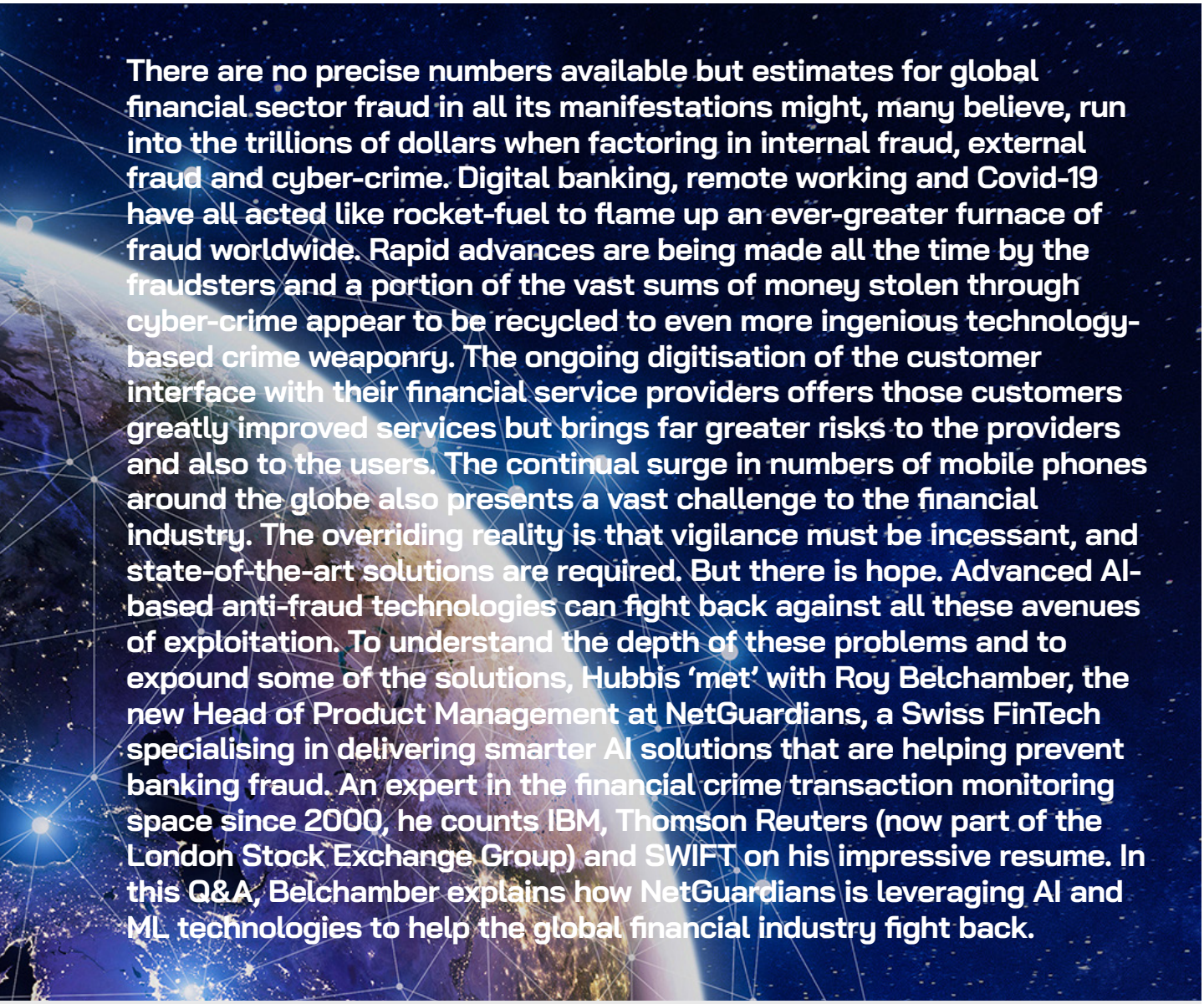
Global Financial Sector Fraud and how NetGuardians leverages AI and ML to Help Banks Fight Back



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. Digital banking, remote working and Covid-19 have all acted like rocket-fuel to flame up an ever-greater furnace of 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 appear to be recycled to even more ingenious technology-based crime weaponry. 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 users. The continual surge in numbers of mobile phones around the globe also presents a vast challenge to the financial industry. The overriding reality is that vigilance must be incessant, and state-of-the-art solutions are required. But there is hope. Advanced AI-based anti-fraud technologies can fight back against all these avenues of exploitation. To understand the depth of these problems and to expound some of the solutions, Hubbis 'met' with Roy Belchamber, the new Head of Product Management at NetGuardians, a Swiss FinTech specialising in delivering smarter AI solutions that are helping prevent banking fraud. An expert in the financial crime transaction monitoring space since 2000, he counts IBM, Thomson Reuters (now part of the London Stock Exchange Group) and SWIFT on his impressive resume. In this Q&A, Belchamber explains how NetGuardians is leveraging AI and ML technologies to help the global financial industry fight back.

GET IN TOUCH

View Roy Belchamber's LinkedIn Profile

Find out more about NetGuardians

ROY BELCHAMBER
NetGuardians

"Over the years that I have discussed these issues with those key people in banks tasked with addressing the fraud problem, it is incredibly clear they are struggling. Not only with the magnitude of the task at hand, but with the tools they have to hand. They want and need effective solutions, urgently and comprehensively."

Can you briefly explain what NetGuardians is and what you do?

NetGuardians is a leading Swiss FinTech that first launched in 2007 and currently helps more than 60 Tier 1 to Tier 3 banks worldwide combat the threat posed by financial crime. Financial sector fraud and cyber-crime are massive and growing problems. 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 seems to be recycled to even more ingenious technology-based weapons of attack. We bring in the best global expertise, and provide banks with solutions that are at the cutting edge of technology, and leverage our deep understanding of the multitude of ways in which cybercriminals can penetrate organisations.

We present solutions that leverage on AI technology. The eradication – through AI technology aligned with smart 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.

You recently joined NetGuardians. Why? And what is your background?

Yes, I arrived here in February to take control of product management, which, in an over-simplistic way, is sitting between customers and developers, making sure that we build the right solution that solves customer problems, that we articulate and communicate what we're doing to our existing clients, that we build the right products for them, and that we're creating solutions of real value and impact.

It is an exciting time to work in this arena. Capabilities exist now that I could only have dreamed about 20 years ago; compute power offered by advances in technology the cloud, the establishment of proven yet innovative techniques, collective modelling, collaborative data sharing, and much more besides.

I most recently came to NetGuardians from SWIFT in the UK, where I helped develop the Financial Crime & Compliance team to help define and deliver the SWIFT real-time, private cloud-hosted payment fraud prevention service, prompted partly originally by the massive Bangladesh central bank heist some years back.

Hubbis: What is the scale of financial sector fraud worldwide?

It is vast, nobody knows the exact numbers, but estimates for global financial sector fraud in all its manifestations, when factoring in internal fraud, external fraud, and all the other segments and sub-categories of financial sector fraud and cyber-crime, is more likely to be in the trillions of dollars equivalent than hundreds of billions globally.

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 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. The continual surge in numbers of mobile phones around the globe – now in the billions - presents a vast challenge to the financial industry.

And the future is certain - there will be more cyber-crime. Those in the financial sector, and specifically for your market, the wealth management industry that want to survive and prosper must fight back with every tool available.

Briefly, what has changed in the past several years in the world of financial crime?

A lot has changed, even in just the past five years. The fraud threat is obviously far greater and across almost all problem domains. Fraud never disappears, but targets shift. The skill, the innovation, the sophistication and the sheer adaptability exhibited by our adversaries is mind-boggling. The pace of change is enormous. Fraudsters have a supreme ability to innovate in their attack vectors and techniques. Attacks are created, deployed and scaled at an almost unfathomable pace. Specialisations exist, and marketplaces connect these specialists with others with frightening efficiency.

This all means that 'Fraud as a Service' is now a practical reality. As with elsewhere, their business has moved online. Just as the targets have - the shift to digital, accelerated by the pandemic.

"AI offers the opportunity to use the enhanced computer power available today to handle the vast proliferation of data. We 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, we can in real time achieve the results we all seek, away from the static rules-based systems that are now defunct."

Over the years that I have discussed these issues with those key people in banks tasked with addressing the fraud problem, it is incredibly clear they are struggling. Not only with the magnitude of the task at hand, but with the tools they have to hand. They want and need effective solutions, urgently and comprehensively. Back when I started in this area 20 years ago, rules were really the only game in town. Unfortunately, many of these solutions still persist today. These solutions are stressed by the scale of the fraud challenge we currently face, the pace of change and the sheer array of threats.

Specifically, has the pandemic made the prevalence of fraud more likely and more pervasive?

Due to the pandemic and remote working and the lack of face-to-face connectivity, we have all digitalised our lives and activities far more than ever before. We have so many people that were never comfortable online forced to operate digitally because there is no other option right now. And with remote working amongst the people staffing the financial institutions, it becomes ever more difficult to coordinate a response, meaning their defences are weakened. In short, there is a pot of gold and a massively bigger field in which to attack. Further, people, including the criminals, have more time on their hands, more time to scale those attacks, to create attack factories, to recruit mules at an industrial scale and to innovate in their attacks.

With the vast scale of the problem, and with the incredible agility with which these criminal act, what is needed exactly, and how can NetGuardians help mitigate these risks?

The word 'mitigate' is the right word, as the reality is that there is ultimately no complete solution; financial crime will not be eliminated, so it must be controlled by whatever means at our collective disposal. It is the sophistication of those numerous threats that is the true danger, as their skills, unfortunately, keep improving. The requirement today is for solutions that span more than just discrete, siloed slices of their business, solutions that can protect their

organisations not only from the typologies they already know of but also from future threats, as yet unknown, and solutions that are manageable, effective and efficient.

NetGuardians promotes itself as an AI-based solutions provider. Can you explain what that means and why you believe it so effective?

NetGuardians specialises in delivering smarter AI that prevents banking fraud. We have a very, very strong analytical platform underlying it and the managed learning process on which we then build packaged solutions for particular subject domains, particular banking domains and particular problems.

What seems evident to me is that this problem – at scale – can only be realistically tackled effectively using Artificial Intelligence, specifically machine learning techniques. This is exactly why I decided to join NetGuardians. I was impressed with the work on class-leading machine learning techniques. But more than this, with the practical, real-world focus. What NetGuardians is all about is 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.

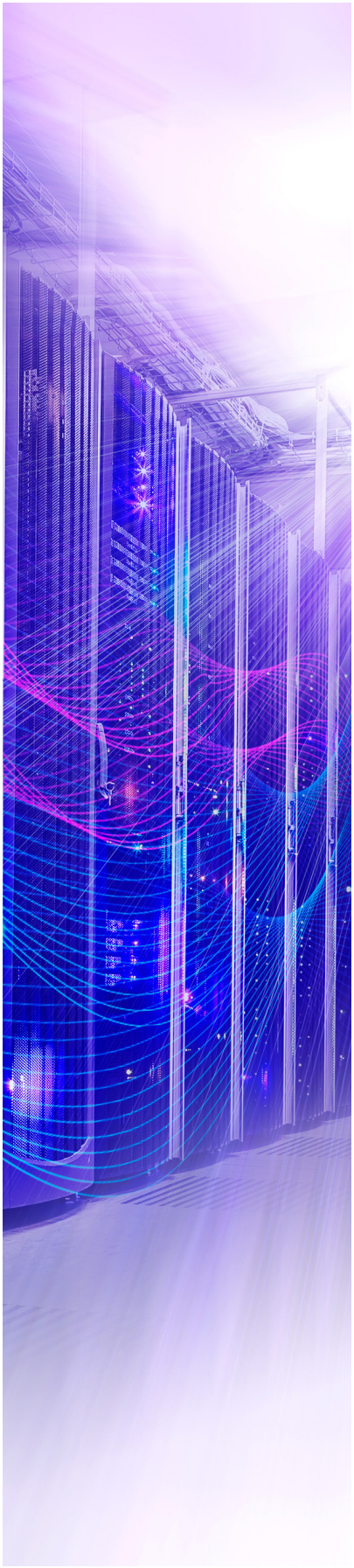
The need is now not just for intelligent AI models but explainable AI models. But it does not stop there, as customers dealing with alerts also need powerful investigation and forensic tools and associated dashboards and management information. AI enables the delivery of accurate insights to these users'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

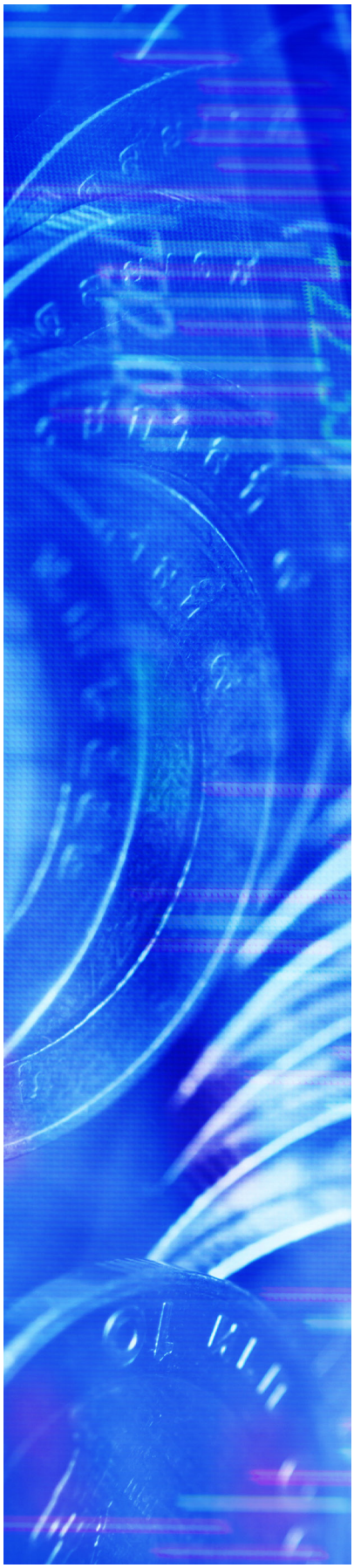
But above all, we need to do this using proven models and methods in a way that is as simple to manage as possible and as quick to deliver value by stopping fraud. At NetGuardians we do this by providing powerful AI and standardised machine learning models proven to work, across different types of banks,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

Could we mine down a bit further into the NetGuardians AI and ML solutions for the banks and how they are changing the older rules-based approach to these problems?

Yes, 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 this 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 banks are embracing 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. We 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, we 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 we can now compare transactions in real time from groups, from customers together, from individuals and thereby compute more accurate risk scores, we are making the system and process far more effective and cost-efficient. Now, with this advanced AI, we can see where there are deviations amongst individuals, corporates and so forth, in relation to their peers. We have a far bigger picture, a broader vision, and we can truly compare on multi-dimensional axis, and we can learn. Artificial intelligence keeps improving all the time and is a fantastic tool for tackling this problem head-on.

Is regulation helping or hindering?

Fraud is not like some other areas of financial crimes, so AML for example is very much wrapped in regulation today. But fraud does not have as much black and white regulation. And thus far, there is not really any cross-jurisdictional coordination in all this, despite everyone being aware that this is such a vast threat.

When we look across what authorities and regulators are doing, central banks and beyond, and there is a degree of regional disparity that certain jurisdictions that are taking the lead in many ways, and Singapore is a good example of that with MAS. They recently published a new paper that includes specific views on the fraud risk for financial institutions. Since they last published this some years ago, the focus has shifted from cards to online transactions, centring on the identification of abnormal activities, device characteristics, and so forth. The key here is the recognition of the threat.

In the UK, the Royal United Services Institute launched a paper in January specifying fraud as a national security threat, which is powerful wording and, in my view, an accurate assessment.

What sort of actions and steps should the banks be taking, and what are some best practices you would recommend?

If we think about the impact of Covid-19, staff working from home, and also the fraudulent attackers working from home as well, you need to have tools that are available to your teams at the point to which

they work. It is not just about being able to identify the abnormal, identify the frauds from the non-frauds, but to be able to understand why that is the case. Accordingly, they and we need to be able to present and articulate the results of the machine learning, the AI models to others in a way that's explainable, and in a way, that's easy for them as internal fraud investigators to understand, comprehend, navigate, and then also if necessary, to drill down into forensically. So, essentially, what you need to do is to be able to provide the insights to those users against what are quite often complex behavioural patterns; you need to be able to provide those insights to their fingertips.

I should add that there is so often a disparity amongst the different business lines within those banks, different systems, the data may be potentially siloed within those systems, and they are often forced to use tools that are not necessarily at the cutting edge. They are often unaware of some of the many threats, internally and externally. This is even more the case since remote working exploded last year. If you haven't got a solution, if you haven't got a system or an approach that will understand and be able to adapt to and identify those emerging fraud or threats, then you create a major exposure for the organisation.

At the coalface, you must therefore have the vital tools that can balance effectiveness and efficiency and not be faced with a plethora of false positives. You need to have tooling also that allows you to understand when something is triggered, why it triggered, and to assist in the remediation of that as well as the downstream resolution of any implications of that, any impacts, customer or beyond.

Looking at the big picture, there is a broader recognition required that we must increase collective engagement across the industry. This means more sharing bank to bank, if not necessarily hard data sharing but at least sharing information about threats. We should see more sharing of the specific actions against those threats. Banks are tasked with an almost impossible task in terms of educating customers about the threat as well as acting as the last line of defence against all these threats. Additionally, you should be publicising internally the threats averted and the achievements made.

Looking ahead, is there any cause of optimism?

Yes, I am optimistic, having been in this line for over two decades. We have more and more sophisticated solutions around transaction monitoring, using AI techniques, machine learning techniques, biometric, and so forth. These tools can increasingly help banks identify and then address the threat, even though that threat is escalating, modifying and adapting.

We also see a recognition amongst the authorities and regulators that the problem is real, and that it needs to be addressed. I think we're seeing increasing evidence of a willingness to consult, not only within the industry, with your peers across the industry, but also public-private partnerships, information sharing, data sharing; all of this is absolutely necessary when you think about the burden that compliance with regulations and compliance with addressing this fraud threat represents.

Today, it is not unusual in the slightest for financial services firms to spend 10%, or even more of their overall budgets on compliance. The reality is that's an almost unsustainable burden. So, the combination of tooling, the combination of kind of consultation and support from your peers and collaboration across the industry, all these elements could hopefully reduce that burden and increase the effectiveness in tackling that threat."

In short, there is most definitely hope, and I remain optimistic that the collective effort of the technology boffins, the anti-fraud industry, the regulators and the banks and other financial sector practitioners can fight back and keep this type of crime under control.

As I indicated, it is idealistic to imagine we can win each and every battle, but we are ahead in the war, and we plan to remain there in the years ahead. we are also evolving at lightning speed, and my mission at NetGuardians is to help make sure we are solving the problems today and looking ahead to the problems and ongoing challenges of tomorrow. ■