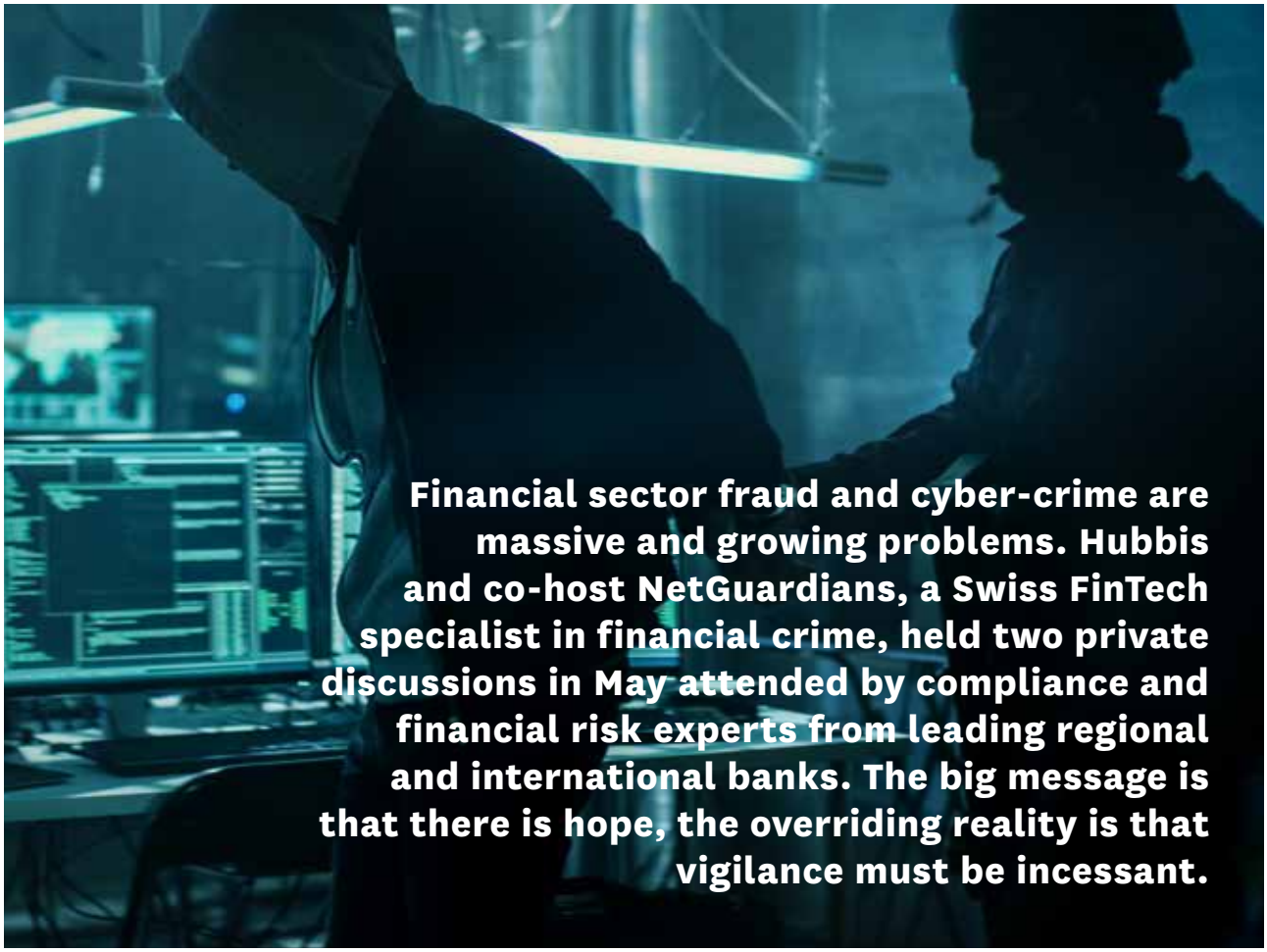
Financial fraud and cyber-crime: New horizons in financial crime prevention



Financial sector fraud and cyber-crime are massive and growing problems. Hubbis and co-host NetGuardians, a Swiss FinTech specialist in financial crime, held two private discussions in May attended by compliance and financial risk experts from leading regional and international banks. The big message is that there is hope, the overriding reality is that vigilance must be incessant.

Executive summary

Financial sector fraud and cyber-crime are massive and growing problems. Hubbis and co-host NetGuardians, a Swiss FinTech specialist in financial crime, held two private discussions in May 2018 attended by compliance and financial risk experts from leading regional and international banks. The big message is that there is hope, the overriding reality is that vigilance must be incessant.

The conclusion to both discussions was that rapid advances are being made all the time by the fraudsters and that 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, money-laundering and all the other segments and sub-categories of financial sector 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 - soon approaching two billion - presents a vast challenge to the financial industry.

The shocking prevalence of criminals - whether serial or opportunistic - operating within financial institutions is another 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 carry out essential maintenance on the core banking systems.

But there is hope. Advanced antifraud 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 faster, tools to help financial institutions fight back.

But tech alone cannot solve this vast and ongoing predicament. Continual vigilance and the utilisation of a multi-faceted approach to technology solutions to cybercrime are essential.

Moreover, banks cannot tackle this problem alone; they must work with industry peers in a coordinated manner. They must bring in the best global expertise, those at the cutting edge of technology prevention and those who best understand the multitude of ways in which cyber criminals 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.

There is no single element of this technology that can solve the problem, it is the combination that will bring success. Combining AI, machine learning, dynamic profiling, mixing all this technology will help. But the reality is that there is no perfect solution, as there is never such a thing as 100% accurate data, or a total vision of the cyber criminals' intent and methodology.

The future is certain - there will be more cyber-crime. Those in the wealth management industry that want to survive and prosper must fight back with every tool available.

ESTIMATES FOR GLOBAL FINANCIAL SECTOR FRAUD in all its manifestations are truly mind-boggling, running into several trillions of dollars when factoring in internal fraud, external fraud, money-laundering and all the other segments and sub-categories of financial sector fraud and cyber-crime. The scale of the problem is therefore remarkably intimidating.

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. With the number of mobile devices expected to reach 1.8 billion globally by 2019 , for example, banks clearly need to look again at how they will tackle mobile device fraud.

There is also a shocking prevalence of criminals - whether serial or opportunistic - operating within financial institutions. It is no exaggeration to say that one of the most worrying categories of fraud risk that banks face walks through their doors every morning and sits down to work. The danger is so great because some highly trusted IT staff will always require 'super-user profiles' to perform their everyday duties or carry out essential maintenance on the core banking systems.

Hope... within reason

But there is some hope. Advanced antifraud 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 effective defence against the biggest fraud risks in banking. Big Data advances are moving so fast that there are ever more, and faster, tools to help financial institutions fight back.

Attendees at both events included top management in positions of immense responsibility covering compliance, fraud, investigations, financial risk, operations and AML (anti-money laundering) from leading banks based in the Asia-Pacific region.

Both discussions were entirely off the record and non-attributable. Topics covered included: suspicious activity detection and fraud prevention; reducing incidences of human error; keeping a lid on compliance costs; AI as a tool to fight financial crime; the reactive or proactive approach; managing the increase in channels

Hubbis - NetGuardians roundtable in Singapore

and therefore bank vulnerability; handling increased volumes; managing the increase in investigations of false positives; and prioritisation of the investigation of transactions that have been flagged as a coded violation.

Co-host NetGuardians, a Swiss FinTech founded in 2007 and now on a rapid growth path globally, was represented at both discussions by Raffael Maio, Managing Director APAC, COO & Co-Founder and Peter Marini, Sales Director, Asia Pacific.

At the Hong Kong discussion, the head of a global private bank who covers the Greater China area asked Maio to zoom in on exactly what topics he felt were most pertinent to the discussion and what types of solutions there are available for the multitude of fraud prevention challenges faced by the wealth management community in general.

RAFFAEL MAIO
NetGuardians

"Private banks and wealth firms, in general, are usually dealing with very large sums for individuals and their families and this can pose additional risks above and beyond the challenges in general retail banking. The risks are very real for all parties."

Crime, like a liquid, pours into every crevice

"Today's fraudsters have for example shifted their focus to the new online and mobile banking channels, pushing some estimates of the projected level of cybercrime to an astonishing USD6 trillion by 2021,"

Maio reported. "With the proliferation of digital channels in banking transactions there is an ongoing multiplication of risks for the service providers and opportunities for the fraudsters as each channel - mobile banking, internet banking and instant transactions - brings its own risks."

One attendee at the Singapore discussion commented that the fraudsters then use some of the money they steal to improve their technology, in some vicious circle of deceit. "This is why we are hoping to see benefits from AI and sophisticated machine learning technology," he said.

"We do not imagine it will entirely replace the human element, but it should, we hope, augment current efforts at financial crime

PETER MARINI
NetGuardians

detection. We provide augmented intelligence to banks."

Wealth managers beware

Maio focused in on the field of wealth management in order to further contextualise the discussions. "Private banks and wealth firms, in general, are usually dealing with very large sums for individuals and their families and this can pose additional risks above and beyond the challenges in general retail banking. The risks are very real for all parties."

The regulators are also watching closely, and the heavy onus of responsibility is on the banks and advisory community in general, so there is much to be lost in both money and reputation for getting this wrong.

"Scaling up on staff will not tackle these problems," Maio warned. "It is not failsafe, it can create further problems and the cost is prohibitive."

"Hence," Maio continued, "we believe technological solutions can dramatically improve the outlook for so many of the wealth management community institutions. Asia is a key priority for us and a huge growth market as many of the problems we are seeing across the globe are being replicated in this region."

Maio explained that NetGuardians has a unique approach developing the first augmented intelligence solution made for banks to proactively prevent fraud. We empower our clients by providing machine learning technology together with contextual information and great user experience.

Banks using NetGuardians' solution achieved 83% reduction in false positives, saved 93% of the time lost in fraud investigation, and prevented new fraud cases.

"Being Swiss by origin we have leading name clients at home from Tier 1 to Tier 3 banks and have been gradually spreading our services across the world as demand for our expertise proliferates."

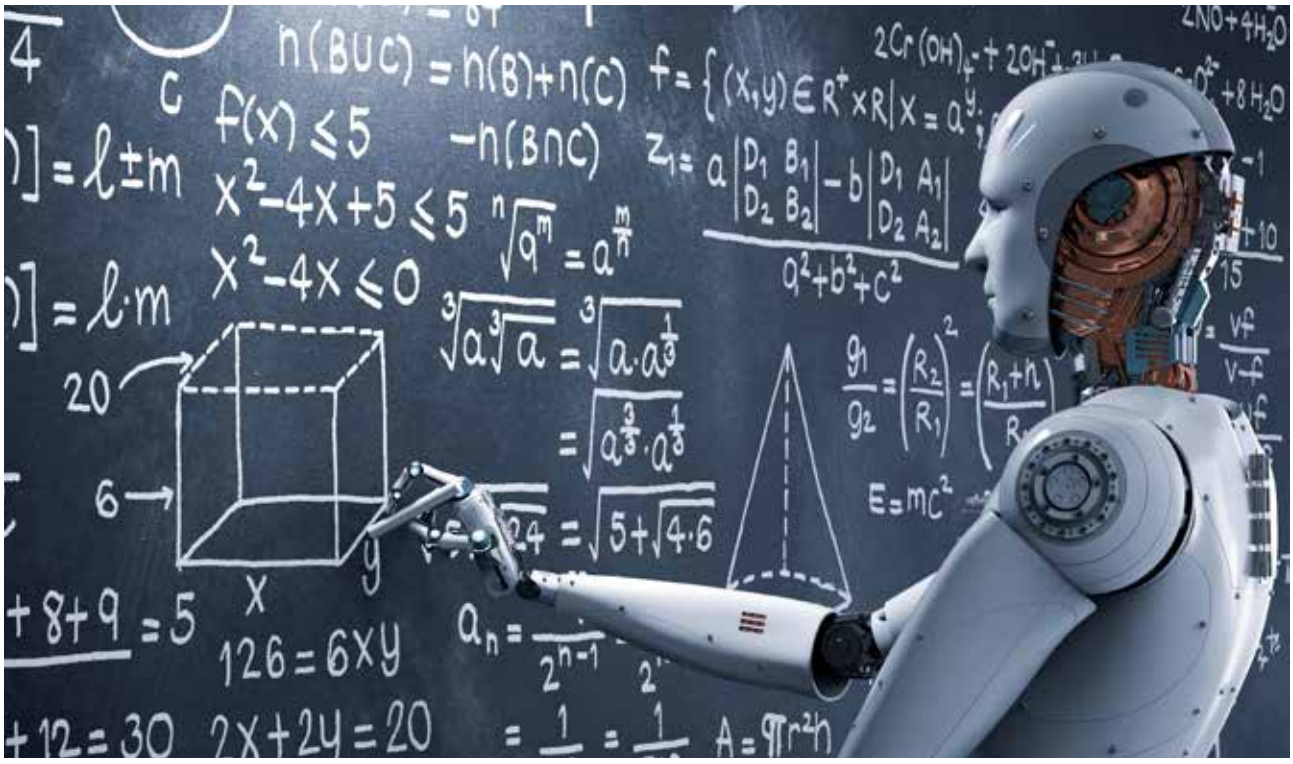
As the NetGuardians COO and Managing Director for APAC, Maio is primarily responsible for securing financing for the company, as well as for business development in Asia. Maio brings his technology experience from security software engineering, in environments ranging from a Silicon Valley start-up to a multinational product security company.

Technology to the rescue

The NetGuardians technological solution, Maio explained, covers every channel, meets the ever-increasing compliance criteria, minimises risks while providing a good customer experience, and protects banks' reputations.

"The only effective solution to detect and prevent fraud is to use technology that can monitor every transaction in real time and block the suspicious activity before the money leaves the account," Maio declared.

"Our enterprise risk platform keeps financial institutions safe



from fraud," he claimed. "By using advanced behavioural analytics and machine learning, our system correlates data from across a bank's entire IT system to detect atypical actions and raise alerts or block a transaction in real time, thereby stopping the fraud, protecting customers and avoiding hefty fines."

Maio explained that banks still largely rely on manual controls, human processing, sampling, and static rules to detect internal fraud. "The problem with this is threefold as we see it," he said. "Alerts are raised after the event, sampling is not failsafe, human processing takes time and is subject to errors and is itself vulnerable to fraud. What we offer is a new technological model that detects and prevents fraud."

Troubles within

Internal fraud carried out by bank employees is a huge global problem. Recent research Maio referred to puts the cost of banking fraud at around USD70 billion a year and cases involving bank insiders account for about 70 per cent of that total (Association of Certified Fraud Examiners, Report to the Nations, 2014). Bank employees are uniquely well placed to discover and take advantage of weaknesses in their organisation's internal controls, perhaps by abusing their level of access to the bank's IT systems or by targeting dormant accounts.

The NetGuardians enterprise risk platform uses big data and profiling to track the behaviour of all employees including front-office/back-office and privileged users (database administrators and IT administrators for example) and then block suspicious transactions. It automatically correlates data from across a bank's IT systems, channels and labels it, while advanced analytics trigger meaningful alerts in single-view dashboards.

Machine learning is a core element of the platform as machine learning algorithms constantly assimilate new data. "The number of false positives is kept to an absolute minimum," Maio explained, "thereby reducing the need for large risk management departments and maximising the use of resources. It is a cost-effective defence in the fight against fraud."

A positive approach to false positives

Compliance heads must also be constantly vigilant to ensure that their banks or their institutions are not being used for money laundering. "Money laundering transactions are estimated at a staggering 2% to 5% of global domestic product annually," Maio reported. "That is anywhere up to about USD2 trillion, a shockingly large number. No wonder the regulatory authorities require banks to do more to stop this criminal

behaviour. But constantly changing regulation is not the only problem banks face. With such vast sums at stake, the criminals keep reinventing themselves and their modus operandi."

Maio believes the NetGuardians' enterprise risk platform powers up dynamic profiling and machine learning to further empower the static rules to address the AML requirements the banks face day in, day out.

Looking for the unusual

"It builds dynamic profiles for each customer against which a bank can check every transaction, and in real time," Maio explained. "For wealth clients, it is also reassuring to know that new regulation can be accommodated easily and because our solution looks for out-of-character customer behaviour rather than criminal behaviour, the need to keep up with new money laundering techniques is reduced or eliminated."

Big Data today allows for data assembly and crunching on a scale unthinkable even ten years ago. "In the past," Maio noted, "we were profiling by category, so commonly banks might have several categories such as low, medium and high risk. But that proved insufficient as, for example, some clients considered zero or low risk might suddenly have some major activities or a major payment, which then generated red flags. So, we came up with the innovation of this big data technology that allows us to conduct profiling and behaviour analysis at the granular level, at the individual level. For every single customer or every single internal employee, we can create a profile, a behaviour."

Maio further explained that a payment he might conduct online from home will involve a system that knows his counterparties and knows what type of devices he might generally use for the transaction. "The system might for example also know my income and it can, therefore, identify what might appear irregular activity. Behavioural analysis can flag this sort of thing at a singular element of one individual, instead of doing it en masse where you cannot have the granularity to highlight the odd kind of behaviour of individuals."

Mind your behaviour

Maio also highlighted that there are other elements to creating a user profile, as technology is limited by technology. "You still need to have domain knowledge, you still need to really understand why a customer behaves in a certain way," he observed. "Sometimes, for example, you will have a personal banking customer mixed in with his business banking relationship and both behave very differently. It really depends on how you do segmentation of the data so that when you profile their behaviour you profile it in the proper way, and that takes a lot of time."

He explained that to address cyber risks there is cybersecurity. "You can have security in place in the form of the static controls but at the same time you are monitoring the transaction pattern, which is really the difficult part," he elucidated. "You can put in place antivirus, firewall, static control, but then the monitoring required is more dynamic, more difficult and presents many challenges."

Maio also explained that enterprise risk system is ring-fenced so that all the data resides at the bank's premises and there is no external information. "The information must be managed internally with the classical security policies and architecture within the bank," Maio noted.

"There is more and more hacking of phones and the bank cannot necessarily completely reassure itself that such and such a call to or from a certain number is bona fide."

Regulators – all questions, but no answers?

An attendee noted that in Hong Kong, where the first discussion was held, a very pressing issue is online fraud. He noted that the Hong Kong Monetary Authority has been eager to push out the TM-E-1 Supervision of e-banking circular and additional guidance on how to monitor the account level as well as the payment level, how banks identify unusual behaviour in customer bank accounts and also log-in behaviour is one of the things that the banks must pay lots of attention to.

Another attendee observed that the HKMA is facing up to one of the biggest challenges, namely endpoint security, but is asking more questions than it is giving recommendations or answers.

"They are leaving an open question for the banks on how to ensure customer devices are clean," he said. "A few years ago, they encouraged staff to follow BYOD [bring your own device] and now they are asking how we can ensure the devices are clean. They have lots of requirements and recommendations and reviews, but they have new interpretations each time and it all leaves us with a lot of open-ended questions. Banks are trying to overcome these challenges by trying to consolidate everything."

Maio remarked that every regulator focuses on what is required as proportionate to the risk that the banks are facing, the size of your operations, but the banks must decide on their own how they react and proceed.

"Yes," replied one participant, "the regulators have to play this role of always pushing the institutions to the limit in order to pressure them to do the maximum for end-customer and bank protection. Ultimately it is the banks that must comply while the regulators see their job as promoting the best standards."

Call-back a key protocol

Current guidelines for controlling external fraud might include call-back procedures. "But nowadays even this protocol is not fully safe," remarked one banker in attendance. "There is more and more hacking of phones and the bank cannot necessarily completely reassure itself that such and such a call to or from a certain number is bona fide. So, if there are some systems able to analyse previous patterns of outgoing transfers that would be immensely helpful."

He also noted that in some markets, for example, Europe, customers are mistrustful of call-backs for verification. "They feel like the bank is not trusting them," he observed, "but with the proliferation of fraud and the fraudsters' growing sophistication we are really obliged to do it this way."

The representative of a global private bank who heads up the North Asia region noted that her bank had prepared leaflets to educate clients as to the risks. "We believe the call-back is definitely a mechanism that can help us. We can also reach out to our correspondent banks to see if certain funds can be stopped once we spot an issue, so in this way we are also relying on the extended network as well.

Generally, if we spot a problem the process of calling back funds can be completed fairly rapidly, in days, not months. Here I am talking about SWIFT transactions."

Do you recognise me? Yet? Ever?

Voice recognition technology is one line of defence. Another might be codes or both protocols. "There are many channels of communication and we now use machine learning and behavioural analysis to help in these areas in order to more accurately understand what is normal

for a client, and accordingly we might spot when something is not right," Maio commented.

For example, in Switzerland there is a malware called Retefe that has been around for the last five years; it has evolved and is only targeting e-banking customers of banks in Austria and Switzerland. "Every day they get 10 to 90 victims and it is five years old already," Maio reported. "This is why AI can also help to augment realities and help spot out-of-the-ordinary activities. There are simply too many false positives today, too much noise."

Maio then elucidated on the concept of the code of violation. "There are different types of violation of false positives and it is important to know how to prioritise these. Fine tuning to find an optimum level of eliminating false positives to determine what transactions are a real trigger, real concerns." He highlighted one bank client of NetGuardians that runs 10 million e-banking transactions per year, with a team of more than 15 people just to handle false positives.

Reality check - scaling back the problems, not eliminating them

"There were about 250,000 false alerts in one year, all of which took a huge amount of resource and money to track through. They often have to check with customers many times a month and those clients sometimes get fed up, but it is essential to protect them. However, we have managed to help them slash the figure to 19,000, thereby providing a safer environment but also freeing up the time and resources of staff." Phishing and spyware are means for fraudsters to masquerade as customers, even down to presenting the bank with the correct signature for instructions and so forth.

"These oftentimes look very real," said one banker, "particularly for private banks with offshore clients, trustee relationships and independent asset managers, those kinds of relationships."

"Phishing emails to hone the perfect defrauding email is now a science that fraudsters have made into an incredible industry," Maio noted. "Sometimes it can apparently take them a year or two to devise the perfect email and all too often, but for some tiny errors, they would succeed more regularly."

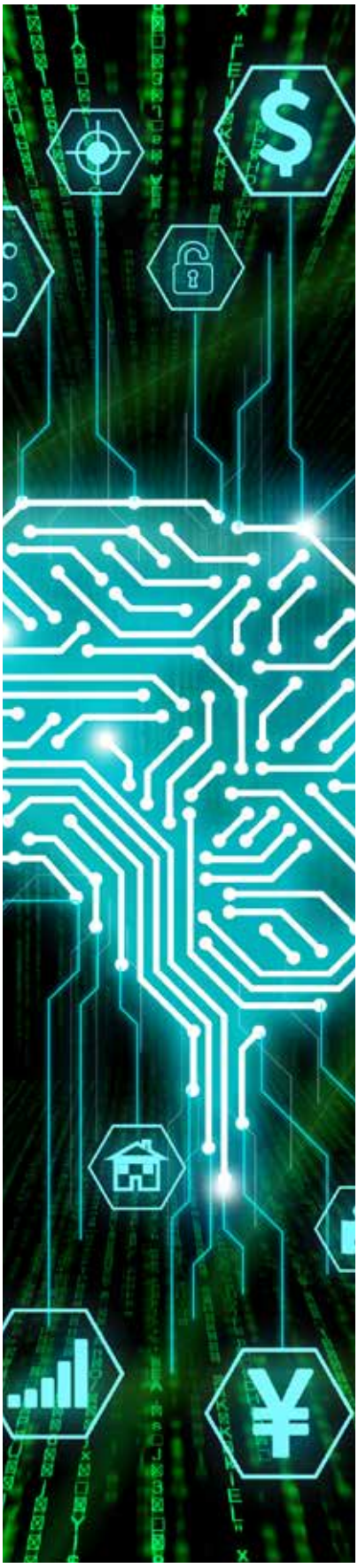
Attendees were asked to give their sense of how much that was flagged internally was coming in as false positives as opposed to real fraudulent activities. "It depends on the products and system," said one participant. Internal fraud might be 1 in 1000, whereas credit card fraud will be a higher accuracy."

Collusion and confusion

Another attendee observed that too often fraud is conducted with the collusion of an internal party working with external parties.

This problem has arisen often and can be related to contractors brought in, for example, to work on IT systems.

"We have seen this issue often in Switzerland," said Maio. "Leakage of data is demoralising all round. Unfortunately, the only productive way to protect the institution is to have a strict control and strict procedures, as well as a strong legal framework for working with different partners. A bank might outsource its data, but the liability remains with the bank. Strong contracts, being able to monitor your partner, conducting regular checks



and audits, all these can help." However," said one senior banker, "it is often difficult to do all this effectively because sometimes the offender can have subcontractors or consultants, so it becomes more problematic to keep tight oversight. Due diligence of the contractors and the outsourcing process and procedures is very important. Moreover, the same tight processes need to apply to internal contractors as well as employees, in other words, individuals that might be in the bank but not full-time staff." Staff turnover in private banks on the relationship, IT and compliance sides is also a key issue to address.

Constraining the risks

"All of these risks can also be constrained by the appropriate measures," Maio explained. "For example, one can track the attendance patterns of staff, who are there early, later and so forth. That helps spot any changes in these patterns. Will an employee do something that is detrimental to the bank because they are missing their targets? We look at all such data, including checking who is in and out of offices, who is on holiday and so forth. It is the ability to leverage this vast amount of data."

Marini noted that internal fraudsters act out of greed, but also because they thought that no controls were in place, so they thought they would get away with their crime. Accordingly, it is essential that organisations create a clear culture of processes so that internal fraudsters are deterred from even thinking about their crime. If the institution is watching internally, then the good employees will have no concerns; they realise that the institution is protecting itself, customers and employees at the same time.

"It is a fair statement to say that most people want to be proud of where they work," said one senior banker. "Having your company or your brand in the news because one of your colleagues has stolen money is never a good thing for employees. From the employee point of view, it should be seen as a positive that the company is trying to protect its brand, trying to protect its employees and customer. If the banks are losing money the chances are they might lose their bonuses or other perks."

"We have different solutions that tackle either internal or external issues," Maio explained. "Traditional solutions rely on patterns. This is a game of cat and mouse, you are always behind, waiting for something to happen. That is why today we see a growing tendency to rely more on a completely different paradigm using machine learning, artificial intelligence and so forth to be able to spot kind of the outlier without having a deterministic pattern. I am not saying that only one method is good but mixing these different technologies or different

paradigms should lead us closer to stopping the cybercriminal. But these cyber fraudsters can also use AI to battle back against us, so the key is to keep the gap between us as tight as possible."

Building skills to tackle fraud

Limitations include skills at the banks, Maio explained, as this financial crime 'industry' moves so fast. "Some institutions are lacking some skills as the fraudsters' technology has evolved so fast. Banks have to be cautious how they adopt new technologies to ensure that they can manage it all. Step by step is better, we advise. The goal is not to use 'sexy' new techniques just for the sake of the technology, but to focus on how the technology can serve the business, so we must be careful not to just jump into things, for example, Big Data.

We all need to keep in mind the business goals and to have a realistic view of technology implementation, in stages. Start smaller, build the skills, and then enlarge it."

Maio explained that the cost of mitigating unknown or unspecified risks is a challenge the industry faces, as it makes it difficult to ask for additional investment in defence protocols or technologies. Attendees conceded that they will never get to 100% protection or accuracy. It would be far too costly to achieve that, so there will always be some element of risk.

Be realistic, money and technology have limitations

"Many look at this problem and say how can we have 80% of success with only 20% of the cost," said Marini. "The customer, therefore, has to become part of the solution as well, so that is part of the education process, to get them involved in the solution. It is important to think that this is not an us versus them, the bank versus the customer, it is everyone combined to fight fraud."

"We all need to keep in mind the business goals and to have a realistic view of technology implementation, in stages. Start smaller, build the skills, and then enlarge it."

Maio reported that NetGuardians has its 'NG|Club' where the firm encourages customers to work together to solve some of the problems by sharing with each other. When one problem hits one country," he said, "it is never long before it springs up in another location." Attendees acknowledged that getting the appropriate spend on fraud and cyber defences can be tough. "We know we need the technology, but we also don't know how much it will really cost to succeed," said one attendee. "So, without knowing exactly where you end up with and how much it would cost in total over, say, the next five years, it can be a challenge to ask for investment from the management.

Another banker agreed. "Technology is something that we are looking forward in terms of applying to risk management or compliance, but frankly speaking it is costly from a management perspective, especially given the number of false alerts out there. Management is, therefore, a bit sceptical about the real performance."

The discussion homed in on some of the challenges facing AI and machine learning. One attendee of the Singapore discussion noted that AI in the medical field was dramatically improving diagnosis of melanomas, for example. The applications in other fields, such as financial services, are around the corner, but not so advanced, he observed.

"In the world of financial crime prevention, many hold out great hope that AI will filter out a massive amount of false positives, actually being able to close an alert, to determine that this is suspicious or not suspicious."

AI and machine learning – still evolving

"In the world of financial crime prevention, many hold out great hope that AI will filter out a massive amount of false positives, actually being able to close an alert, to determine that this is suspicious or not suspicious," said Marini. Confirmed through a case study NetGuardians conducted at one of their retail bank clients.

According to this study, compared to the previous control environment of the bank, NetGuardians' machine learning solution decreased the number of false positives by 83%. "But AI is not there yet. However, in terms of augmented intelligence then AI may be valuable in aggregating all the data, looking at all the analytics, and thereby helping the compliance officer make the final determination. I do not think, for example, that a major regulator will want AI to be making all the decisions on these matters."

"We certainly have to be realistic about where AI is right now," added another expert. "Currently it is helping but not controlling decisions, taking over jobs that are relatively painstaking and lower added value. We must be aware that there is perhaps more hype than real advances that will revolutionise our activities." Another panellist noted that a hindrance to AI was the application to existing systems, whereas perhaps what is required is a whole new way of looking at these matters.

Freeing up the human capabilities

"My compliance officers, particularly the more experienced ones, just do not have enough time to look at specific transactions," said a senior compliance and risk banker. "AI is an enabler at this stage to reduce the amount of work, because in the world of AML, for example, we need to process this within a reasonable period of time to meet regulatory requirements.

If I can help free up these team members, then the technology is playing its part, as we can refocus the team on more valuable challenges. In the future, for example, I hope to be able to focus only on higher-risk categories of clients. This will help us identify major fraud or inappropriate activities much more efficiently."

One banker commented that AI needs to support transaction monitoring, as well as producing a more productive alert. Another attendee highlighted the importance of the client experience, for example of someone who travels extensively on business but who bank or banks sometimes blocks his cards as he is moving rapidly across jurisdictions.

"AI and machine learning should be able to help in this regard, identifying unusual rather than more typical behaviour," he said. "Sometimes, it seems the checks are more about protecting the bank rather than thinking about the consumer of our service." AI can certainly be useful in helping to connect with the dots on things that seem disparate and disconnected, with the end result of weeding out many of the false positives and freeing up time and money all around.

Living in the real world

Maio concluded the second discussion in Singapore by emphasising that advances are being made all the time by both the fraudsters and those fighting back.

He emphasised the need for ongoing vigilance and the employment of a multi-faceted approach to technology solutions.

"What we believe," he said, "is that there is no single element of this technology that is the key, it is the combination that brings success.

Combining AI, rules, dynamic profiling, mixing all this technology with the human intelligence and expertise will help you in your journey. ■