Caught in the Web

Falling victim to a sophisticated scam begs the question: who pays?

BY SASHA BORISSENKO

It was a Sunday in late February. I woke up early and managed to sweat off a week's worth of cortisol at the gym — either that or it was the last of the pinot grigio I had consumed the evening before.

Feeling saintly, I turned to Facebook Marketplace, where I'd put a mammoth-sized toaster up for sale, desperate to get rid of it. A few buyers had shown interest overnight — Jeff could only pick it up in a month, Jenny was a no-go as her profile looked dubious, and Mary could drive from Lower Hutt, but it would be much easier if she organised a courier. All I had to do was confirm receipt of payment. A no-brainer, I thought, choosing the latter.

The email I soon received from NZ Post looked official and took me to a POLi banking portal. The Kiwibank website required my access number, password, and answers to my KeepSafe security questions. For example, Where was I born? Given the number of boxes that matched my specific answers — San Fran, not San Francisco — the site seemed completely legitimate.

And so I continued to believe. For two days, the toaster sat in the postage-ready box by the front door of my apartment. Mary even reassured me at one point, saying I'd get a call from the courier shortly.

Annoyingly, I missed the call at 5:27 p.m. on Tuesday, or so I thought. It was actually Kiwibank alerting me that something was amiss. Shortly after, a text from a four-digit number said I should give the bank a ring if I suspected anything was wrong. When I went online to check, I saw that all my Kiwibank accounts were at zero.

I was alarmed, but it was a mistake, surely?

My blood ran cold when the Kiwibank representative told me the NZ Post, POLi-banking and Kiwibank sites I'd engaged with over the courier parcel were fake. It was a phishing scam and in nine minutes all of my tax, mortgage, student-loan and credit-card reserves were cleaned out. I'd lost $12,500.

I howled, dry-retched, and shed a lot of tears. Feeling ashamed, confused, violated and increasingly paranoid, I couldn't understand how I could have been so stupid. Kiwibank, police, my friends, and even a legitimate NZ Post-pinned Facebook post would tell me it was common, however.

"Facebook Marketplace is considered a high-risk platform for sales and purchases, due to the ease with which profiles can be manipulated. This NZ Post scam is common and has been linked to overseas offenders on multiple occasions," an email from police read.

And yet in a 2023 survey, Netsafe found 17 per cent of Kiwis have lost an average of $3165 to scams, amounting to $2.05 billion. Combined data from New Zealand banks provided to the Ministry of Business, Innovation, and Employment (MBIE) suggests customers lost $198 million last year alone.

Same script, different scam

Jane* is one of those people. A small business owner based in the South Island, she had $300 stolen from her credit card in 2023. BNZ gave her

Facing page: Sasha Borissenko was the victim of a Facebook Marketplace phishing scam. Above: The toaster she was selling.

a call via an unknown number and walked her through several easy steps before reimbursing the cash. Fast forward to June this year, Jane received another call, this time from her "local BNZ branch".

The representative — "William" — said there had been suspicious activity on her credit card. After asking to confirm contact details and Jane's online account access number, William listed some legitimate transactions and one that wasn't accounted for.

"Listening to this person use the same script, almost word for word, it never crossed my mind that it wasn't BNZ. He spoke so fast, and I got swept up in the sense of urgency," Jane said.

Four hours and two BNZ alerts later, Jane learned $40,000 had been transferred, not from her credit card, but from a separate business account. William had free range to access Jane's staff wages, GST, and other business funds.

She said she had no idea how the scammer knew all her contact details.

"It took me a couple of minutes to realise what had happened, and then I felt completely nauseous. It was awful. I really felt like I was going to throw up."

A BNZ spokesperson said it could not discuss Jane's case without a privacy waiver but could confirm there had been no breaches of BNZ's systems or data in 2023 and 2024.

"We have worked with New Zealand's three largest telecommunication companies — 2Degrees, Spark, and One New Zealand — to stop scammers based overseas from spoofing our 0800 number [and] other published BNZ telephone numbers."

The spokesperson said banks were required to promptly notify regulators if there was a cyber interference or data breach, including remedial actions and potential impacts to customers.

"The safety and security of our customer information is our utmost priority, and we strongly refute any suggestion that our BNZ systems have been compromised.

"Every year, we invest tens of millions of dollars in cyber security and scam and fraud protection measures. We continuously monitor, audit, and inspect our security systems, equipment and online banking transactions for suspicious activity."

All stressed out, nowhere to go

In my case, a police complaint proved fruitless. Official police correspondence would tell me that due to "investigative demands and prioritisation, we regret to advise you that it will not be investigated further". For Jane — who also lodged a police complaint — the decision whether police would investigate was ongoing, she said.

Speaking generally, Detective Superintendent Dave Lynch said although scams had no legal definition per se, they tended to fall under "fraud", which carried a maximum sentence of up to seven years imprisonment under the Crimes Act.

Police figures suggest there were 488,000 fraud and cyber offences between November 2022 and 2023, affecting 11 per cent of New Zealanders. Police had no datasets capable of providing readily retrievable information specific to online banking, Lynch said.

It seems the issue is widespread. The Independent Police Conduct Authority reviewed the situation after receiving 52 complaints about police responses between 2018 and 2022. Police acknowledged in their findings that they struggled to assess the scope of fraud offending and that many reports were not recorded correctly in the police database. The authority highlighted that cases were often complex, police lacked specialist fraud squads, and investigations varied between regions.

The problem isn't unique to New Zealand. In the UK, a 2018 Police Foundation report estimated that of the 3.24 million fraud offences in the year ending March 2018, just 638,882 frauds were recorded by police and industry bodies.

The UK report found only one of every 13 reported crimes was investigated. Of those, only three per cent resulted in a charge or resolution, compared to 15 per cent of violent offences.

Back in New Zealand, the Serious Fraud Office is working with the Ministry of Justice and police to develop a National Financial Crime and Corruption Strategy. MBIE also chairs an inter-agency Fraud Working Group, which aims to raise awareness and share collective intelligence across government, law enforcement and industry.

In the meantime, Lynch said police continued to work with banks and international institutions to tackle organised crime that "so often sits behind these scams", he said. "Given a significant proportion of frauds involve offenders being able to acquire funds unlawfully from victims' bank accounts, banks are often the first place victims turn to for assistance."

The appeal of keeping your cash in a kitchen jar

If finding and prosecuting scammers is near impossible, where do the banks fit into the equation?

For me, Kiwibank's fraud investigation team managed to retrieve $3000, leaving me originally out of pocket $9500. The retrieval process took about a week, far longer than the nine minutes it took to snaffle.

For Jane, BNZ had retrieved $500 and the investigation was still pending at the time of this interview.

Speaking generally, a BNZ spokesperson said that once a customer's funds have been transferred from BNZ to a third party, "we must rely on the third party to investigate and recover the funds, which means we can only move as fast as they do.

"We understand this can be frustrating for customers. However, these investigations can be complex and lengthy as the scammers can move funds multiple times, including to overseas banks," the spokesperson said.

But how could the transactions happen in the first place? As Jane and I both would argue we didn't receive a bank notification to authorise or confirm payments of such large sums? The fraudsters could also use foreign devices to roam around in our respective accounts with abandon.

A Kiwibank spokesperson said the bank took the security and protection of its customers very seriously, having invested heavily in its people and technology and providing education on how to stay safe. "We continue to upgrade our fraud monitoring systems, to enable enhanced detection and blocking of suspected fraud in real-time. These changes signal a multi-year commitment to achieve better outcomes for our customers."

BNZ had stopped sending links in text messages and introduced an additional two-factor authentication requirement within internet banking for actions such as changing contact information, creating or editing payees, and making payments to unsaved payees.

The BNZ spokesperson also said the bank introduced a new way for customers to verify their identity through the BNZ app when prompted by staff members to confirm the bank's identity.

"This is particularly effective in combatting bank impersonation scams as it allows a customer to respond to a prompt without giving any identity details to the staff member."

A case for reimbursement

But are banks doing enough? The New Zealand Banking Association's Code of Banking Practice is voluntary, industry-led and sets minimum banking standards, including setting out terms of liability banks have for unauthorised transactions.

Banking Ombudsman Nicola Sladden says the code requires banks to reimburse transactions a customer didn't authorise, provided they weren't dishonest or negligent, that they complied with the bank's terms and conditions, and that they took reasonable steps to protect their banking.

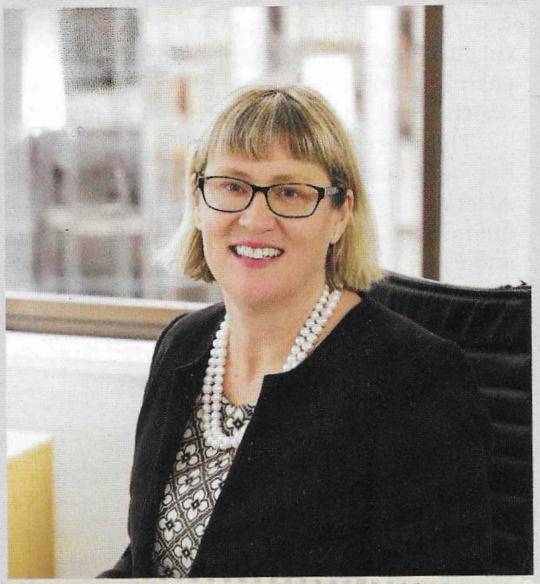
"A bank can only rely on customer actions that fall below this standard of care and contributed to the loss to deny reimbursement."

In addition to the victim-blaming logic, there is a paradox in which, by revealing the circumstances that led to the loss, customers may also inadvertently shoot themselves in the foot.

Because Jane didn't provide her access code or password details, she would theoretically have a good case for BNZ reimbursement.

For me, all signs pointed to "fresh out of luck". Because I failed to recognise the signs of fraudulent activity and provided my details, I essentially contributed to the loss.

Incredibly, after 40-odd calls, a life's worth of being on hold, a seven-page legal-esque brief,



Top: Banking Ombudsman Nicola Sladden. Above: Banking Association chief executive Roger Beaumont.

and various calls to "talk to the manager", Kiwibank reimbursed me the shortfall on a goodwill basis.

Sladden says banks may offer goodwill payments to fraud victims — even when they're not obliged to do so. The watchdog was not aware of any formal guidance as to what constituted goodwill.

BNZ and Kiwibank did not respond to questions about their respective goodwill policies. Instead, both spokespeople said goodwill payments were assessed on a case-by-case basis.

For BNZ, any goodwill payments or reimbursements for unrecoverable scam losses were paid out of BNZ's operating funds.

For Kiwibank, the spokesperson said fraud and scams were not insurable events, hence the need for "all parties to work together on this issue and for customers to look out for known warning signs".

Cracking down on a lagging framework

The Banking watchdog has seen a 700 percent spike in complaints since 2015.

There were 233 complaints between April and June this year, compared to 120 complaints in all of 2015. Of the 949 scam cases between July 2023 and June 2024, the independent body resolved 38 percent partially or fully in favour of the customer.

In its 2023 annual report, scams made up 32 per cent of the watchdog's investigations, involving an average loss of $57,000.

"But it is not simply the volume of scam complaints that has been rising," Sladden says. "The sums involved have grown, too. The sums involved can be considerable — in the tens and hundreds of thousands of dollars. Some complaints have involved losses over $500,000, outside our current jurisdictional limit."

In April, the United Kingdom introduced regulations requiring banks to reimburse victims of "authorised push payment" fraud, with only limited exceptions. The move will come into force in October. Singapore and Australia have established anti-scam centres that promote prevention, recover lost funds and prosecute scammers.

Sladden believes comprehensive, mandatory codes of practice are needed for banks, telecommunication companies, and digital platforms to govern their responsibilities in preventing scams and their liability in the event of a scam.

"The reimbursement framework should give customers and banks alike an incentive to be vigilant to scams, and to respond effectively and promptly when they do happen."

After the Banking Ombudsman's calls for change, Commerce and Consumer Affairs Minister Andrew Bayly in February urged the banking industry to "take immediate and concerted action".

He called on the sector to introduce new security measures such as Confirmation of Payee technology, update its Code of Banking Practice, and investigate a voluntary reimbursement scheme by the end of 2024.

"Banks have a duty to act with reasonable care and skill, which includes identifying and acting on possible signs of fraud. Where you do not act on possible signs of fraudulent behaviour, or suspicious payments, my view is that you should reimburse customers," the minister told the banks.

If the Banking Code was not updated within a year, Bayly warned he would consider options for a regulated mandatory code.

For now, Bayly told *North & South* a mandatory code wasn't on the table.

New Zealand Banking Association (NZBA) chief executive Roger Beaumont said the 18 member banks would begin rolling out the new confirmation of payee technology in December. The advocacy group has also launched the first phase of an "Anti-Scam Centre", which allows banks to identify and share information about "mule accounts" used to move stolen money.

Since launching in December last year, banks have identified more than 2000 mule accounts. But Beaumont says banks are often at the end of the scamming food chain. Everyone needs to step up, including the government, telcos, social-media companies, and search engines, he said.

"If you're aiming to prevent scams, it makes sense to ensure all potential links in a scam chain are targeted. Also, if you're looking to shift liability from the criminals onto others, it may be reasonable for that liability to be shared among all participants who could have prevented the scam."

Beaumont said banks also committed to reviewing the international best practice for reimbursement by September this year. "The review's findings will be required before the NZBA and its members consider any updates to the reimbursement in the Code of Banking Practice," he said.

Where to from here?

Although Jane was waiting for the outcome of her investigation at the time of this interview, she was thankful she had enough money in reserves to make up for the loss and pay her 10 staff.

"Compared to others who have experienced similar frauds, it could be much worse. I don't want to say it's not a huge loss because it is. But we didn't suffer hugely because of it. Obviously, though, as time goes on, that money will be missed."

The psychological impact would take longer to recover from though, as she was now afraid of incoming calls.

"I can feel my heart beating really fast and even if it's BNZ calling, I'm really nervous whether it's actually going to be them or not, despite knowing full well that they're often who they say they are.

"It's hard because you like to think of yourself as an intelligent or capable person who would be able to see this type of thing, but when it happens, you're like, 'How did I not see it?'" ■

**Jane asked to remain anonymous.*