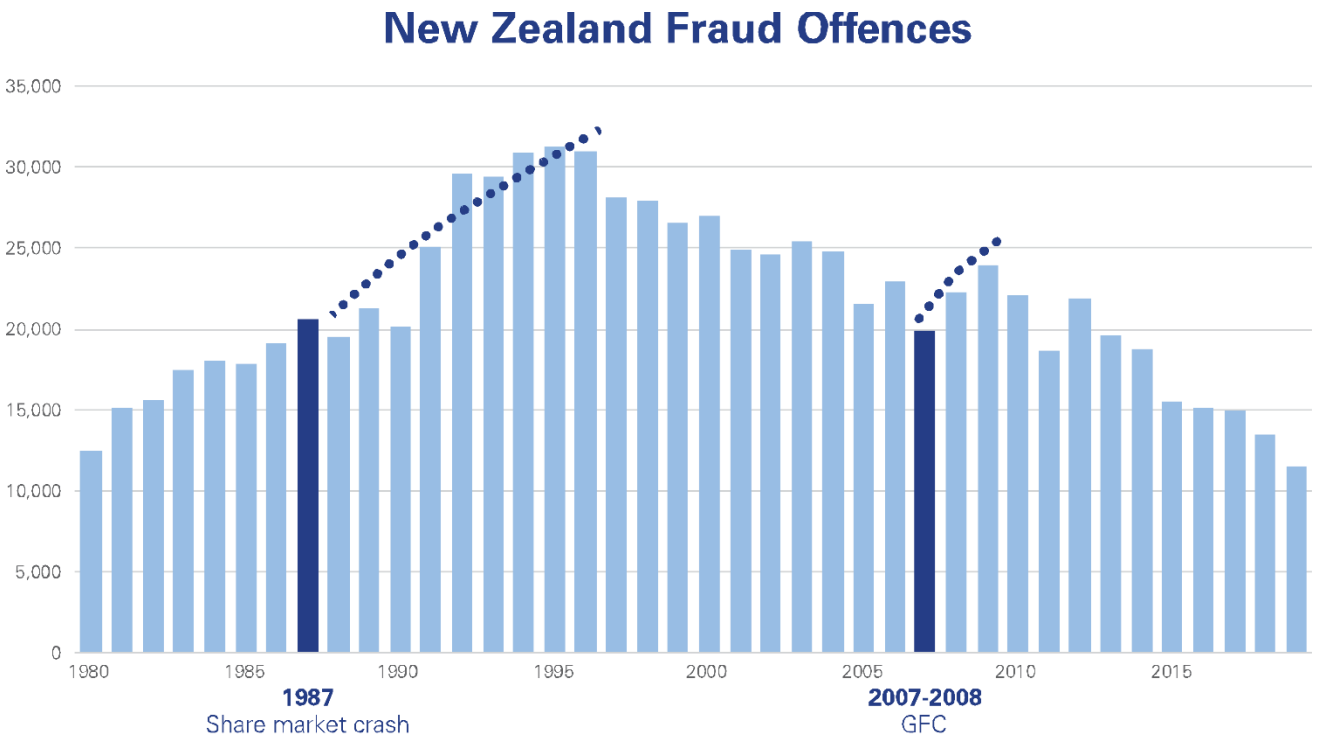
COVID-19

Fraud Risk

COVID-19 has created previously unthinkable consequences for our society. Organised crime has been quick to respond, mounting large-scale orchestrated campaigns to defraud banking customers, preying on fear and anxiety related to COVID-19.

In these uncertain and difficult times, fraudsters are opportunistically preying on the confusion created by this public health emergency, looking to profit from the public's desire to regain a sense of safety and security. They look to mimic the behaviour of those who are re-establishing norms and rely on impersonating entities that are genuinely trying to help.

History tells us that sudden changes to the economy can result in a period of increased fraud. The 1987 share market crash and the 2007-2008 Global Financial Crisis (GFC) both resulted in increased levels of fraud reporting. In both instances, as the economy recovered, the levels of detected fraud reduced.



Source: Stats NZ

Fraud typically occurs when three components align; opportunity, pressure and rationalisation.

The COVID-19 crisis has created the perfect storm in which all three factors are flourishing:

- social disarray and uncertainty has created opportunities that fraudsters are exploiting. Deviations from normal checks and controls present greater opportunities for fraud;
- financial uncertainty and reduced job-security have created financial pressure; and
- the uncertainty has created an environment in which it is easier for fraudsters to rationalise deviant behaviour (e.g. "my employer may fail and in any case, it's not my fault" or "bending the rules is ok in these circumstances").

Across the world, we have seen an increase in fraudulent scams associated with COVID-19. Victims are typically targeted via phone, email and social media.

Furthermore, as governments roll out stimulus packages in response to the pandemic and provide fiscal support to their citizens, the risk of being defrauded by scams related to COVID-19 will likely continue to rise. Financial pressures also increase the risks of bribery and corruption.

For the financial sector in particular, there are great challenges. The industry has already begun to provide an unprecedented response but is also busy with its own business continuity issues. Demand is far outstripping supply as concerned customers inundate call centres and fraud typologies are changing, almost on an hourly basis.

Businesses are currently focused on limiting the impact of COVID-19 on daily business routines. As a result, little to no time is allocated to monitor relevant key risks. This can lead to blind, or weak spots in business processes. Now that many companies have instructed their employees to work from home, a number of opportunities for increased fraud risks have been created.

Some COVID-19 related scams we have seen include:

- **Phishing scams:** Fraudsters are posing as members of domestic and international health authorities, such as the United States Centre for Disease Control and Prevention (CDC) or the World Health Organization (WHO). Victims are being targeted with emails including malicious attachments, links, or redirects to "updates" regarding the spread of COVID-19, new containment measures, maps of the outbreak or ways to protect yourself from exposure. Once opened, the computer may be infected with malware or expose sensitive personal information, or credit card details saved online, to a hacker. Fraudsters are also creating false bank emails complete with bank logos to target bank customers and obtain banking passwords.
- **COVID-19 fraudulent websites**: There has already been a significant rise in new fraud risk typologies, in particular related to the registration of large numbers of 'COVID' internet domains.
- **Compromised business email**: The increase in remote working, accompanied with organisation-wide updates regarding COVID-19, has opened the avenue for fraudsters to target businesses and their employees. Using emails disguised as COVID-19 updates, fraudsters attempt to trick employees to hand over their credentials by requesting their login to a faked company 'COVID-19' portal. Once an employee has entered their credentials, the fraudster has unfettered access to the employee's company accounts and the organisation's network. Bank logos are increasingly used to target bank customers and obtain passwords.
- **Charity scams**: In times of crisis, it is not uncommon for individuals to feel a personal sense of responsibility to help reduce the impact on the community. Fraudsters prey on this desire, soliciting donations for non-existent charities claiming to help individuals, groups, or areas affected by the virus, or contribute towards the development of a vaccine to fight the virus.
- **Mobile app scams**: Fraudsters are developing or manipulating mobile phone applications which outwardly look as if they track the spread of COVID-19. However, once installed the application infects the user's device with malware which can be used to obtain personal information, sensitive data, or bank account/card details.
- **Investment scams**: Keeping with the tradition of a classic investment scam, this scam has a twist, purporting to generate significant returns from investing in a company that has services or products that can prevent, detect or cure COVID-19. We have also seen superannuation funds targeted, in relation to early release of funds.
- **Taking advantage of uncertainty around new regulatory regimes**: There has been increased media coverage in NZ around employers taking advantage of wage subsidies and not passing these through to employees as intended, an area which the Government has said it will monitor and enforce strictly.

In addition, there is an increasing opportunity for fraudsters to target vulnerable members of our community during this period of change. We all need to ensure that we continually check-in on vulnerable family members, to ensure they are not taken advantage of during this time.

There are many ways to help protect yourself and your business from falling victim to COVID-19 scams. Paramount to reducing vulnerability is ensuring that people remain aware of how criminals are attempting to take advantage of the global health crisis.

So, what should you look out for and do to protect yourself?

- **Don't lose sight of your core values**. In a time of crisis, doing the right thing is more important than ever. The demise of a number of finance company directors through the GFC was at least in part due to them convincing themselves that the end justified the means.
- **Follow-up on suspicions of fraud, bribery and corruption**. The tendency of companies in crisis situations is to keep so focused on the crisis that they may miss other significant events occurring.
- **Carry out a risk assessment on any changes in business practices**, including an assessment of any IT risk that may have arisen through remote working.
- **Show compassion towards your employees** and keep them informed of key events. One of the key risk indicators for employee fraud is poor staff engagement.
- **Anti-malware and anti-virus software** installed on your devices must be kept up-to-date.
- **Be wary of fraudulent emails** claiming to be from experts who have vital information regarding the virus. Do not click links or open attachments from unknown or unverified senders.
- **Check email addresses** from sources claiming to have information regarding COVID-19 for irregularities, such as spelling errors or miscellaneous symbols. Fraudsters often use addresses that only have a marginal difference to those belonging to the entities they are impersonating.
- **Conduct background research** before donating to any charities or crowd-funding campaigns. Be wary of any business, charity, or individual soliciting donations in cash, through the mail, via fund transfers or other unusual channels.
- Finally, now is the time to **reflect on your fraud risk management system** and review its robustness in the current situation.

Please feel free to contact either the authors or your regular KPMG contact if you would like any further information.

Stephen Bell
Partner, Forensic
T: +64 21 412 769
E: stephencbell@kpmg.co.nz

Mike Lowe
Director, Forensic
T: +64 21 111 8545
E: mikelowe@kpmg.co.nz

Matthew Preece
Senior Manager, Forensic
T: +64 21 244 9297
E: matthewpreece@kpmg.co.nz