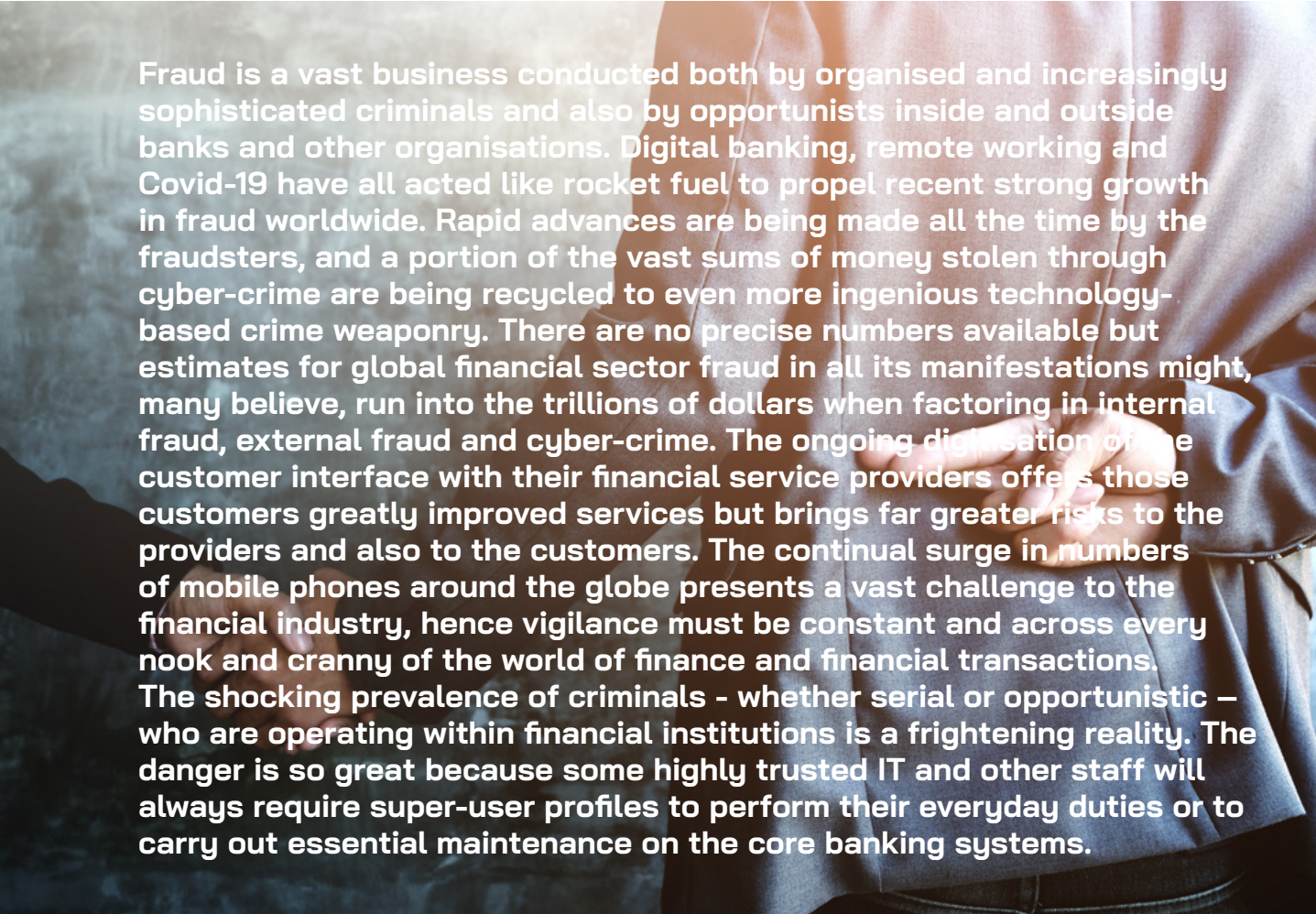


# Fraud Trends and Best Prevention Practices in the APAC Wealth Management Market



Fraud is a vast business conducted both by organised and increasingly sophisticated criminals and also by opportunists inside and outside banks and other organisations. Digital banking, remote working and Covid-19 have all acted like rocket fuel to propel recent strong growth in fraud worldwide. Rapid advances are being made all the time by the fraudsters, and a portion of the vast sums of money stolen through cyber-crime are being recycled to even more ingenious technology-based crime weaponry. There are no precise numbers available but estimates for global financial sector fraud in all its manifestations might, many believe, run into the trillions of dollars when factoring in internal fraud, external fraud and cyber-crime. The ongoing digitisation of the customer interface with their financial service providers offers those customers greatly improved services but brings far greater risks to the providers and also to the customers. The continual surge in numbers of mobile phones around the globe presents a vast challenge to the financial industry, hence vigilance must be constant and across every nook and cranny of the world of finance and financial transactions. The shocking prevalence of criminals - whether serial or opportunistic - who are operating within financial institutions is a frightening reality. The danger is so great because some highly trusted IT and other staff will always require super-user profiles to perform their everyday duties or to carry out essential maintenance on the core banking systems.

GET IN TOUCH

[Know more about NetGuardians](#)

Contact: <https://netguardians.ch/contact/>

## A HUBBIS VIRTUAL PANEL DISCUSSION IN PARTNERSHIP WITH NETGUARDIANS



# NetGuardians

## All Speakers



**PETER MARINI**  
NetGuardians



**BRENT SELLORS**  
PwC



**DENNIS CHEAH**  
UOB Bank



**YOU JUNG KEE**  
INTERPOL



**NAVINESH CHAND**  
Synpulse

But the big message emanating from the Hubbis virtual discussion event of April 14 is that there is hope, that the fightback is nevertheless taking place. Advanced AI-based anti-fraud technologies can fight back against all these avenues of exploitation. FinTech anti-fraud solutions are improving all the time as their ability to identify and block suspicious activity in real-time is becoming the trusted defence against the biggest fraud risk in banking. Big Data advances are moving so fast that there are ever more and ever-faster tools to help financial institutions fight back.

Moreover, the banks are increasingly working together and with the authorities as well, knowing that they cannot tackle this problem alone; they must work with industry peers and other parties in a far more coordinated manner. They must bring in the best global expertise, work with those firms and experts at the cutting edge of technology prevention, and with those who best understand the multitude of ways in which cybercriminals can penetrate organisations.

The eradication - through technology and human solutions - of vast numbers of false positives every day at every financial institution is a vital step in mining out the real criminal activity. Constant vigilance is needed, optimal digital solutions must be employed, greater domestic and global coordination must become the new norm. All these elements combined will very probably never stop fraud, but they will most certainly help to keep a lid on the worse excesses.

### The Key Observations from the Panel

#### Multiple and multiplying scenarios

There is already a plethora of scenarios for fraud, and these are multiplying daily. "A panellist said that no matter how many models they came out with, the new ways and means of attack just keep coming. Referring to all sort of Machiavellian tricks in Australia, it is just astounding how these new scenarios just keep emerging.

#### Trading on weaknesses

A panellist pointed, by way of example, to a newer area being exploited, namely in the trade finance space, where an existing customer of a bank puts through false documents, with bogus collateral, and bogus activity. However, because this is an existing customer the red flags are not raised internally, so the bank can more easily become the victim.

#### Psychological warfare

Another panellist likened it to psychological warfare, where in many instances, the victims are being frightened or coaxed into taking action or releasing information that will make them vulnerable. He gave the example of someone impersonating a police officer who calls an office to report that the company account has been used to receive trafficking money or money laundering. But he said it is also surprising how readily some people fall prey to these attacks, even though education is being rolled out in most jurisdictions.

#### Tools for the job – trust and more trust

Another expert remarked that so often, the fraudsters pretend that the target has themselves already been a victim of fraud. Playing on trust is the fraudsters' key tool, as it represents the weakest link, and it continues to surprise and disappoint him how many people fall prey to these approaches.

#### Fraud sans frontiers (without borders)

Interpol represents 192 countries and is incredibly busy through its Financial Crimes Unit, with almost all such financial crimes becoming more and more transnational and borderless.

#### Taking a holistic approach

To fight back, all stakeholders need to be involved, with a holistic approach involving law enforcement, keen cooperation with the private sector, and greater awareness and communication.

#### Audacious criminals, simple means

An expert warned that the sheer audacity of the methods used, and the usually highly personal approaches is both worrisome and scary, especially as so often it is the phone that is used, direct to someone's home or mobile.

#### Smartphones and smarter criminals

The Australian situation is increasingly difficult – and this simply serves as a bellwether for the planet at large – due to the continuous rise in smartphone banking apps. And there is somewhat of a laissez-faire attitude, especially amongst millennials and younger generations, who rather assume that problem is the banks and the authorities, not their problem. More complex ownership, corporate and other structures open the door to fraud ever wider, so too remote onboarding and account opening, with fraudsters targeting portfolios of all types of assets. As more branches are shut, especially since the pandemic, so the room for fraud expands.

### **A perfect storm is brewing**

This same expert said the result is a perfect storm brewing constantly, with the 'good guys' trying to race to stay ahead of all of the numerous scenarios that the fraudsters are trying to exploit.

### **Four malevolent avenues to defraud**

An expert pointed to four typical broad-brush approaches by the fraudsters. First are the more traditional financial crimes such as impersonation and deception in order to take money out of accounts directly or indirectly. Another is the public proposal scam, such as creating a bogus charitable or another website. The third is 'phishing', plying vulnerable people for information and data, with the elderly especially at risk. And finally, there is the worsening phenomenon of money laundering related to crypto or virtual assets.

### **Enhancing awareness of risky activity and behaviour**

An expert highlighted how in Singapore, the police and authorities are working with the banks and other parties to help fight back, but that the effort does depend on the willingness of the people involved to recognise the dangers they face and to communicate with the financial institutions. He explained that it is all too often difficult to persuade some people that they are taking risky steps, for example, sending money to people they might have met online and that they believe they trust. He explained that all too often, emotions get in the way of common sense and good judgement.

### **Spotting the rotten apples**

With the vast majority of transactions and activity non-fraudulent, it is increasingly difficult to identify the criminal activity. An expert advised not to answer any questions whatsoever from anyone who calls in unless the recipient had themselves instigated the call. Start each such call with the assumption that it could be someone trying to defraud, and with such an approach, most of the fraudsters quickly hang up.

### **Lessons from 'Neverland'**

Another expert listed some of the 'never-do' reactions. Never give away account information over the phone, never download documents, never offer up passwords or highly personal information, never make transfers unless 100% certain the right recipient is at the end, never succumb to fear, for example, if told that some authorities will come to visit because of tax or other fraud, after all the police do not announce their intentions in advance, and never believe people when they say something is extremely urgent, even when deep emotions are involved, for example in the case of someone pretending to have kidnapped a relative.

### **Fight back with sophisticated and coordinated data management and analysis**

Take a much more sophisticated approach to data capture and a less siloed organisational structure between different arms and legs of any organisations, with better analysis of activity data, transaction data, behavioural data, contextual data, and from external sources as well. Drawing on all these data sets to gain insights in a cohesive manner, including sharing data amongst teams and even third parties with which the organisation works will help significantly.

### **AI is here to stay, and it works**

Artificial intelligence opens the door to analyse data in a much more holistic and responsive way, helping refine the triggering of alerts and accelerating the process too.

### **But more coordination is required, locally and across many borders**

However, a major impediment remains the inability of some organisations and some jurisdictions to adopt and use such technologies and to then coordinate a response. Much more work needs to take place. However, Interpol, for example, does not have the mandate or right to force any jurisdictions to take any particular steps, instead trying to enhance cooperation, introducing the Financial Action Task Force (FATF) recommendations, so that Interpol member countries can prepare their own regulatory compliance efforts in the financial sector.

### **Action is taking place at the regulatory level, but only gradually**

There is no doubt that in a great number of countries, the regulators are now mandating some level of fraud control, but these are generally recommendations only.

### **Safety in the cloud, or greater risk?**

An expert pointed to the expansion of data held in the 'cloud', which reduces the weak links in the physical, terrestrial infrastructure organisations used to require.

### **WFH and Codes of Conduct**

In Singapore, the MAS is working hard to encourage a more rigorous code of conduct for the banks in relation to staff working from home. Better processes, better sets of rules and guidance, better training, improved monitoring, better systems for identifying risks or risky individuals, and other methodologies and steps will all help mitigate the very significant and elevated risks.

### **Watch out for internal collusion!**

An expert highlighted how in Australia, there is enhanced awareness of the risks of team members who are working remotely and colluding to defraud the institution or third parties. Better oversight, strengthened policies and procedures, more detective technologies and processes, and tighter controls on who has access to data, all these are vital steps to fighting back.

### **Mind the gap**

A speaker highlighted how it has often taken a year or more for organisations to discover internal fraud, and that there is little doubt that the WFH phenomenon has worsened the risks. This expert reported that accordingly internal fraud almost certainly is a bigger issue than had been seen so far and that more will be discovered over time, no doubt.

### **The more we know, the more we discover**

An expert reported that fraud cases are sharply on the rise, judging by the sheer number of cases they were receiving across their desk.

### **The 'Fraud Triangle'**

A speaker highlighted the opportunity for fraud, which has risen since WFH became commonplace. He cited the ACFE (Association of Certified Fraud Examiners) report of late 2020, which reported that 48% of respondents involved had seen an increase, especially in internal fraud, and that 71% believed this would get worse in 2021. "Internal fraud is therefore a huge and rising threat," he reported.

### **Systems must perform**

An expert said that when organisations selected IT hardware and software, they need to buy the right equipment and solutions.

### **Education is essential, while the right processes and systems are vital**

A guest highlighted the vital importance of communication and education of all parties involved, including those who might at some stage be subjected to fraudulent activity. And that should then be aligned robustly with the right internal controls, the right culture, the appropriate systems and the best processes.

### **Creativity is also a key element in the fight against fraud**

Another expert pointed to the value of trying to incorporate an element of creativity or imagination in the efforts at fraud prevention. Imagining where the gaps are, where there is potential for exploitation from internal or external sources, and continually questioning and probing the ecosystem for resilience or weaknesses are all valuable elements in the fight.

### Be proactive, not just reactive

A guest called for both a proactive and reactive approach. To be proactive, banks and other financial sector parties must introduce and then refine detection based on enhanced analysis and processes – for example, email monitoring for rapid response – and well-conceived and well-organised responses, right from the KYC/onboarding through improved CDD - customer due diligence - as well as raising internal awareness of the risks and best practices.

### Shared resources

An expert advised banks and other organisations to share financial intelligence, for example, on compromised accounts or potential criminal account activity.

### Technology investment is critical for survival

A banker highlighted the need to factor in the investment in the latest digital solutions as a core element of the overall return on investments. He explained that even when the latest solutions are brought in, the organisations must spend a lot of time and effort on continuous analysis of new trends, evolving trends, new fraudulent activity patterns, for example, leveraging behavioural biometrics. "We need continuous investment into fraud prevention and detection technology," he warned.

### A coordinated response required

The same banker also pointed to the need for other parties and the state to work together. For example, very often, the fighting of fraud should involve the telcos or others who deliver the phone, sim cards, internet or other mobile communications services. "All parties must get involved in tackling this fraud menace," he advised.

### Work with the right partners

The final word went to an expert who said that it was vital to acquire the right technologies and work with the right partners and fraud prevention vendors, and also to boost collaboration amongst the banks and other parties at risk or involved in some way or another. Being super smart at fraud prevention is not going to win new customers, but the financial and reputational risks of the bank or organisation being a victim of fraud or its clients being defrauded are both highly significant and rising all the time.

### NetGuardians – AI & The Future of Banking Fraud Prevention

Peter Marini offered the panel and delegates a brief introduction to [NetGuardians](#), an award-winning Swiss FinTech company. NetGuardians is helping financial institutions in over 30 countries to fight fraud. More than 60 banks, including UOB Singapore and Pictet & Cie, rely on NetGuardians' smarter artificial-intelligence (AI) solution to prevent fraudulent payments in real time. Banks using NetGuardians' software have achieved reductions of up to 83 percent in false positives, reductions up to 77 percent in operational losses, spent up to 93 percent less time investigating fraud, and have detected new fraud cases.

NetGuardians therefore specialises in delivering smarter AI that prevents banking fraud. The firm boasts an incredibly powerful analytical platform underlying it and the managed learning process on which it then builds packaged solutions for particular subject domains, particular banking domains and particular problems.

Marini explained that by leveraging big data analytics and AI to help try to understand the way customers transact or employees work within the banks, to prevent both internal fraud, payment fraud and digital fraud, the firm has grown its solutions and offices around the world, with its HQ for Asia Pacific in Singapore. "The major elements our customers are focused on when we talk to them," he reported, "is obviously how do they prevent fraud, but also how do they lower the false positive rates and how do they make that investigation process as easy and as simple as possible, and therefore protect both their revenue streams, their brand, and obviously the customers money. And that is precisely what we dedicate ourselves to."

NetGuardians takes the view that this problem – at scale – can only be realistically tackled effectively using Artificial Intelligence, specifically machine learning techniques, and has therefore developed class-leading machine learning techniques. And the firm believes it has a key role in democratising the use of AI for real-time fraud prevention, focusing on simplifying the tasks at hand for our customers, and delivering value by preventing more fraud, more rapidly, with fewer false positives.

The need is now not just for intelligent AI models but explainable AI models. But it does not stop there, as customers dealing with alerts also need powerful investigation and forensic tools and associated dashboards and management information. NetGuardians' use of AI enables the delivery of accurate insights to these users' screens and memory banks.

The firm employs proven models and methods in a way that are as simple to manage as possible, and as quick to deliver value by stopping fraud. At NetGuardians they do this by providing powerful AI and standardised machine learning models proven to work, across different types of banks, across regions, for both known and emerging fraud threats. All without the need for in-house data science expertise at the banks themselves.

AI can augment and improve on the current protocols generally employed by banks to root out non-compliant transactions and clients. The main limitation of the wealth industry today is the lack of scalability, it cannot keep hiring people endlessly, infinitely in order to solve the challenges of all the new rules that keep coming, non-stop. Moreover, the more people there are, the greater the risk of mistakes, and not actually in real-time. This is why NetGuardians knows that banks must embrace technology; they must move faster and more efficiently, especially in a world where instant transactions are the new norm.

And here is where AI can make a dramatic difference. Rules-based protocols are no longer valid. When there was far less data, the rules-based system was acceptable. But the complexity has magnified exponentially, and the rules-based system creates far too many false positives and as a by-product has created financial impact for some institutions and reputational damage, as well.

But AI offers the opportunity to use the enhanced computer power available today to handle the vast proliferation of data. NetGuardians can analyse several years of information in moments, whereas ten years ago it was simply not possible, logistically or financially. But with new AI solutions today, which also learn by themselves, by the way, they can in real time achieve the results we all seek, away from the static rules-based systems that are now defunct.

The machine can learn about the habits of individuals, employees and other and detect suspicious transactions. It can analyse transactions over several years; it can build dynamic profiles and then keep those profiles up-to-date in real-time. It can then compare transactions with the customer/user profiles and thereby compute a risk score and take a decision.

Real-time solutions that can automatically change dynamically are therefore the way forward. As NetGuardians can help the banks and other organisations compare transactions in real time from groups, from customers together, from individuals and thereby compute more accurate risk scores, they are making the system and process far more effective and cost-efficient. Now, with this advanced AI, they can help the industry see where there are deviations amongst individuals, corporates and so forth, in relation to their peers. They have, in short, a far bigger picture, a broader vision, and we can truly compare on multi-dimensional axis, and they can keep learning. Artificial intelligence keeps improving all the time and is a fantastic tool for tackling this problem head-on.

**In your view, is financial sector fraud increasing in Asia, and if so since when and why (briefly)?**

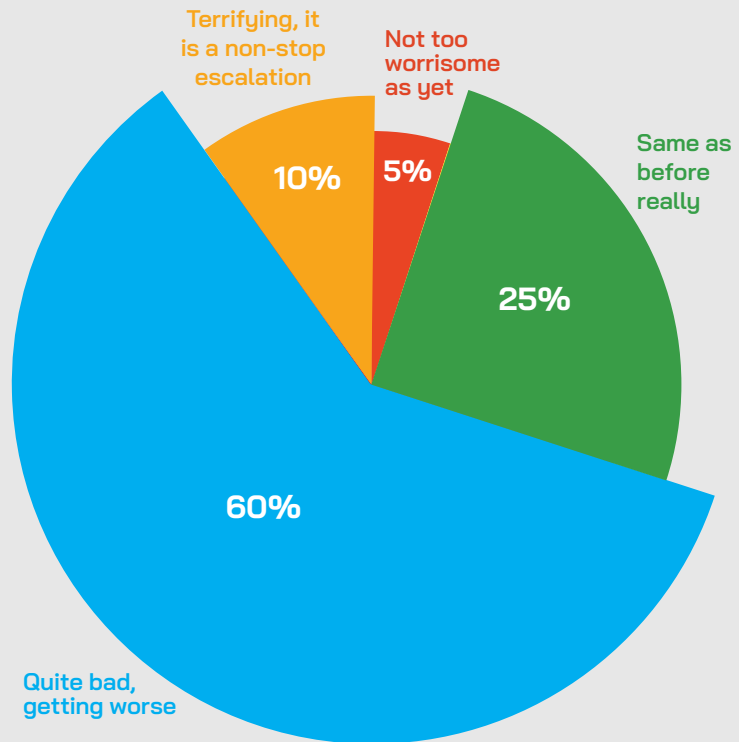
We received many replies to this question. There is no doubt in the minds of the finance industry practitioners in this region that fraud and the sophistication of the attacks had increased dramatically in the past five-plus years, particularly as digital banking has become so prevalent, and as more and more transactions and communication are taking place online or via smartphones and tablets. One reply also referred to the 'lackadaisical' attitude of users. The respondents called for better cybersecurity in the region and for the Big Tech businesses to step up their internal efforts to complement and assist the authorities in the region to combat and prevent such activities.

Since the pandemic hit, there has been ever-greater pressure to accommodate digital banking and online transactions, opening the door even further to the criminals who are smart and prey on the emotional and psychological needs of individuals, who are especially vulnerable during times of personal financial stress. .

**Do you think that banks, private banks and wealth management firms are well protected against fraud, or is it all moving too fast?**

The replies here indicated that the banks and the wealth firms of all types are all pumping up their compliance and IT resources, and there is a far greater awareness of these issues, and meanwhile,

**HOW WOULD YOU CHARACTERISE FINANCIAL SECTOR FRAUD IN THE WEALTH INDUSTRY IN ASIA TODAY?**



**TO WHAT EXTENT DO YOU THINK REMOTE WORKING PRACTICES HAVE ADDED FUEL TO THE FIRE?**







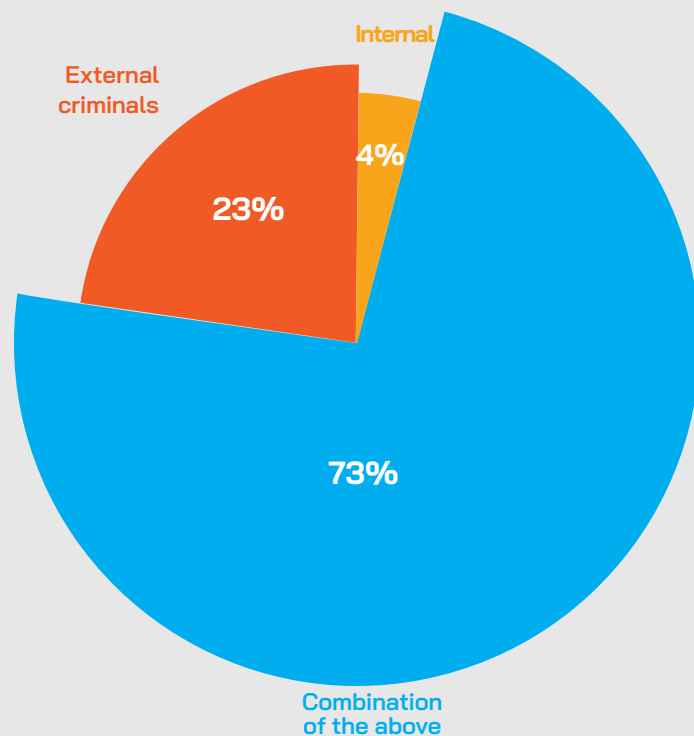
the authorities are boosting their initiatives. There appears to be a general optimism that combined with the arrival of more sophisticated digital technologies, including AI and ML, the industry can keep the lid on the worst threats, both internal and external. However, it is also clear that more investment is required, and more focus needed to keep up with the criminal, whose innovation and determination appear limitless. The external threats can be mitigated by better monitoring, better hiring, better internal systems and processes, and by regular outreach to the clients/users and enhanced education about the threats and

the ways such weaknesses are exploited by the fraudsters.

**Has your bank or wealth management firm been significantly increasing its defences against fraud in recent times?**

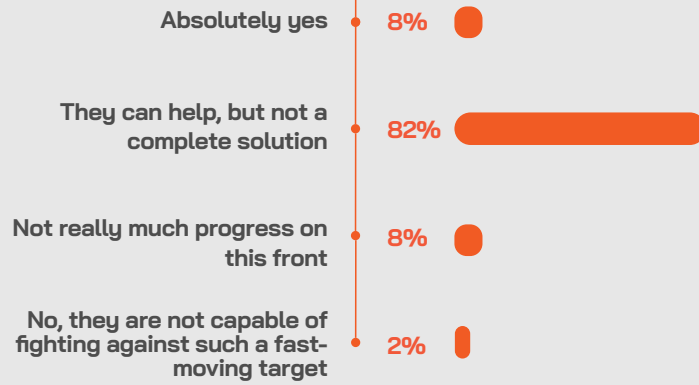
There was an emphatic 'yes' voiced by all respondents here, with replies listing a host of ways in which their organisations and the industry, in general, are upping their games, boosting investment, improving processes, technology, monitoring, outreach, and also enhancing communication with the authorities and with the digital solutions businesses that can help them fight back.

**IN YOUR VIEW, ARE THE DANGERS POSED MORE FROM INTERNAL OR EXTERNAL THREATS, OR A COMBINATION?**





**ARE DIGITAL TECHNOLOGY, AI AND ML SOLUTIONS CAPABLE OF FIGHTING BACK AGAINST FRAUD?**



**HOW WELL IS THE WEALTH INDUSTRY AND THE AUTHORITIES COORDINATING TO TACKLE THESE ENORMOUS PROBLEMS?**



### VERY BRIEFLY, WHAT SHOULD THE PRIVATE BANKING AND WEALTH MANAGEMENT INDUSTRY DO TO DEFEND ITSELF AND CLIENTS MORE ROBUSTLY?

#### We have summarised some of the replies below:

- » Strengthen fraud risk awareness, imbed fraud signals or rather fraud checks into operational systems, trading or reporting systems. Increase '4 Eye' meetings (where possible, schedule online client 'visits' by senior management or client advisor supervisors.
- » Boost education of employees and client regarding fraud and its manifestations.
- » Develop contingency plans and resilient measures so that in case of system breakdown, financial institutions will still manage to provide services and recover in time.
- » Implement more sophisticated fraud surveillance tools.
- » Training, awareness, continuously test processes and teams.
- » Perform trend analysis following incident reports and strengthen controls.
- » Risk management and fraud mitigation have risen to the top of the agenda and are moving decisively towards predictive and preventive fraud-protection tools and procedures.
- » Be up to date with the threat, anomalies and technology, be transparent on what you are doing to protect the customers' interests and share best practices to overcome any gaps/weaknesses.
- » Communication is required with the clients on the need to protect their bank account information, transaction activity and to keep a close lookout for suspicious transactions and communication.
- » Focus more on the character of the people you hire.
- » Educate staff (through training) and clients (through workshops or digital dialogues) to recognise fraud and scam activity and advise how they should then react, and offer them easy access and simple processes for reporting such suspicious activity.
- » We need more and much better procedures for verifying accounts and transactions.
- » More background surveillance.
- » Implementation of AI-Driven Technology.
- » Invest in the latest technologies. Keep abreast of the latest threat and prevention developments.
- » Try to create a culture where there is less turnover of RMs and other key staff, so that clients are familiar with their RMs and other key people they might be dealing with.
- » Divert more resources towards cybersecurity along with proper legal and compliance initiatives.
- » Make sure the primary corroborative evidence of client's source of wealth is obtained during onboarding the client, and make sure that client's net worth is supported by documentation, and all the supporting should be verified and recorded.