FINANCIAL CRIME
PREVENTION NETWORK

Threat assessment

Transnational Organised Crime
Financial Sector Vulnerabilities

February 2024

Contents

About FCPN

The Financial Crime Prevention Network (FCPN) is a Public Private Partnership (PPP) created in 2017 to enhance knowledge sharing and collaboration between law enforcement agencies and the financial sector.

Our purpose is to protect New Zealand against financial crime by working together to create and share intelligence, disrupt financial crime, and increase the nation's resilience against the threat of financial crime.

Chaired by the New Zealand Police Financial Crime Group, the FCPN is currently made up of Police specialists, New Zealand Customs, and the five major banks: ANZ, ASB, BNZ, Kiwibank, and Westpac.

FCPN members are committed to building and growing an effective network of dedicated intelligence resources to enhance financial crime detection and prevention capability, inform decision making and assist efforts to combat crime and victimisation in New Zealand and on a global scale.

About FCPN Threat Assessments

FCPN Threat Assessments are developed from the knowledge shared between FCPN members. They are designed for reporting entities and are publicly available.

The assessments include case studies, indicators, and learnings from operations FCPN members have been involved with. The assessment aim to assist in the detection of financial crime and identify disruption opportunities.

Acknowledgements

The FCPN acknowledges the contribution of our members and partners who contributed to this threat assessment.

Thank you to the Fintel Alliance for their support in the development of this product.

Publication & Copyright

The FCPN owns all material produced in this threat assessment.

Published February 2024.

About this Threat Assessment:

Transnational Organised Crime Financial Sector Vulnerabilities

This assessment has used NZ Police operations as case studies and considered the financial system vulnerabilities that were exploited by Transnational Organised Crime (TNOC) groups, focusing on:

- Cash placement
- Drug-related offending

It is most useful to New Zealand financial institutions, who may benefit from FCPN learnings. This information may help financial institutions identify and deter financial crime or identify activity to be submitted to the FIU as a Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR).

Introduction & Purpose

Money laundering generates approximately $1.35 billion in New Zealand each year, mainly from transnational organised crime (TNOC) linked to illicit drug activities. Cash from illicit proceeds is placed into the legitimate financial system so it can be moved or used in the economy. Greater understanding is needed of the specific financial system vulnerabilities being exploited for TNOC networks.

The purpose of this assessment is to assess financial sector vulnerabilities in relation to the money laundering risk posed by TNOC groups in New Zealand – drawing on Operation Brookings, Ida, and Martinez as case studies – and to identify potential change, disruption, and prevention opportunities. It will examine high-risk typologies and channels being used to launder TNOC proceeds through New Zealand's financial system, with a primary focus on cash placement. While banks and law enforcement agencies adjust their response to disrupt identified illicit activity, money launderers continue to search for vulnerabilities of banks and other financial institutions.

This assessment aims to raise awareness and assist reporting entities in the detection of financial crime and identify disruption opportunities. Behavioural and financial indicators are identified to assist in tackling the infiltration of TNOC into New Zealand's legal economy.

This assessment will focus on the laundering of illicit proceeds from drug-related crimes, however other crime types as set out below were incorporated in the vulnerabilities assessment. These other types were determined by the *Transnational Organised Crime in New Zealand: Our Strategy 2020-2025*[1] and include:

- Human trafficking
- Fraud
- Tax evasion
- Illegal, unreported, and unregulated (IUU) fishing
- Illegal wildlife trafficking.

[1] https://www.police.govt.nz/sites/default/files/publications/transnational-organised-crime-in-new-zealand-our-strategy-2020-to-2025.pdf

Background

TNOC is defined as systematic illegal activity for power or profit coordinated across borders.[2] For illicit proceeds to be available to organised crime syndicates, they need to be placed into the formal financial system and converted into readily accessible assets; allowing the transfer of value to facilitate business. In many instances, this involves the corruption or coercion of individuals within key industries as 'facilitators' who assist TNOC groups with laundering illicit proceeds.

TNOC groups instigate harm to society through physical, wellbeing, and community impact; harm to the economy through tax, income, business, and government impact; and harm to New Zealand's global reputation.[3] As money laundering is one of the key enablers of TNOC, the financial sector plays a crucial role in preventing, disrupting, detecting, and reporting the movement of TNOC proceeds.

The Global Illicit Economy

The 2021 report produced by the *Global Initiative Against Transnational Organized Crime (GI-TOC)*[4] states that despite international efforts to combat transnational organised crime, TNOC transformed beyond recognition and has grown exponentially since the 1990s. *Figure 1* and *2*, from the same GI-TOC report, show the increase in human exploitation and drug market evolutions from 2000 to 2020. Although rapidly emerging modern technologies have the potential to make money laundering faster, cheaper, and more effective, the traditional typologies are still widely used, particularly the involvement of shell companies, cash intensive businesses, real estate, high value dealers, and overseas investments.

The criminal economy takes advantage of the banking secrecy that can be afforded by some offshore jurisdictions. The use of both tax havens and cryptocurrencies to obscure fund movements allows criminals to hide their money. This has created enormous wealth for criminal groups.

New Zealand Context

According to the 2019 *National Risk Assessment (NRA)* published by the NZ Financial Intelligence Unit (FIU), money laundering generates approximately $1.35 billion domestically every year. The largest proportion of this relates to transnational organised crime linked to illicit drug activities. As New Zealand's financial system is dominated by the banking sector, this places the banks at the highest money laundering risk.

To be laundered, illicit funds must be placed within the financial system before being moved internationally or integrated into the legitimate economy. While there is a broad understanding of the processes by which this occurs, greater understanding is needed of the specific financial system vulnerabilities being exploited for TNOC networks.

---

[2] https://www.police.govt.nz/sites/default/files/publications/transnational-organised-crime-in-new-zealand-our-strategy-2020-to-2025.pdf

[3] Ibid.

[4] https://globalinitiative.net/wp-content/uploads/2021/03/The-Global-Illicit-Economy-GITOC-Low.pdf

TNOC in New Zealand

Illicit Drug Crime

New Zealand has a lucrative market for illicit drugs, especially methamphetamine, which is increasingly targeted by transnational criminal groups. According to national assessments our rate of drug consumption is much higher than most other countries,[5] and drug trafficking is considered to be the primary generator of illicit cash in New Zealand. This market has seen a shift from domestic methamphetamine production to the importation of finished products and is now largely controlled by TNOC groups within offshore networks.

A recent assessment on cash activity conducted by the FIU identified that four distinct criminal networks[6] collectively deposited at least $107 million in cash – derived principally from drug offending – to the banking system between 2018-2021. The report highlighted in-branch, ATM and drop-box deposits to be the placement methods used, however the vast majority (96%) of the $107 million was deposited in-branch.

$107 million

was collectively deposited by four distinct criminal groups, mainly from drug offending, between 2018-2021

[5] Ibid, 9.

Situation

At a fundamental level TNOC groups need to be able move and access illicit proceeds to function effectively. Profit is the primary motivation behind TNOC activity and money laundering is a key enabling element of TNOC. It is therefore almost certain that TNOC groups will continuously be looking to make their illicit proceeds appear legitimate by identifying and exploiting vulnerabilities within New Zealand's legitimate financial system.

To protect the integrity of the financial system and mitigate the risks of money laundering and terrorism financing, New Zealand has an Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime in place. The AML/CFT Act is the cornerstone of the regime. An assessment of New Zealand's financial system in terms of compliance effectiveness is periodically conducted. The latest evaluation[7] by the Financial Action Task Force (FATF), which assesses the New Zealand AML/CFT regime, identified key vulnerabilities:

- Cash transactions and the banks' vulnerabilities to the placement of cash
  - Cash and cash deposits are primary vehicles for drug proceeds to be laundered
  - Cash is anonymous, forms no formal paper trail, exists outside of formal financial institutions, and doesn't require recordkeeping
- Professional facilitators and remittance services
  - Police investigations routinely involve professional facilitators, including complicit involvement
  - Layering by professional facilitators ultimately may not appear out of the ordinary, making detection of money laundering more difficult
- New Zealand's legal structures and arrangements
  - Relative ease in setting up a company and perceived credibility of New Zealand companies and legal arrangements exposes them to exploitation risk
  - Can be utilised to convert cash proceeds of crime into other assets which are less suspicious

At its heart, the AML/CFT regime is about collaboration and partnerships to help keep New Zealand communities free from harm. The Financial Crime Prevention Network (FCPN) is an important part of this vision. It facilitates collaboration between public and private sectors to enhance information sharing and develop a shared understanding of the risks. Barriers caused by legaland regulatory limits to information sharing are currently being reviewed.

[6] Identified through Operations Brookings, Martinez, Ida, and Worthington.

[7] https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-new-zealand-2021.html

Financial Sector Assessment

Under the auspices of the FCPN, the FIU worked with three FCPN member banks who reviewed the behaviour exhibited by the groups and individuals involved in the investigations Ida, Martinez, and Brookings between 2015 and 2021. The key findings identified are set out below.

Cash Placement

Banking facilities and services are exploited by criminal groups to place illicit proceeds. Criminals also exploit the shortcomings of various systems in New Zealand, such as the ease of the company registration process, identity document issuance, and Money or Value Transfer Services (MVTS) licensing. These enable criminals to establish businesses for either commingling funds,[8] or the sole purpose of money laundering. The following methodologies were identified from the case studies:

- Extensive use of third-party depositors (smurfs)
- Use of mule accounts
- Use of ATMs to avoid face to face interaction with bank staff
- Structured cash deposits made under reporting thresholds including multiple deposits made the on same day, to the same account, at different branches
- Use of multiple IDs, obtained by officially changing names
- Use of fake IDs to open bank accounts
- Registering front or shell companies on the New Zealand Companies Register
- Opening business accounts for the front companies with multiple IDs
- Not declaring the true purpose when opening accounts
- Not declaring the expected high volume of cash activity, and who the depositors will be when opening accounts
- Opening personal accounts on a limited visa that are then used by third parties after leaving the country
- Falsely declaring income from China at the time of opening account
- Use of family members' personal accounts for money laundering operations.

Vulnerabilities

Insights from agencies such as FATF and those gleaned from New Zealand's NRA and money laundering investigations point to specific areas where financial systems can be vulnerable to TNOC groups. This includes cash placement, remittance, virtual currency, trust and entity formation procedures, and overseas investment.

Cash Placement

In recent years, criminal prosecutions have highlighted that domestic TNOC actors have been able to place their illicit proceeds into the financial system. Cash placement is a key technique used by criminal groups and is a considerable issue in New Zealand. Professional Money Launderers (PMLs) have been able to do this on the actors' behalf and have 'professionalised' the operations for them.

Recent investigations highlighted the following cash placement methodologies:

- the use of third party and mule accounts
- third-party cash deposits made both in-branch and via ATMs by mules
- shell companies
- multiple aliases and false identity documents.

[8] Commingling is the act of combining proceeds of crime with business money to obscure the source of funds.

FCPN Member Bank One

FCPN Member Bank One (Bank One) provided information relating to all cash activity. Figures provided by Bank One indicate that ATM cash deposit facilities are the primary channel used to make cash deposits valued under $10K. Cash deposits over $10K cannot be made via ATMs, therefore in-branch is the sole method used.

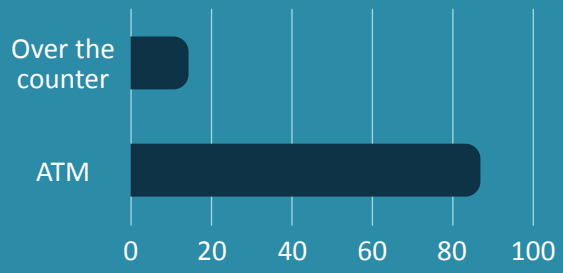
Behavioural information provided by Bank One, based on an assessment of SARs they had submitted which were ultimately linked to Operations Brookings, Ida, and/or Martinez found:

- **Deposits were made late in the day.** Offenders would often arrive late in the day when depositing large amounts in-branch. The bank believes the offenders did this to avoid further questioning by staff who were keen to finish for the day. This practice ceased when the bank stopped accepting large deposits made late in the day because it was also seen as a physical security issue.
- **Cash deposits contained small bills.** Offenders mainly deposited $20 bills. When the offenders were asked why they banked so many notes in that denomination, they said their money exchanger offered better rates if they took such notes instead of larger bills when exchanging foreign funds.
- **Common transaction references.** The transaction references used by offenders were often obvious, such as the initials of the PML or one of their companies. For example, the following were observed relating to Operations Ida and Martinez: QDD (Quan Duo Duo), LD (Li Dong), AA (Winner Group's director's initials), WD (WD Global), and Quicksale.

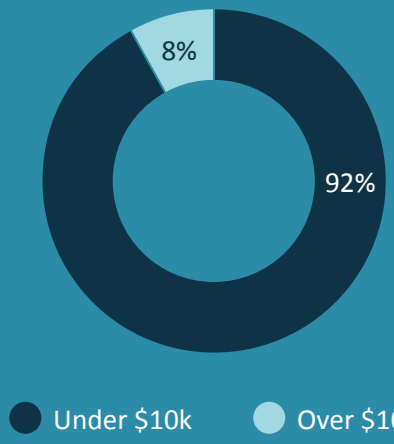
The bank's assessment also found that PMLs have evolved over about five years from having a smaller number of people depositing large amounts, to having dozens of smurfs depositing cash mostly via ATM in small value and high velocity transactions. The smurfs tend to onboard remotely, use very basic products and attract less scrutiny, especially when such small value transactions are involved. International wire transfers were seldom seen, and it was assessed by the bank that the international component involved informal value transfer systems such as Daigou.[9]

Cash Deposit Method – under $10k

Cash deposit activity over a 12-month period (2021) provided by Bank One identified that 92% of cash deposits made were valued under $10K. 86% of these were via ATM cash deposit facilities. The remaining 14% was conducted via over-the-counter channels.



Channels used for cash deposit activity under $10k for Bank One in 2021



Overall cash deposit activity for transaction amounts at Bank One in 2021

Cash Deposit Method – over $10k

Cash deposits exceeding $10K can only be made in-branch and over-the-counter. Overall, over-the-counter deposits account for 21% of total cash deposits by volume.

[9] A form of informal value transfer often used in the China context to evade foreign currency restrictions and/or import duties.

When Bank One detects smurfing behaviour (e.g., a newly opened account that only deposits and withdraws cash) and they attempt to contact the customer, the customer rarely calls back and often clears the account before abandoning it. Ideally banks would like to find methods to more quickly deal with or deter smurfing. Additionally, banks need to consider vulnerable customers[10] and avoid de-banking such customers.

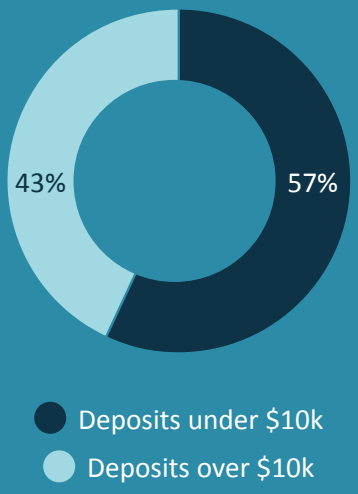
FCPN Member Bank Two

FCPN Member Bank Two (Bank Two) conducted an assessment on suspicious transactions related to cash deposits between 2017 and 2021 and found:

- Personal accounts remain the most common form of cash placement into the financial system.
- The wholesale, retail, and finance sectors have ongoing money laundering risks. The construction sector also had a growing amount of unusual or suspicious behaviour being detected.
- Auckland saw the highest proportion of suspicious ATM deposit activity (for first-party deposits), broadly consistent with the spread of NZ's population, followed by Hamilton, Christchurch, and Hastings.
- Third-party cash deposits account for 22% of all suspicious cash activity.
- Suspicious in-branch cash activity accounted for 86% of all suspicious cash deposits; during the period looked at, in-branch banking was more accessible than ATMs for Bank Two. Auckland also featured as the top location for suspicious cash deposits made in-branch.
- Criminal abuse of smart ATMs is a growing risk for the structured placement of suspicious cash. In Auckland alone, suspicious cash activity occurring via ATMs has almost doubled year-on-year over a two-year period.[11] The increase in ATM usage may also relate to Covid conditions where branch closures created an inability to deposit cash in-branch.

Suspicious Cash Deposit Transactions

Over the five-year period (2017-2021):



Around 93% of all suspicious deposits involved personal accounts, with only 5% occurring in business accounts. Business accounts classified (by ANZSIC code)

E – Constructions,
F – Wholesale Trade,
K – Financial and Insurance Services,
O – Other Services, and industry unspecified featured the most.

- Suspicious cash activity was concentrated around a trade and business hub in Auckland. Wholesale trade and finance service industries, particularly grocery wholesalers that offer Pacific remittance, were also a key area of growing concern.
- Hawala-type informal money remittance is being used in the Pacific as an alternative to traditional international bank-to-bank transfers, and third-party cash deposits among these customers have increased in line with this method.

[10] "A vulnerable consumer is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care" – https://www.fma.govt.nz/assets/Reports/CustomerVulnerability-ourexpectationsforproviders.pdf

FCPN Member Bank Three

A third FCPN Member Bank (Bank Three) made the following observations related to suspicious cash placement between 2018 and 2021 when the four criminal groups[12] were operating:

- The PML groups were operating in the remittance sector and had both criminal and non-criminal clients. When cash deposits to a bank account triggered enhanced customer due diligence (ECDD), the bank client (who was also the remittance companies' client) was often able to explain, and evidence, that they were moving funds from offshore through a remittance company to their New Zealand bank account. They were not expecting cash specifically but were expecting funds to be deposited and were able to provide evidence of their offshore wealth and the engagement they had with the remittance company.
- This suggests the PML group had little need to initiate international payments to move illicit funds out of New Zealand. The PML could make use of an offsetting arrangement to accept illicit cash in New Zealand and offset it against the funds received offshore from their non-criminal clients.
- This operating model meant that while activity was being identified and reported in SARs, generally the suspicion did not fall on the bank customer who was the recipient of the cash, rather the third-party depositor and the source of cash in their possession.
- Initially large one-off cash deposits were the primary placement method. These were conducted by just a handful of third-party depositors. As these transactions exceeded the occasional transaction threshold, customer due diligence (CDD) was obtained at the time of the deposit. The depositors made no attempt to hide their identity.
- The bank implemented process and control changes to disrupt the large cash deposit activity, which included training and awareness and adjusting thresholds as a result of the activity observed. This displaced the cash placement and resulted in a shift by depositors to use drop-boxes[13] and structuring. The deposits were structured by splitting deposits into a series of smaller transactions (less than $10K), enabling the recipient to still receive a large amount of money.
- In response the bank made additional process and control changes and removed the ability for drop-boxes to be used by third parties and removed the ability for deposits to be made to personal customers' accounts through drop-boxes.
- The bank observed that as the control environment changed the cash depositors were quick to adjust their methods, such as movement to over-the-counter deposits when drop boxes were restricted.

Remittance

The alternative money transfer system has varying degrees of contact with the formal banking system. As found in the case studies, the remittance sector is highly exploitable by PMLs which poses substantial risk for the banking sector. The case studies revealed that cash is being deposited on a large scale directly to remitters, and then sent on to offshore accounts.

The cost of compliance for smaller remitters is high and they are likely to continue conducting their business without registration. Furthermore, it can be difficult for AML regulators and other more well-established financial institutions to differentiate between legitimate and criminally motivated remitters/businesses due to the business structure. For example, a dairy may offer remittance services as a secondary, undetected business.

The following typologies were identified from case studies where PMLs operated or used the services of a remittance business:

- **Use of registered remittance business for placement, and movement of funds offshore.** The money transfer business was registered which made it appear legitimate but based on observations by the DIA, the entity was immensely underreporting SARs and Prescribed Transaction Reports (PTRs). Investigations also revealed that other PMLs were using this remittance business for placement and movement of funds to offshore.

[12] From Operations Brookings, Ida, Martinez, and Worthington.

[13] A bank drop-box is a deposit point at many banks where certain customers can use special envelopes or bags to deposit cash. Deposit bags and envelopes have been phased out or are now restricted at many New Zealand banks.

- **High volumes of cash deposits made by third parties (mules).** These individuals claimed they were employed by the remittance business when questioned by the banks.
- **Use of shell companies.** These were used for cash placement and outgoing electronic transfers. Often the industry classification did not match the account activity. The directors were either associates, including a foreign national who only spent three months in the country just to open business accounts, or the PMLs themselves who owned multiple, valid identity documents.
- **Strong links with the funds' destination country – in these cases China.** The money launderers were Chinese nationals. They sent funds to their holdings in China or received funds from China.
- **Commingling.** Illicit proceeds were placed within the legitimate remittance business, making it difficult to separate these activities.
- **Cash deposit to remittance business operated by a PML.** The remittance business operated by Op Ida's PML was also used by Op Martinez and Brookings' money laundering networks. Covert surveillance revealed links between these networks when they organised cash drops.
- **Unregistered remitters.** A PML was operating front companies registered as tour arranging, tourism development consultancies, or wholesale trade businesses. FIU analysis indicates this group offered a combination of international remittance, foreign exchange, and tourism-related services to largely Chinese clientele. It was also identified that high value payments originating from this network were destined for investment in New Zealand real estate, indicating the PML also offered opportunities for investment in New Zealand real estate.
- **Shift from business accounts to personal and mule accounts.** After closing business accounts (tourism related businesses), activity continued from personal accounts and mule accounts which were used to deposit large amounts of cash and move money from China to New Zealand.
- **Use of multiple identity documents, aliases, and false names when opening bank accounts.** Staff in banks and other financial institutions are not expert document examiners so it can be difficult for them to identify if a fraudulent document has been submitted as proof of identity.

Vulnerabilities

Remittance

Another area that is extensively being exploited is remittance services. This is not a new phenomenon. The sector has been identified in previous NRAs[14] and FATF mutual evaluations[15] as an area of risk. It is likely that TNOC groups will continue to target the remittance sector in New Zealand as transnational criminal activities increase. As mentioned previously, New Zealand's drug market is increasingly being targeted by offshore criminal networks, which in turn increases the demand to move profit offshore.

The remittance sector is a regulated area and has AML/CFT compliance obligations and effective controls in place. However, there are some key shortcomings in the compliance framework such as:

- No specific requirement for agents to be licenced
- Remittance businesses are not required to maintain a current list of their agents that is accessible by authorities.

MVTS providers are not required to include their agents in their AML/CFT compliance programme or monitor their agents' compliance with their programme, making the remittance sector a target for TNOC actors.

The latest FATF evaluation also highlighted the minimal effort taken to identify unregistered MVTS providers and rated this sector as partially compliant. As the remittance sector has a varying degree of contact with the formal banking system, inadequate compliance poses considerable risk to the banking sector.

[14] https://www.police.govt.nz/about-us/publication/national-risk-assessment-nra
[15] https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-new-zealand-2021.html

Virtual Currency

Cryptocurrency can be used as a tool for layering illicit proceeds through regular cryptocurrency deals, as well as through peer-to-peer trades which do not go through a VASP platform.

VASPs are reporting entities and regulated in New Zealand by the AML/CFT Act, however, some gaps identified by FATF exist in the understanding and the implementation of the AML/CFT Act obligations, and the level of Suspicious Transaction Reporting by VASPs remains low.

New Zealand currently does not have crypto ATMs which would enable the cash sale and purchase of crypto currency. It is likely that the purchase of virtual currency by cash will be facilitated by peer-to-peer networks and crypto brokers.

Peer-to-peer virtual currency trading can pose high risks to the banking system as the activity is often disguised, it is not declared what the account is intended to be used for, and this is not indicated in the transaction reference.

Illicit crypto wallets may be identified when multiple customers send funds to the same external wallet address (that is not a service).[16]

Crypto activity was identified in the case studies. Bitcoin was advertised for sale on an online public platform, localbitcoins.com, and transactions were completed using the following methods:

- PML obtained large amount of cash during clandestine meetings (criminal proceeds). Cash would then be sent via a New Zealand bank account, to the PML's Chinese holding company and then through remitters to a Chinese bank account, where the PML would buy Bitcoin. It is likely that Bitcoin transactions took place instantly when the cash was handed over.
- Bitcoin is sold on the online public platform, PML provides payment instructions for funds to be sent to his New Zealand bank account held under his name, or in his associates' name.
- PML would instruct customer to use references such as 'app', 'usana', 'web', 'book', to hide Bitcoin activities; however, occasionally people did not follow the PML's instructions and used references such as 'bitcoin' or 'btc'.
- Small crypto asset purchases were made to obscure the layering process.

It is likely that PML customers (criminal groups) receive crypto for cash. Cryptocurrency could be used to make dark web purchases or be cashed out through a registered crypto platform. Cryptocurrency dealing is often visible to the banks because it usually involves, for example, a customer conducting a lot of transactional activity with third parties followed by a large transaction with a registered cryptocurrency dealer.

As the crypto service was advertised on a public platform, it is possible that legitimate crypto purchases were commingled with illicit cash.

Vulnerabilities

Virtual Currency

Criminal actors are expanding their money laundering methods with the use of cryptocurrency. The growing use of virtual assets to facilitate anonymous financial transactions is increasingly observed in New Zealand and international criminal investigations. The anonymous, cross-border nature of crypto coupled with gaps in regulatory settings create significant gaps in our understanding of the scale and nature of crypto-enabled money laundering.

Virtual Asset Service Providers (VASPs) also intersect with the formal banking system; therefore, insufficient compliance, unlicenced agents, and unregistered service providers pose a high risk to the banks.

[16] https://www.austrac.gov.au/sites/default/files/2022-04/AUSTRAC_FCG_PreventingCriminalAbuseOfDigitalCurrencies_FINAL.pdf

Trust and Entity Formation Procedures

New Zealand government agencies currently have no obligation to obtain, verify, and maintain adequate, accurate and current information of beneficial ownership and control of New Zealand trusts. Registration requirements only extend to foreign and charity trusts.

In addition to personal accounts, the money laundering networks in the case studies typically used multiple shell companies and trusts accounts to place and layer their illicit proceeds. The following methods were observed:

- Front companies were established as legitimate businesses to conceal the illegal activities of the entity controlling it. The companies had no classification or were often disguised as online retailing or building and construction companies. The companies were typically used for the placement of cash. Although declaring an industry classification is not a legal requirement, it assists the bank to understand whether the account activity is normal for the business, particularly when a business that is not known to the bank interacts with their customer.
- The use of trustee companies to conceal high-value property ownership was observed, as was the use of a family trust account to launder proceeds. Account activity showed funds being layered and included frequent high-value transfers, funds received from third parties, entities, and individuals, and funds sent to individuals not linked to the trust.
- The transfer of shareholdings to individuals in China, while the director is a New Zealand resident, was also observed. In New Zealand non-resident shareholders and directors are permitted, however a company is required to have a least one New Zealand director who lives in New Zealand or Australia (who is a director of a company incorporated in Australia). Numerous companies used by the network also had registered shareholders in Australia, which were both entities and individuals.

Vulnerabilities

Trust and Entity Formation Procedures

The criminal misuse of entities and limited companies are an international problem. New Zealand entity formation processes are exploited by TNOC actors, through the creation of shell companies and the abuse of trust structures. The Panama Papers leak in 2016 revealed the involvement of New Zealand companies[17] and foreign trusts in facilitating international tax evasion and money laundering schemes.

In addition, trusts are known to be highly vulnerable to criminal misuse in New Zealand. They commonly feature in money laundering cases domestically and can be used to obscure beneficial ownership. New Zealand was rated only partially compliant in the 2021 FATF evaluation with the requirement of transparency and beneficial ownership of legal arrangements due to there being no obligation to obtain, verify, and retain adequate, accurate and current information of beneficial ownership and control of trusts by government. In New Zealand, registry requirements only apply to foreign and charitable trusts.

[17] https://www.reuters.com/article/us-panama-tax-newzealand-idUSKCN0Y000W

Overseas Investments

Police have identified occurrences of significant funds derived from criminal offending overseas being invested in New Zealand's financial and property markets. Several occurrences involving the investment of illicit funds from offshore in New Zealand industries were also reported in the media.

While New Zealand is eager to have higher levels of investment from individuals based overseas, it is crucial that adequate checks and balances are in place to determine the source and legitimacy of the funds being invested.

Discussion with OIO revealed that in some instances investors did not have adequate information of source of funds and OIO recommended declining the investment application. However, the investors were able to secure high value loans within the financial sector. Case studies also revealed attempts to launder illicit funds from overseas through investment schemes. Although the case studies could not establish links between offshore investments and drug related offences, it is likely that transnational criminal groups involved in drug trafficking are exploiting such systems.

Vulnerabilities

Overseas Investments

FIU have received numerous requests from overseas partners where a money laundering link to New Zealand was identified and involved offshore illicit proceeds moving through New Zealand bank accounts. Property and investments are also vulnerable to TNOC actors where they may have domestic links.

While the exact value of the illicit proceeds is not known, the value of transnational money laundering in New Zealand is likely to exceed NZD $1 billion annually.[18]

[18] https://www.police.govt.nz/sites/default/files/publications/fiu-nra-2019.pdf

Conclusion

TNOC continues to be an evolving challenge generating millions in money laundering each year. As set out in the *Transnational Organised Crime in New Zealand: Our Strategy 2020–2025*,[19] New Zealand's law enforcement and regulatory bodies can have the greatest impact on combatting TNOC through three strategic areas: Unify, Prevent and Detect, and Dismantle. The strategic cross-agency approach as set out under 'Unify' can be strengthened with a cross-organisation approach for banks to increase capability to 'Prevent and Detect', and ultimately contribute towards the third strategic focus, 'Dismantle'.

Indicators

- Name changes across multiple identity documents.
- Inconsistencies across multiple identity documents (i.e., look for customers' name, date of birth, place of birth, ID photo, issue date).
- A customer on a short-term visitors' visa or student visa continues to make use of a local bank account beyond their departure date for high value or low-value-high-volume activity. For instance, a payment for a deposit or purchase of a property may be unusual activity for a customer who is in NZ for a limited period on a student visa.
- A short-term visitors' account being used by a third party.
- Shifts in activity when a remitters' business account is closed, such as an increase to a personal account or mule accounts.
- Unusual activity on a personal or business account when another person has been authorised onto that account.
- Common transaction references that may relate to a PML or one of their companies.
- Shifts from fewer people/large amounts to more people/smaller amounts in higher frequencies.
- Large deposits being made late in the day.
- Large deposits using small bills.
- Structured deposits occurring where CDD had previously been completed for a large deposit.

Opportunities

- Examine potential displacement of money laundering behaviour when specific prevention initiatives are introduced. Risk assessments should be updated as part of these changes. Financial institutions should consider any potential shifts they might expect to see and how they may be able to respond to them.
- More importance could be placed by financial institutions on their risk assessments at the on-boarding stage of a potential money remitter wanting to open a new bank account.
- Consider methods to more quickly deal with or deter smurfing behaviour, while being mindful of vulnerable people to avoid de-banking such customers.
- Consider verifying IDs for customers when registering both online and in-branch.

[19] https://www.police.govt.nz/sites/default/files/publications/transnational-organised-crime-in-new-zealand-our-strategy-2020-to-2025.pdf

Glossary

Acronyms

AML/CFT, AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism, also references the Anti-Money Laundering and Countering Financing of Terrorism Act 2009
ARU	Asset Recovery Unit (NZ Police)
FCPN	Financial Crime Prevention Network
FIU	Financial Intelligence Unit (NZ Police)
GI-TOC	Global Initiative against Transnational Organized Crime
IUU	Illegal, unreported, and unregulated fishing
MLT	Money Laundering Team (NZ Police)
MVTS	Money or Value Transfer Services
NRA	National Risk Assessment
NZTA	Waka Kotahi, New Zealand Transport Agency
OIO	Overseas Investment Office
PML	Professional Money Launderer
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TNOC	Transnational Organised Crime
VASP	Virtual Asset Service Providers

Terminology

Commingling

The mixing of funds, such as personal vs. business, legitimate vs. illicit, or client vs. company, to hide the ownership or remove distinction of the true source.

Cuckoo smurfing

Cuckoo smurfing (also known as, 'third party payments'), involves the transmission of cash into numerous bank accounts of seemingly unwitting recipients.

The term "Cuckoo" is used as the process is like the Cuckoo bird who lays her eggs in the nests of unsuspecting birds who then raise the Cuckoo bird hatchling as their own.

In 'cuckoo smurfing', criminally derived cash is dispersed into accounts where the account holder has no idea, or presumably no idea, about the origins of the cash.

In these circumstances, a money laundering network is made aware of and acquires transactions involving the remission of money from an overseas jurisdiction from a legitimate or illegitimate source, be that a person, company or money remitter. Cash is collected from the criminal syndicate and is deposited by using the smurfing typology.

Daigou

A form of informal value transfer often used in the China context to evade foreign currency restrictions and/or import duties.

Facilitator

An individual within a key industry who helps to enable the movement of funds or assets. They may be a professional money launderer, or corrupted or coerced into facilitating.

Layering

Moving, dispersing, or disguising illegal funds or assets to conceal their true origin (for example, using a maze of complex transactions involving multiple banks and accounts, or corporations and trusts).

Mules

A mule (also known as, 'cash courier') is a person who transfers money acquired illegally on behalf of another or allows their bank account to be used to transfer money acquired illegally for such a purpose. Typically the mule is paid for services with a small part of the money transferred.

Offsetting

The common alternative remittance practice of offsetting — hawala or hundi — enables the international transfer of value without actually transferring money. This is possible because the arrangement involves a financial credit and debit (offsetting) relationship between two or more dealers operating in different countries.

Remitters

Money transfer businesses and alternative remittance services transfer money within and between countries, often outside the formal financial and banking system, and without necessarily maintaining an account. They can offer a cheap and reliable service for getting funds to countries and locations which do not have modern formal banking services.

Smurfing

When multiple individuals deposit large amounts of cash into a bank account in a series of small amounts at different banks on behalf of an individual or syndicate, in an attempt to avoid suspicion of banking staff or law enforcement officials.

Structuring

When an individual deposits large amounts of cash into a bank account in a series of small amounts at different banks in an attempt to avoid suspicion of banking staff or law enforcement officials.