalty of $5,000. In addition, it is a criminal offence to manufacture or supply a suppression tool and/or to acquire or possess a suppression tool. These offences carry fines of up to $250,000 and $50,000 respectively.

Inland Revenue has stated that where it identified specific instances of ESS tools being used to evade tax, it would require payment of any evaded tax, plus 150 percent shortfall penalties and use of money interest. Anyone who believes they may have become involved with ESS tools should discuss the matter with their tax advisor or Inland Revenue, as well as consider whether they may need to make a voluntary disclosure.

What Actions Can be Taken?

Professional auditors

Financial or tax auditors may use the following audit methods to help uncover the electronic sales suppression:

- Compare financial ratios to industry benchmarks
- Use auditing software to recognise sales with unusual patterns
- Calculate expected salaries and wages based on average hours and salaries compared with expectations of business results
- Educate auditors on how to find zappers and phantom-ware devices

Request a receipt

Although consumers may not notice if a business appears to be using ESS software, they can do their part to ensure tax compliance by always requesting a copy of their receipt. This step may counteract steps taken to delete sales and evade taxes.

Financial institutions

Entities who provide business loans should request GST or Income Tax returns in addition to financial statements from applicants to ensure the amount of revenue shown is consistent.

INTERNATIONAL AML/CFT NEWS

Australia

Call for cashless cards to curb billions in dirty cash gambled in pokies

According to the findings of a joint law enforcement agency inquiry, billions of dollars in illicit cash was laundered through NSW poker machines. Project Islington, led by the NSW Crime Commission, found "a significant amount of money which is put through poker machines is the proceeds of crime", and called for the introduction of cashless gaming cards. The inquiry also found "compelling evidence that drug dealers were gambling on a large scale via electronic gaming machines with the money obtained by their offending".

Criminals coerce elderly scam victims into working as drug mules

The Australian Federal Police is investigating a new crime trend involving elderly scam victims being forced to act as drug mules by organised criminals. The trend was detected after the Australian Border Force (ABF) identified a series of elderly passengers carrying illicit drugs at Sydney airport over the last year. When questioned by detectives, some of those arrested claimed they had been coerced into the role after becoming the victim of an online financial scam.

EUROPOL

30 tonnes of cocaine seized in raids against European 'super cartel'

Under the codename Desert Light, police carried out joint raids in several European countries and the UAE between 8 and 19 November with the aim of dismantling a 'super-cartel' suspected of controlling one-third of the cocaine trade in Europe.

EUROPOL announced that 49 suspects were arrested during the investigation, after raids in Europe and the UAE targeting the cartel's 'command and control centre' and logistics network. The arrests followed parallel investigations in Spain, France, Belgium, the Netherlands, and the UAE, coordinated by EUROPOL, into a criminal network involved in large-scale drug trafficking and money laundering.

INTERPOL

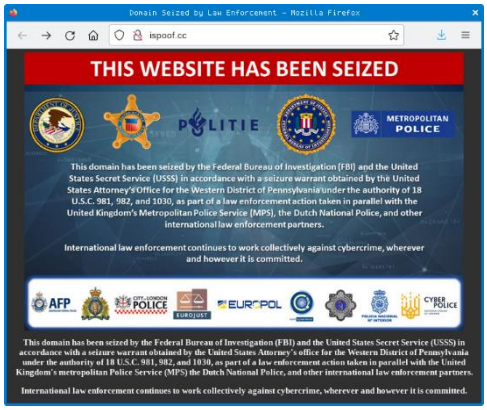
Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams

A two-month operation, codenamed First Light 2022, was coordinated between INTERPOL and local police agencies in 76 countries around the world. Police in participating countries raided national call centres suspected of telecommunications or scamming fraud, particularly telephone deception, romance scams, email deception, and connected financial crime.

In the course of the investigation, police say they identified 3,000 different suspects, froze 4,000 bank accounts, arrested over 2,000 operators, fraudsters, and money launderers, while conducting raids at 1,770 locations worldwide.

United Kingdom

More than 100 arrests in UK's biggest ever fraud operation



In the 12 months to August 2022, around 10 million fraudulent calls were made globally via iSpoof, with around 3.5 million of those made in the UK.

iSpoof allowed users, who paid for the service in Bitcoin, to disguise their phone number so it appeared they were calling from banks, tax offices, and other official bodies.

In the UK, more than 100 people have been arrested, the vast majority on suspicion of fraud.

United States

Justice Department announces takedown of nationwide catalytic converter theft ring

Federal, state, and local law enforcement partners from across the United States executed a nationwide takedown of leaders and associates of a national network of thieves, dealers, and processors for their roles in conspiracies involving stolen catalytic converters.

The operation included arrests, searches, and seizures in in nine states across the country. Over 32 search warrants were executed, millions of dollars in assets seized, including homes, bank accounts, cash, and luxury vehicles. In total, 21 individuals in five states have been arrested and/or charged for their roles in the conspiracy.

The US Department of Justice said many stolen converters were sold to DG Auto Parts LLC of Freehold, New Jersey, which allegedly sold precious metal powders it extracted from the devices to a metal refinery for more than US$545 million (NZ$855m).

Amazon packages of garden stones are being used to smuggle meth, Feds say

Amazon is working with Homeland Security Investigations (HSI) to investigate an alleged global narcotics organisation shipping methamphetamine under the guise of decorative stones that are used for gardens and model railways.

Investigators say Amazon and HIS have uncovered at least five vendor accounts using Amazon's international shipping services to move the narcotic across the world. One package that contained 'bulk controlled substances' was intercepted by Customs and Border Protection in Kentucky before it could be shipped to its destination in Australia.

Corruption

Australia announces plan for new corruption watchdog

Prime Minister Anthony Albanese and Attorney General Mark Dreyfus announced a plan to create a National Anti-Corruption Commission, which would have broad jurisdiction to investigate serious corruption in the public sector.

The proposed commission would operate independently from the government, be able to make findings of fact including findings of corruption and have the power to refer findings to federal police or the director of public prosecutions, according to the statement.

Former Government of Bolivia Minister pleads guilty to conspiracy to launder proceeds of bribery scheme

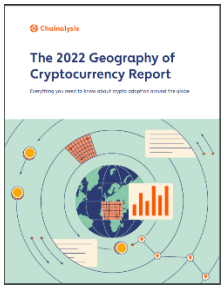
According to a US Department of Justice statement, Arturo Carlos Murillo Prijic, the former minister of the government of Bolivia, pleaded guilty to conspiracy to launder bribes received from a US company for helping them win a US$5.6 million (NZ$8.8m) contract to provide tear gas and other non-lethal equipment to the Bolivian Ministry of Defense.

According to court documents, Prijic received at least US$532k in bribe payments from a Florida-based company then laundered the proceeds of the bribery scheme through the US financial system. Prijic's co-conspirators previously pleaded guilty in September 2021 to their roles in the scheme.

Guatemalan former president and vice president convicted of fraud, conspiracy

A court in Guatemala convicted former President Otto Perez Molina and his vice president, Roxanna Baldetti, on fraud and conspiracy counts. Both resigned in 2015 and have been in custody on charges of permitting and benefiting from a customs graft scheme. The scheme involved a conspiracy to defraud the state by letting businesses evade import duties in exchange for bribes.

Cryptocurrency



Chainalysis: The 2022 Geography of Cryptocurrency Report

Chainalysis has published its third annual guide to cryptocurrency adoption and usage around the world. The report contains research and data on where crypto adoption is increasing most rapidly, the most prevalent use cases by region, and the differences in usage between emerging and developed markets.

SEC charges creator of global crypto Ponzi scheme in connection with $295m fraud

The United States Security and Exchange Commission (SEC) announced charges against four individuals for their roles in Trade Coin Club, a fraudulent crypto Ponzi scheme that raised more than 82,000 Bitcoin, valued at US$295 million (NZ$463m) at the time, from more than 100,000 investors worldwide.

The SEC alleges that Trade Coin Club operated as a Ponzi scheme and that investor withdrawals came entirely from deposits made by investors, not from crypto asset trading activity. The four individuals are alleged to have taken over US$59 million (NZ$93m) worth of the bitcoin invested.

Websites offering crypto payment for child sexual abuse images 'doubling every year'

The Internet Watch Foundation (IWF), a UK-based non-profit that is dedicated to finding and removing images and videos of child sexual abuse material (CSAM) from the internet, has formed a new 'crypto unit' in response to the increasing numbers of CSAM websites accepting virtual currencies. IWF has found the number of websites accepting cryptocurrency payments for sexual content of children has doubled almost every year since 2015.

IWF receives daily requests for information from law enforcement around the world, and thousands of reports are shared daily with hotlines in other countries and law enforcement agencies so that websites can be removed, and distributors can be investigated. The payment information displayed on commercial CSAM websites is also shared with partners in the financial industry.

Wildlife Trafficking

Global Initiative Against Transnational Organised Crime offers new tool to fight wildlife trafficking

The Global Initiative (GI-TOC) and the Alliance to Counter Crime Online (ACCO) collaborated to analyse common characteristics among social media posts advertising exotic pets and illegal wildlife parts to determine if typologies could be developed to assist law enforcement, tech firms, the financial industry and other civil society organisations in detecting wildlife trade offenders online, specifically on social media platforms.

This work led to the development a community tool that provides a sample typology report that is intended to assist institutions and organisations researching and responding to the illegal wildlife trade by giving them a template to report their data in a clear and succinct manner that highlights the most important information for responders.

US Justice Department charges 8 in alleged international monkey smuggling ring

Two Cambodian wildlife officials were among eight people charged with running an international monkey smuggling ring which shipped primates to the US that were poached from the wild and falsely labelled as coming from breeding facilities.

Two top executives at the Hong Kong-based Vanny Resources Holdings primate supply company are accused of working with black market dealers and corrupt wildlife officials in Cambodia to obtain wild-caught macaques and 'launder them' through Cambodian breeding facilities.

Australian Transaction Reports and Analysis Centre (AUSTRAC)

AUSTRAC 2021-22 Annual Report

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money laundering and counter-terrorism financing regulator and financial intelligence unit. AUSTRAC is responsible for detecting, deterring, and disrupting criminal abuse of the Australian financial system to protect the Australian community from serious and organised crime.

The annual performance statements in the 2021-22 Annual Report detail AUSTRAC's progress against the performance measures in AUSTRAC's 2021-25 corporate plan.

Preventing Trade-Based Money Laundering in Australia

This guide provides indicators and behaviours to help financial service providers, particularly those engaged in trade financing, to detect and report suspicious financial activity.

Trade-based money laundering schemes vary in complexity and can be challenging to detect as they can involve multiple parties and jurisdictions and misrepresent the prices, quantity, or quality of imported or exported goods.

Fintel Alliance

Fintel Alliance 2021-22 Annual Report

Fintel Alliance is an AUSTRAC initiative, established in 2017 as a public-private partnership (PPP) to increase the resilience of the financial sector to prevent exploitation by criminals, and support investigations into serious crime and national security matters.

In the 2021-22 year, the Fintel Alliance received two international awards for projects targeting illegal wildlife trafficking and professional money laundering, released 5 financial crime guides and contributed to the arrest of two fugitives.

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

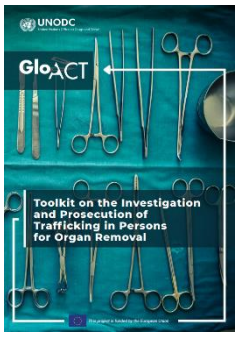
Operational Alert: Laundering of proceeds from illicit cannabis

A recently published Operational Alert, developed to advance and facilitate Project Legion, details a series of indicators developed by FINTRAC following an analysis of suspicious transaction reports (STRs) related to the laundering of proceeds derived from illicit cannabis activities.

Project Legion is a public-private partnership initiative led by Toronto-Dominion Bank (TD), supported by Canadian law enforcement agencies and FINTRAC. It targets illicit cannabis activities by focusing on the money laundering aspect of the crime. The objective of the project is to improve the awareness of the crime and to improve the detection of the laundering of proceeds from illicit cannabis.

UNODC

UNODC launch manual to tackle underreported crime of organ trade

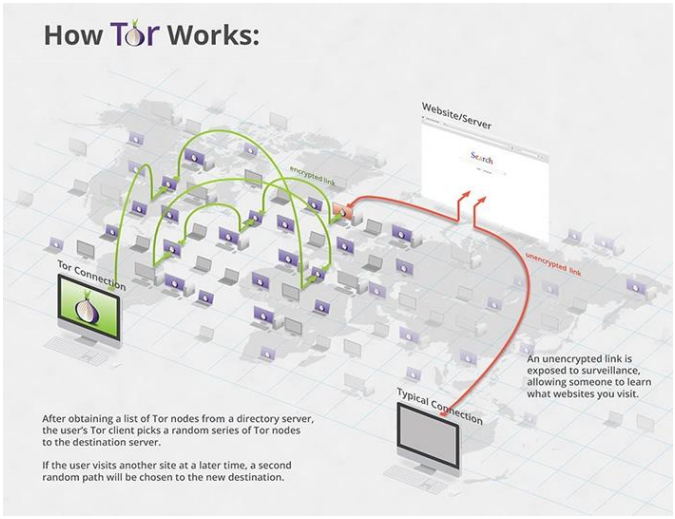


The United Nations office on Drugs and Crime (UNODC) has launched a new toolkit on how to effectively investigate and prosecute the trafficking of people for the purpose of organ removal. The complex network of actors for this crime, paired with this transnational nature and the lack of expertise in identifying and investigating it, makes organ harvesting an exceptionally underreported crime.

The UNODC toolkit features a virtual reality crime scene to better identify and collect evidence from medical surgeries and clinical settings, a victim interview protocol, and an investigation and prosecution manual. The organ trade market is estimated to bring in US$840 million (NZ$1.3bn) to US$1.7 billion (NZ$2.7bn) annually, according to a 2017 Global Financial Integrity report, and according to the UNODC toolkit, has been growing in scope.

Privacy Affairs

Dark Web Price Index 2022



Written for the February 2021 to June 2022 reporting period, this guide provides updates to information published in their previous report as well as insights into some of the most popular products that are for sale on the Dark Web and lists the average price of each product.

Paypal account details, Netflix logins and stolen credit card details are the most widely found information on the Dark Web, and also the least expensive. Overall, the data shows the Dark Web data market grew larger in total volume and product variety since the previous report.

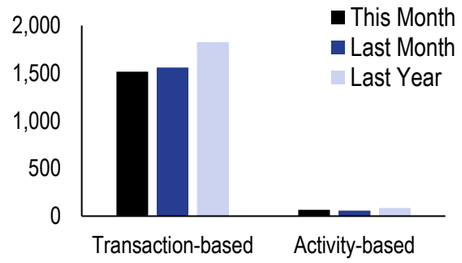
Visual Capitalist provides a basic explanation of the Dark Web, as well as charts the data provided by Privacy Affairs.

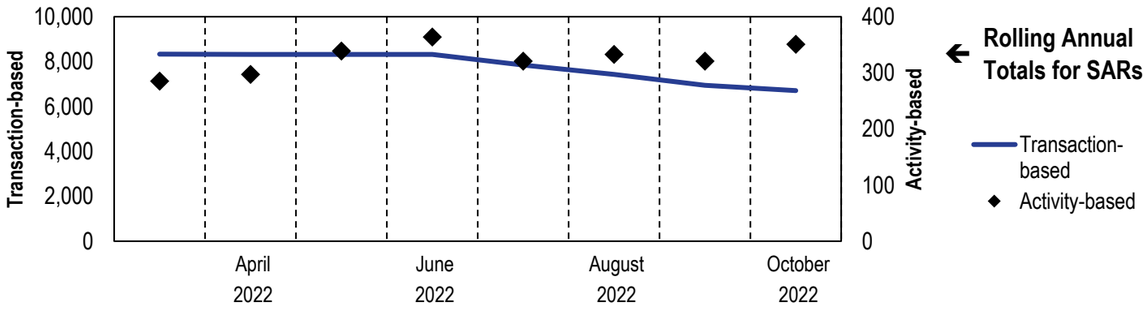
MONTHLY STATISTICS* | NEW ZEALAND POLICE **FINANCIAL INTELLIGENCE UNIT** October | 2022

SUBMITTED REPORTS to the FIU*

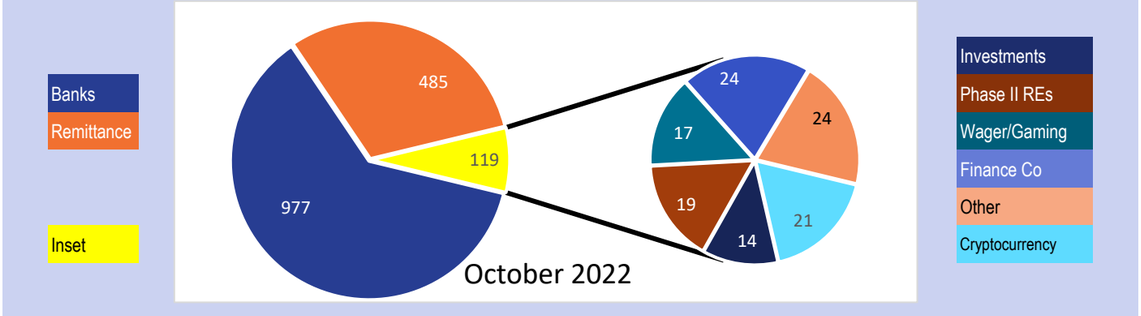
Processed Suspicious Activity Reports (SARs)

	This Month	*Last Month*	*Last Year*
	October 2022	**September 2022**	**October 2021**
Transaction-based	**1,515**	**1,559**	**1,827**
Activity-based	**67**	**59**	**86**
Total	**1,582**	**1,618**	**1,913**



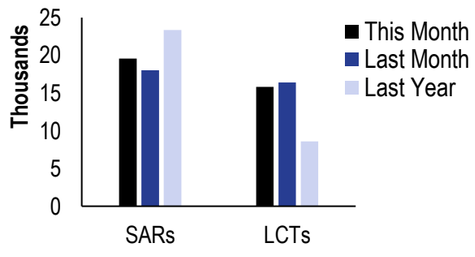


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

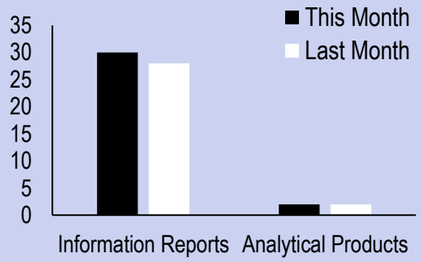
	This Month	*Last Month*	*Last Year*
	October 2022	**September 2022**	**October 2021**
SARs	**19,569**	**18,007**	**23,351**
IFTs	**398,825**	**509,528**	**436,066**
LCTs	**15,802**	**16,401**	**8,583**



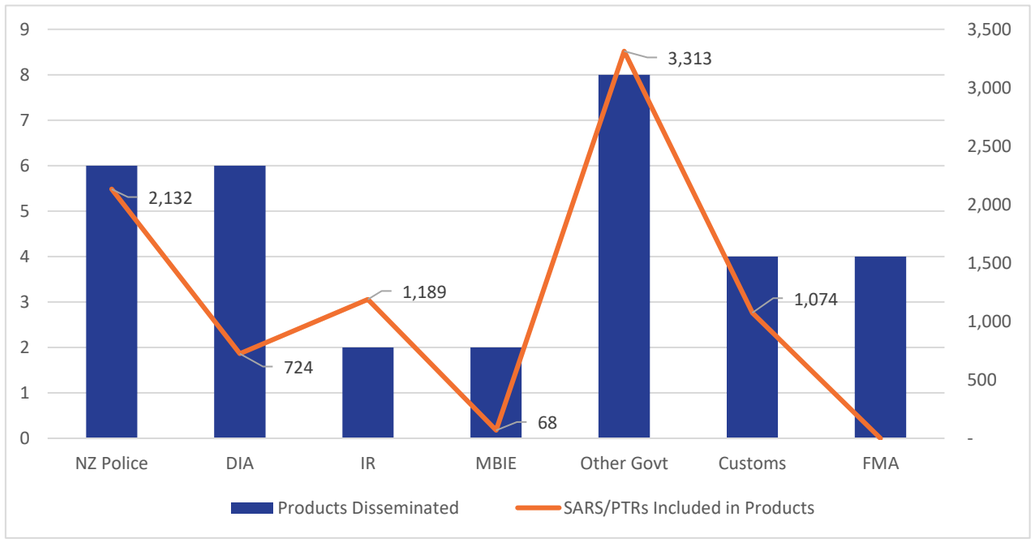
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

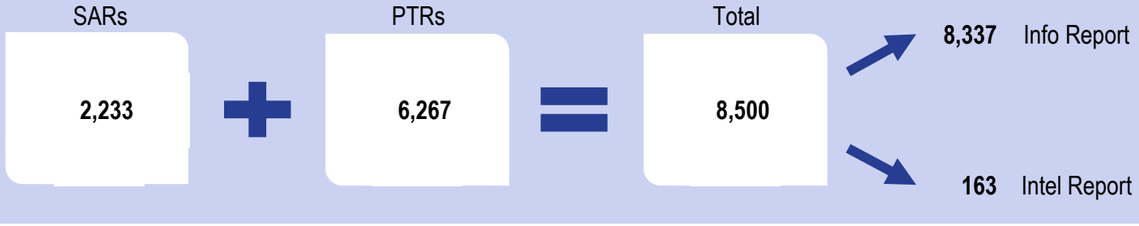
	This Month	*Last Month*
	October 2022	**September 2022**
Information Reports	**30**	**28**
Analytical Products	**2**	**2**
Total Products	**32**	**30**



Disseminations of Products by Recipient



Disseminations of Products by Included SARs and PTRs



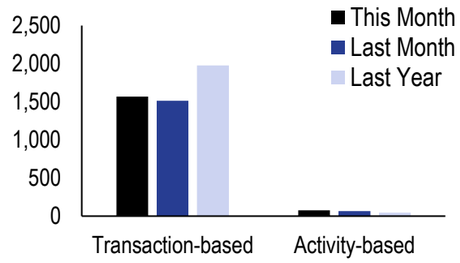
*Statistical data for transaction reporting and intelligence products may be updated as new information is processed, and so there may be minor discrepancies between the statistical figures contained in this report and subsequent reports.

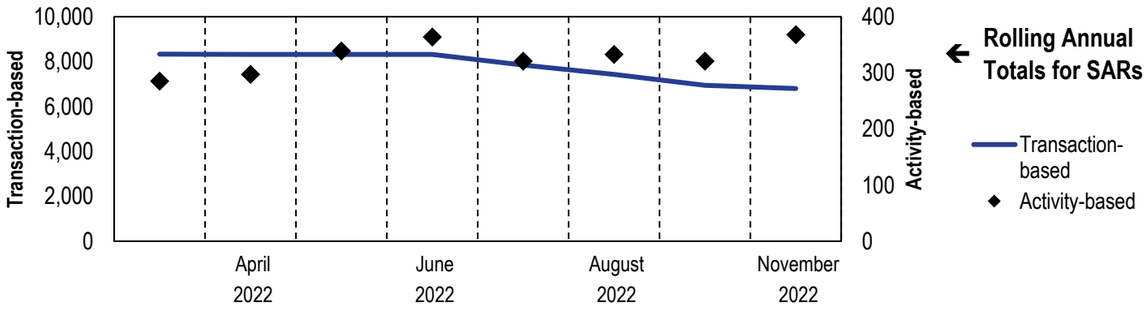
MONTHLY STATISTICS* | NEW ZEALAND POLICE **FINANCIAL INTELLIGENCE UNIT** November | 2022

SUBMITTED REPORTS to the FIU*

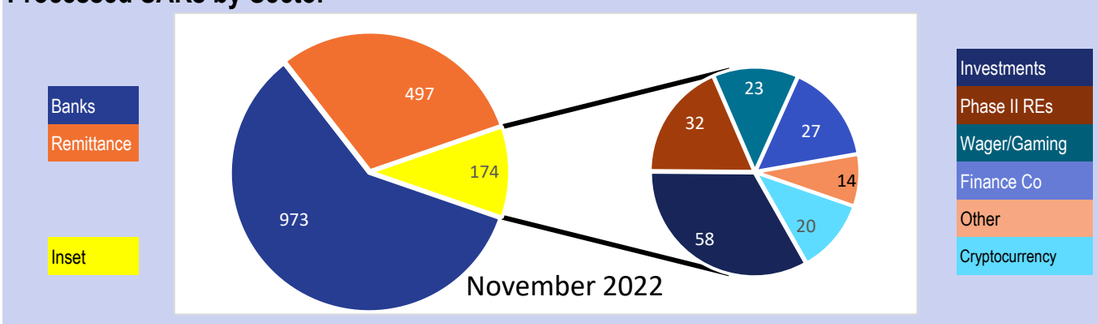
Processed Suspicious Activity Reports (SARs)

	This Month	*Last Month*	*Last Year*
	November 2022	**October 2022**	**November 2021**
Transaction-based	**1,568**	**1,515**	**1,978**
Activity-based	**77**	**67**	**46**
Total	**1,645**	**1,582**	**2,024**



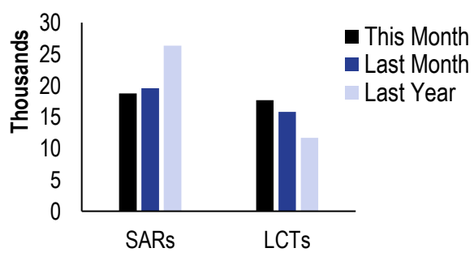


Processed SARs by Sector



Transaction Volumes within SARs and PTRs

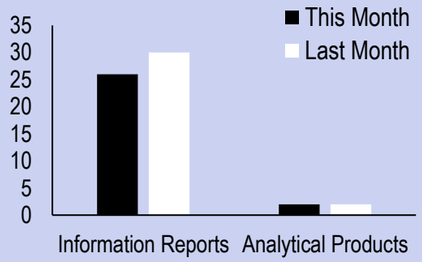
	This Month	*Last Month*	*Last Year*
	November 2022	**October 2022**	**November 2021**
SARs	**18,720**	**19,569**	**26,326**
IFTs	**438,486**	**482,188**	**454,964**
LCTs	**17,680**	**15,802**	**11,693**



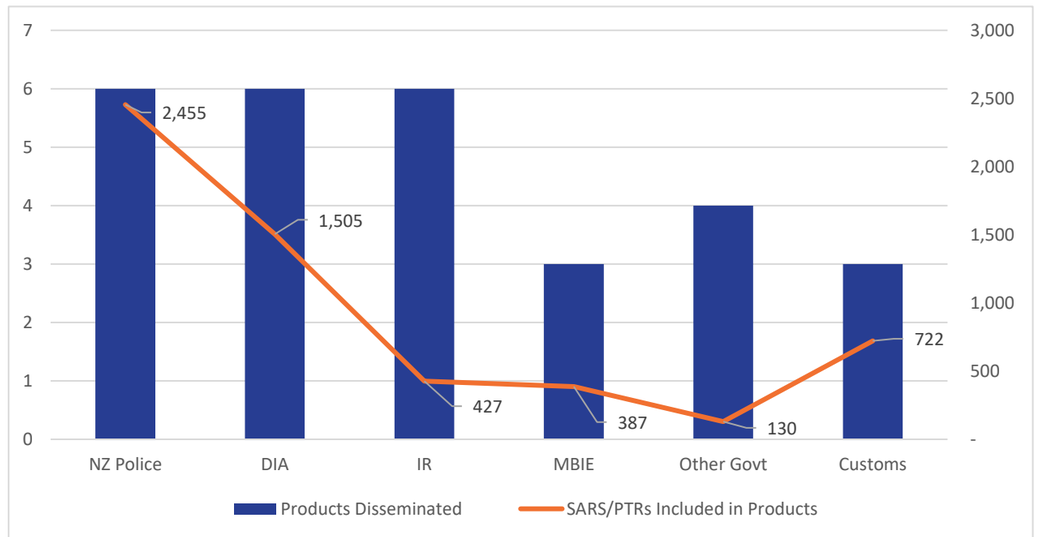
FINANCIAL INTELLIGENCE PRODUCTS

Disseminations of Products by Type

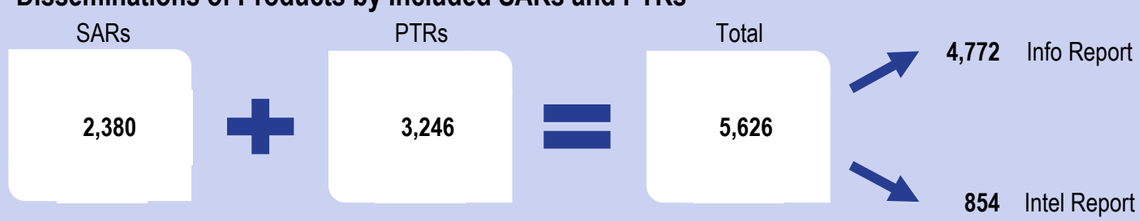
	This Month	*Last Month*
	November 2022	**October 2022**
Information Reports	**26**	**30**
Analytical Products	**2**	**2**
Total Products	**28**	**32**



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.

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

@NZFIU

www.police.govt.nz