FINANCIAL CRIME PREVENTION NETWORK

Threat assessment

Understanding Profiles of Scam Victims

November 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, Immigration, Inland Revenue, and major NZ banks: ANZ, ASB, BNZ, Kiwibank, TSB, and Westpac.

The FCPN has enabled the National Fraud Centre to progress, and has acted as a key coordinator around alignment and amalgamation between private and public which is critical for action to combat fraud.

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.

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 aims to assist in the detection of financial crime and identify disruption opportunities.

Acknowledgements

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

Published November 2024.

About this Threat Assessment:

This assessment is designed for New Zealand's financial institutions.

Financial institutions are in a unique position to intercept or detect scams, as the financial component of the scam happens. Larger financial entities, such as the FCPN member banks who contributed to this assessment and occupy a majority market share[1], collect a lot of fraud and scam data that smaller institutions may not see on the same scale. The FCPN member banks have submitted some of this data for this assessment, which has been anonymised and aggregated with trend analysis for use as 'FCPN data'.

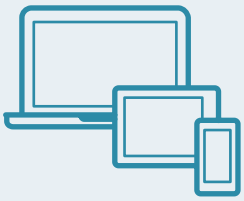
Data has been assessed on a customer-volume basis, rather than a loss-value approach. This has been done to show how many people have been affected by scams and fraud, which will enable financial institutions using this paper to assess their own customer cohort.

This assessment may be used to develop indicators, focus resources, policy development, strengthen monitoring and improve support for customers. It has been written to contribute to a robust, strong financial industry and assist in reducing losses for all New Zealand.

[1] The FCPN Member banks make up over 90% of the market; https://www.globaldata.com/store/report/new-zealand-retail-banking-competitive-benchmarking-market-analysis/

Key Points

All New Zealanders can potentially be the victim of a scam.



Scams can be encountered in many places and forms.

Victims suffer an emotional toll as well as a financial loss.

The financial system is a key point of detection.

The likely age of both a scam victim and a mule are trending down, towards younger people.

Smaller banks are more likely than larger banks to have new accounts opened by mules.

Repeat victims are more likely than first time victims to not know the source of the scam. Making efforts to identify the original scam event therefore has the potential to reduce the number of repeat victims.

Introduction

Scams are on the rise around the world and all New Zealanders can potentially fall victim of a scam or scam-related activity. Scammers are creative and persistent, with a variety of scam types targeting different demographics; there is something for everyone. While financial institutions can monitor for phishing sites, suspicious activity, and fraudulent transactions, this often results in a whack-a-mole exercise in a resource-constrained operating environment.

In developing this Threat Assessment, the FCPN member banks have pooled their data and insights – looking at high-level trends and demographics in confirmed scam and mule cases, as well as repeat victims – to identify hot spots, patterns, and higher-risk customers.

The (almost) $200 million problem

New Zealanders lost about $198 million to scams in 2023.[2] Nine out of ten Kiwis have reported being targeted by a scam, and fraud is now the most common crime in New Zealand, continuing to occur at a rate that is increasing year on year.[3]

Prevalent scam types in New Zealand include:

- investment scams
- phishing
- invoice scams
- bank impersonation
- online shopping including Facebook Marketplace
- cold call scams
- remote access
- relationship scams

Scams can be encountered via multiple channels: social media, email, text, phone calls, mobile apps, websites, and internet searches.

The cost of this problem is not limited to financial losses. Victims experience upset and inconvenience, disruption of their ability to engage with their normal lives, may need to take time off work, and often report feelings of shame or embarrassment. People may experience re-victimisation, as some scammers go on to leverage a victim's compromised or vulnerable state to carry out a tailing scam, further defrauding their victim. In addition to re-victimisation, individuals are targeted by scammers for use as money mules; wittingly, or unwittingly, they may become part of the scam and move illegally acquired money on behalf of the scammers.

New Zealand is not alone in this, as scams and fraud are increasing globally, with record increases in other countries and there is a widespread response to combat the problem.[4]

A core objective advanced by the Police is for everybody in New Zealand to 'Be safe and Feel safe'.[5] This approach, central to the current Police strategy, places importance on the response to the wider financial crime landscape as the effects of scams and fraud are keenly felt at growing scale.

In addition to Police, New Zealand has several organisations in the public and private sectors working against fraud and scams. These include: Netsafe, CERT NZ, the Serious Fraud Office (SFO), Financial Markets Authority, Department of Internal Affairs, the Commerce Commission, Customs, and the National Fraud Centre. There is opportunity for disruption, working with the differing remits and operations of these organisations. Scams have several stages that organisations can target their resources to support prevention, including fraud awareness, law enforcement action, consequences as deterrents, cyber security, phishing takedowns, and victim support.

Formative discussions are taking place between these agencies and private industry including banks, telecommunications companies, and social media platforms about improving New Zealand's overall response to fraud.

---

[2] https://www.mbie.govt.nz/about/news/198-million-dollars-lost-to-scams-in-the-last-year

[3] https://www.justice.govt.nz/assets/Documents/Publications/NZCVS-2023-Key-Stories-Cycle-6.pdf

[4] https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2022

[5] https://www.police.govt.nz/sites/default/files/about-us/about-nz-police/our-business-2024.jpg

Scams

General observations

The most prominent scam types reported across the FCPN data sets, looking at individual customers, are:

- Phishing and smishing
- Cold call scams and bank/trusted business impersonation
- Online shopping and marketplace scams
- Investment scams
- Relationship/romance scams

Scam victims across the data assessed are slightly more likely to be women than men; this was similar to unwitting mule activity.[6,7] Scam victims generally have established banking relationships: they are usually not new to their bank or seeking out new accounts at the point that they have been targeted by a scam.

Across the majority of FCPN data sets, for most scams, the breakdown of victims is fairly even across age, gender, length of banking relationship, and location; however, there are some variations depending on the channel used, i.e., digital banking as opposed to card activity.[8]

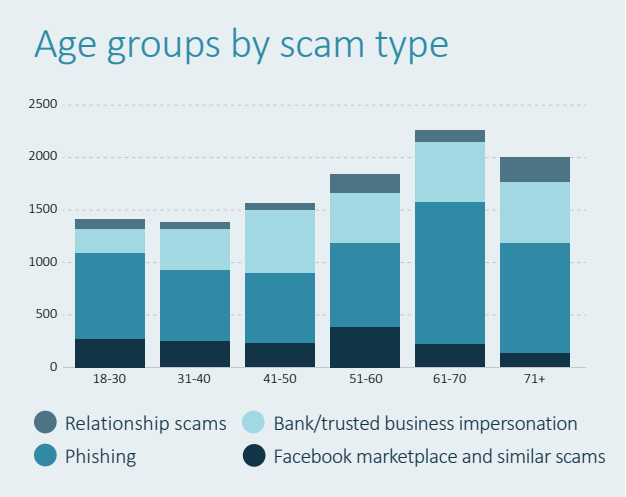
The age group differences have shown some trends based on scam type, but broadly all ages have been represented in the victim groups, with only a slightly higher likelihood of victims to be aged 50+ rather than 18–50-year-olds (yo). The example in *Figure 1* is from one FCPN data set, showing the number of victims in each age group ranging from 1343 (smallest, 31-40yo) to 2182 (largest, 61-70yo),a difference of less than 48% between the ends of the range and indicating how all age groups are at risk of being victims of scams.

While individuals aged 50+ are common victims and targets of scams, there is a global rise in younger generations as scam victims; they may be Gen-Z, younger millenials, or digital natives. Multiple factors are contributing to this:

- The amount of time Gen-Z is spending online, increasing the chance of being targeted
- The number of different accounts Gen-Z will operate online, creating more opportunities for account compromise; such as by phishing emails or data hacks and leaks, as well as the different forms of technology they are using
- Lack of understanding of how certain processes work, for instance an investment scheme
- Increased online purchasing, allowing more opportunities for fraudulent websites or marketplace scammers to be taking advantage

Digital natives may be more trusting of online communications and mechanisms, which can be exploited. Their older counterparts, while more naïve in the world of online connectivity, may be a little more cautious – a hesitation that could be paying off in their favour and protecting them from some scams. Either way, the data of victims in New Zealand across the FCPN members shows that there is a scam for everyone.

Figure 1: Phishing is the prominent scam type for all age groups. One FCPN data set, charted here, shows the ages affected by scams. The difference between the largest and smallest age groups of victims is less than 48%.



[6] An unwitting or unknowing mule is someone who moves illegally acquired money on behalf of someone else, without realising that there is a scam or any illegal activity.

[7] See page 16, section 'Mules'

[8] Private FCPN members, as individual banks, keep data about customers, scams, and scam victims differently. This means there is disparity in how the trends present as the originating data sets have been recorded in different ways, resulting in fewer common points of comparison.

Phishing/smishing scams

Phishing and smishing scams are the most prolific across the FCPN data set. The prominence of phishing scams is evident across all demographics.

It is likely that established communication practices amongst some large organisations in New Zealand may lead individuals to be complacent about the emails and SMS they click on, and what information they provide to those who ask for it. At the same time, savvy customers who are highly aware of scams are starting to delete genuine communications, highlighting the need for strong and consistent communication methods.

Observations in the FCPN data sets recorded a variety of differing insights, highlighting that phishing and smishing affect all age groups and genders. It has been a driver of mule account use in New Zealand, with data showing a lot of mule account activity has stemmed from phished customers. One data set showed phishing and smishing have also appeared as the most common fraud type for repeat and long-term victims. As the most common scam type, it is unsurprising that it would remain prominent from first-time victims to repeat victims.

Another data set recorded phishing as the most common scam affecting individuals across 2022 and 2023 – with phishing emerging as a prominent scam type for businesses in 2023 as well. There was an increased number of scam victims in this data set, largely due to the rise in phishing which showed a 249% increase in individual victims from 2022 to 2023. This highlights the ability for criminals to reach large numbers of New Zealanders through scam emails and texts, and successfully obtain banking details.

In the data from one FCPN member, people in their 20s are the most common age group of scam victims, making up 19% of all scam victims; this was primarily driven by the fact that people in their 20s were most likely to be a victim of phishing/smishing, which was the most common scam type by volume.

Within another data set, people aged 60-plus made up almost half of the phishing victims, and almost a quarter of all scam victims that the FCPN member saw.

Another member recorded the mean age of phishing victims as 52; others showed significant numbers for those in their 20s and 30s, and 60s and 70s.

The one group not shown as a primary victim group in the FCPN data appears to be those in their 40s. However, as phishing is so prolific, individuals in their 40s are still highly likely to fall victim to this kind of scam.

Phishing and smishing

Scam profile

A fake website has been created, imitating a legitimate business, in an attempt to coerce victims into entering thier login information or banking details. Victims are usually sent to this website via email or smishing, which has a similar approach but targets victims via text. Details captured through phishing sites are usually used to compromise other accounts or defraud victims.

Victim profile

Highly likely to be **anyone**

Local phishers

Operation Camperdown in April 2024,[9] targeting phishing as a service platform, LabHost. With numerous customers affected that belonged to FCPN members, the FCPN contributed intelligence on fraudulent activity to assist the Police's cybercrime unit. The Police executed search warrants at three addresses across Tāmaki Makaurau with much success, seizing a number of computers, as well as other electronic devices and documents.

[9] https://www.police.govt.nz/news/release/nz-caught-worldwide-phishing-sting

Cold call scams and Bank/Trusted Business Impersonation

Cold call scams

Cold call scams and bank/trusted business impersonation scams were shown to impact a notable proportion of victims. There was a prominence seen across FCPN data sets in the rise of impersonation scams; one member saw a 122% increase in 2023 compared to 2022. Another FCPN member recorded cold call scams as their most prolific, affecting the highest number of victims in the data assessed.

The mean age of a cold call scam victim is 60, and they are slightly more likely to be female than male. This is likely due to the generational difference in relationships with phone calls: a younger person will tend to prefer alternative forms of communication over phone calls, and so is less inclined to answer a phone call, whereas a person aged around 60 is much more likely to pick up the phone and engage with the caller, bringing more trust to the interaction from the outset.[10]

Bank or Trusted Business Impersonation scams

The scam typology is broadly similar to cold call scams – unsolicited contact pretending to be making contact for a legitimate reason – however scammers may contact victims in other ways; they may text, email, or use a messaging service like WhatsApp which may also be forms of phishing/smishing. Scammers will pretend to be a bank or other trusted business, such as PC Technical support, a utility provider, charity, or even loved ones like family and friends. They aim to trick customers into giving over banking details or other personal data, or simply sending them money directly.

Victims of bank or trusted business impersonation scams are a similar cohort to cold call scam victims: they are highly likely to be over the age of 40, most likely over the age of 60, and slightly more likely to be female.

An exception to this is younger males.[11] One FCPN data set revealed that younger males, aged 18-30, were almost twice as likely as females in the same age group to fall victim to an impersonation scam. For males under the age of 18, they were over ten times more likely to fall victim to an impersonation scam versus a female of the same age.

Cold call scams; Bank/Trusted Business Impersonation

Scam profile: Cold call scams

Cold call scammers aim to get personal or payment information from a victim by pretending to be a legitimate business, or by trying to sell a fake product or service. There are a variety of approaches the scammer may take, telling the victim about an issue with thier computer, an invoice is due, there is a refund or payment owed, and so on.

Scam profile: Bank or Trusted Business Impersonation scams

Scammers will call, text, email, or message via an app such as WhatsApp pretending to be a bank or other trusted business. They may carry out a remote access scam. Their aim is to trick customers into giving over banking details or other personal data, or access to this information.

Victim profile

Likely to be **aged 40-plus**
Highly likely to be **female and aged 60-plus**
May be **males aged 30 and under**

[10] https://www.rnz.co.nz/news/national/519797/telephonophobia-why-so-many-young-people-don-t-answer-the-phone

[11] As this data set is from a smaller bank, this group is a very small proportion of the overall scam victim population.

Online Shopping and Marketplace scams

A victim of an online shopping or Marketplace scam is more likely to be a younger person, in their 20s or 30s. Online marketplaces, such as on Facebook, have created opportunities for low-level fraud within New Zealand which has been capitalised on by scammers, many of whom are Kiwi themselves. While the fraud may be relatively low-value – for instance, a few hundred dollars rather than thousands or higher as often seen in other scam types – it still has a material impact, particularly as the fraud loss would likely be proportionately higher for a younger person compared to an older individual, who may have more financial stability, more savings, or a higher income.

With the emergence of the 2019 pandemic, many businesses moved online or started operating web stores. Businesses operating primarily out of social media or smaller, niche businesses that can pop up quickly and attract customers via apps like Instagram are very common. It has become more acceptable for a business to not have an established online presence, therefore adding a layer of complexity for the average consumer when deciding whether or not to trust an online store.

One FCPN member received over 5000 reports of this kind of fraud across a two-year period. This scam type was also common for unwitting mule activity, as victims may be directed to pay into accounts that do not belong to the scammer, making detection more difficult.[12]

A correlation was observed between the age and gender of online shopping victims. Female customer groups appear to be more susceptible to these scams in line with an increase in their age group. Younger victims of marketplace scams, therefore, were slightly more likely to be men, who were more affected in the under 18 group, as well as those aged 18-30, and 30-40. This is possibly due to the nature in how these groups are using the internet and seeking goods online: a younger male may be online shopping and be deceived by an opportunist scammer; and older females may be too trusting of a scam online shop.[13]

Online Shopping scams

Scam profile

Also known as Marketplace scams. Goods will be advertised for purchase online, but buyers never recieve their items. This may occur through a fraudulent website shop or a site like Facebook Marketplace, which has inspired a rise in opportunist scammers. The goods are often high-demand items like vehicle parts, electronics, or designer clothing. Offenders appear to prefer Facebook Marketplace over other online marketplaces like Trade Me, which are more regulated.

Victim profile

Likely to be **female, aged 50 and up**
Highly likely to be **male aged 30 or younger**

[12] See page 14, section 'Mules'
[13] See footnotes 17, 18 under section 'Mules'

Investment scams

Investment scams attract victims by promises of legitimate-sounding schemes, attractive return rates, and may even use fake dashboards to show victims how their 'investments' are tracking. Investment scams may be for legitimate-sounding businesses – or companies that do exist, but the scammer has no association with – and victims can struggle with determining legitimacy when doing their due diligence. Some of these common scams have used names of overseas banks, like HSBC and Citibank. Large sums, often in the tens or hundreds of thousands, can be stolen in an investment scam, having significant impact on victims. Investment scams also feature heavily amongst repeat or long-term victims.[14]

The ability for criminals to create fake websites, and have those sites elevated on search sites such as Google, means all New Zealanders can potentially be the victim of investment scams. Scam results will be returned when conducting searches online for investment opportunities, and victims are then receiving call-backs from scammers claiming to be from reputable businesses.

Investment scams are more prominent amongst older customers, generally around their 50s-60s. This is a typical group who would be seeking investments, and have life savings or capital to invest, making them an attractive target for scammers.

Investment scams

Scam profile

Scammers offer investment 'opportunities' into companies or schemes that may exist, but they are not legitimately associated with, or companies which are completely fake. Money is typically sent offshore quickly and is difficult to recover.

Victim profile

Likely to be **aged 40 to 75-plus**
Highly likely to be **in their 50s and 60s**

[14] See section 'Repeat Victimisation', page 18, and footnote 20

Relationship/romance scams

Relationship scam victims are highly likely to be individuals aged 50 and up; males above the age of 70 are the most prominent demographic of the victim group. The losses from relationship scams can be significant, due to the emotional involvement and financial stability of the likely victim type – these victims present a major opportunity for relationship scammers, as they will usually have some assets, some form of life savings or retirement funds, or meet criteria to be able to take out loans or lines of credit.

There are multiple ways a customer who has fallen victim to a relationship scam may try to send funds: they may use a NZ-based mule or attempt to send money straight offshore under the guise of the scam. Financial institutions can watch out for an emergence in transactions being made to a new party, of high and/or increasing amounts, with emotive support reasons or travel arrangements given as the justification for the payments.

Relationship scams

Scam profile

Also known as romance scams. Scammers will use a fake online persona to develop a personal relationship with a victim. They will build the relationship to earn the victim's trust and then begin to request sums of money for legitimate-sounding reasons, such as investment recommendations, urgent medical care, or talk of problems that could be resolved by financial assistance, to which a victim might offer money.

Victim profile

Likely to be **above the age of 50**
Highly likely to be **male, aged 70-plus**

At-risk individuals

By scam

Phishing and smishing

Victim profile

Highly likely to be **anyone**

Cold Call Scams; Bank/Trusted Business Impersonation

Victim profile

Likely to be **aged 40-plus**
Highly likely to be **female and aged 60-plus**
May be **males aged 30 and under**

Online Shopping scams

Victim profile

Likely to be **female, aged 50 and up**
Highly likely to be **male aged 30 or younger**

Investment scams

Victim profile

Likely to be **aged 40 to 75-plus**
Highly likely to be **in their 50s and 60s**

Relationship scams

Victim profile

Likely to be **above the age of 50**
Highly likely to be **male, aged 70-plus**

By age

Under 18; 18-30s

This customer is most likely to be affected by phishing, online shopping or marketplace scams, and trusted business impersonations. **This customer will become more likely to be targeted or fall victim to scams.**

30s-40s

This customer is slightly more likely to fall victim to an investment scam or trusted business impersonation scam.

40s-50s

This customer is often a victim of phishing, investment scams, and cold calls and bankor trusted business impersonation scams.

50s-60s

This customer is often a victim of phishing, cold calls and remote access scams, bank or trusted business impersonation scams, online shopping and marketplace scams, and investment scams.

60s-70s; 70s-plus

This customer is likely to be a victim of phishing, cold call and remote access scams, and bank or trusted business impersonation scams. They're also highly likely to fall victim to an investment scam or relationship scam.

Mules

General observations

A money mule is 'someone who transfers or moves illegally acquired money on behalf of someone else' and may be moving money through almost any means.[15] They could be:

- Unwitting – having been duped into the scheme to have their account or handling of cash exploited.
- Witting – have an idea that they are involved in illegal activity.
- Complicit – be fully involved in the money laundering process and scheme.

The average age of mules is dropping. FCPN data shows that only a couple of years ago, mules were more commonly in the 40-plus age group. This has steadily decreased year-on-year. Mules were more likely to be in the 30-40 age group in 2023, and so far in 2024, more recently identified mules are more likely to be under the age of 30. Mules are also more likely to be male than female.

In some data sets, no complicit mules were identified – that is, none of the mules in the data were confirmed as being a part of the money laundering process and scheme. However, up to 80% have been identified as witting, a concerning statistic that points to awareness of the mule's engagement in illegal activity and choosing to be involved anyway. Their chosen involvement could be because of the vulnerability of their situation, need for money, lack of experience or understanding, or pressure from involved parties.

The increasingly younger demographic of both witting and unwitting mules is likely being driven by a number of factors. Increasing cost pressures and lack of employment stability in an unstable job market can be common across a range of age groups; however, a younger demographic is likely to have higher internet and social media use which can open them up to being targeted for recruitment. They may lack the experience to identify where a deal seems too good to be true or trust another peer who is also being used as a mule, exposing themselves as a target. Additionally, local and international students – a typically younger demographic – may be targeted to carry out payment transfers, either while they are in the country or once they have left New Zealand, in a manner akin to a typology which has emerged in Australia.[16] This is another factor which is likely to contribute to the prominence of increasingly younger mules.

Unwitting mules are slightly more likely to be women than men, just as scam victims are also more likely to be women. Women may be targeted or exploited in ways that would be less common or successful amongst men. This is possibly due to the prominence of women performing more emotional and cognitive labour than men in 'invisible labour' and decision fatigue. Simply put, women generally do more mental work than men, reducing their likelihood to critically assess a possible scam in front of them.[17,18]

A lot of unwitting mule activity came from phishing and relationship scams. These are scam types which benefit from having New Zealand mule accounts; it can add a sense of legitimacy for victims to pay into a local account. For other kinds of scams such as investment scams, it can make sense for the scam typology for victims to send money overseas, for instance for a scam company purporting to be in Australia or the United States, lessening the need for mules in those cases.

[15] https://www.austrac.gov.au/sites/default/files/2024-06/2024_AUSTRAC_FCG_StudentMoneyMules.pdf
[16] Ibid.
[17] https://www.bbc.com/worklife/article/20210518-the-hidden-load-how-thinking-of-everything-holds-mums-back
[18] https://www.abc.net.au/news/2024-08-19/understanding-decision-fatigue-and-how-it-plays-out-in-families/104185036

Bank account age

Mules are more likely to be opening new accounts at smaller banks than bigger banks.[19] Among the FCPN data, bigger banks (i.e., with more market share) had a much smaller proportion of mules who had held a banking relationship with them for less than 12 months – as little as 10%. This increases in relation to the bank size: the proportion of customer accounts under 12 months old was 25% for one smaller bank, and as high as 49% at another smaller bank.

Mules may be opening or being instructed to open accounts with another bank for the purpose of carrying out mule activity, where it could be more difficult for a bank to identify what 'unusual' activity would look like for that customer. With the increased probability that an individual will already hold an account at a bank with higher market share, mules are then less likely to be able to open a 'new' account with no banking history, therefore being attracted to or directed to a smaller bank they have not used before.

Mules at bigger banks generally have longstanding bank accounts, which will include ordinary spending. There is a possible correlation with the younger people being recruited and newer accounts being used at smaller banks. Younger people may be more inclined to open new bank accounts for a set use: similar to how they may start a secondary email address or 'fake' social media account for a specific purpose outside of their regular usage.

Repeat victimisation

Phishing and smishing are the most common fraud type for repeat and long-term victims which aligns with these scam types being the most prominent overall. Investment scams are also prominent with one FCPN data set identifying repeat victims of investment scams making up 28% of all repeat and long-term scam victims, despite investment scams making up only 8% of all scam victims within that bank. This overrepresentation is likely due to the nature of investment scams, which can involve significant sums over an extended period, and the offer of 'services' to assist scam victims with retrieving their money but is in actuality another scam type, known as a 'money recovery scam'.[20]

Repeat victims are also more likely to not know the source of the scam – where the scam type was unknown or unexplained, and the customer is unsure of how they've been defrauded. This is likely a result of the repeat victims being unable to identify or recall any specific event that led to the fraud attempt in the first place and still having a vulnerability either with their personal banking details or with their ability to identify the scam.

Making efforts to identify the original scam event, or convincing a victim that a scam is occurring where they may be in denial, therefore has the potential to reduce the number of repeat victims.

Being clear with customers about scam support services, and giving advice and expectations about legitimate scam response and recovery procedures, are approaches that financial institutions can use to improve outcomes for scam victims and lessen the likelihood of revictimisation.

[19] Smaller or bigger by market share

[20] https://www.accc.gov.au/media-release/criminals-targeting-victims-of-previous-scams-promising-financial-recovery.

Recommendations: Support for victims

Engaging with external agencies

Several other agencies can contribute to wrap-around support for victims. These include:

NZ Police
Reporting scams through 105:
www.police.govt.nz/use-105

Age Concern
www.ageconcern.org.nz

ID Care
Several FCPN members have collaborated with ID Care:
www.idcare.co.nz

Netsafe
www.netsafe.org.nz

In-house support and protocols

Arrangements can be made with victims to receive follow up care and education from frontline teams. When a scam initially occurs, a victim will often be primarily focused on resolving or managing the financial loss and breach of personal information. Afterwards, they may have other questions, be open to further education, or be in a position to make changes in their financial security.

Organisations may want to implement processes so that vulnerable customers, who are victims, can arrange a face-to-face meeting at a local branch for more in-depth and personalised conversation.[21] Customers suffering financial hardship could be referred to a dedicated customer financial wellbeing team.

The opportunity to support victims at this stage post-scam could make an impact to broader scam education and reduce re-victimisation. These support mechanisms can build a customer's trust in their bank and create a positive connection out of a negative event.

[21] "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

Education

Financial institutions, whether in a proactive way, immediately when a scam has occurred, or after a period post-scam event, should share steps which customers can take to validate a situation in the future. This could be information already posted on the organisation's website. For example:

- Phone conversations with education and awareness on scams, in particular highlighting red flags
- Calling back on a publicly-listed phone number
- Referring to the Financial Markets Authority (FMA) website https://www.fma.govt.nz/scams/
- How to contact banks more quickly, if there has been a delay in the scam being reported, such as a 24/7 fraud line the customer can use
- Maintaining a fraud and scams informational page on the organisation's website with up-to-date information and processes, including contact details to report fraud or seek further education or validation resources
- Notifications and alerts on banking apps with prominent, emerging scam types
- Including scam education pieces in regular communications, or dedicated informational emails on preventing scams

Internal mechanisms

Organisations could use 'special care' notes, documenting in records or admin notes on a customer's account, ensuring that all bank staff are informed if customer is a previous scam victim. In other cases, the use of limitations or restrictions on banking, or putting thresholds in place may be effective mechanisms to prevent future scams. Alternatively, watchlisting at-risk customers to monitor for suspicious transactions may create the opportunity to disrupt any future scam attempts.