STRATEGIES TO FIGHT NEW FRAUD AND MONEY LAUNDERING SCHEMES

Lisa Wyver and Gerard McDonnell of SAS on Detecting and Preventing New Scams

ISMG INFORMATION SECURITY MEDIA GROUP

With the rampant surge of fraudulent schemes hitting the world at the moment - including the creation of fake cryptocurrencies, bank websites and investment scams - a more dynamic and holistic approach to detection and prevention is mission-critical for banks and regulators.

Lisa Wyver and **Gerard McDonnell** of sas looked at the source of these scams, highlighted the relationship between fraud attacks and subsequent money laundering schemes, and explained how "joining the dots" between them dramatically improves the fraud detection rate for banks and identifies money launderers with unprecedented accuracy.

In this interview with Information Security Media Group, Wyver and McDonnell discussed:

- New fraud schemes and how they work;
- Why fraud and anti-money laundering departments often work in silos and the problems this separation creates;
- How financial institutions can better join the dots for more effective scam detection.

SOPHISTICATED SCAM ATTACKS

ANNA DELANEY: Lisa, we have seen a huge surge in the creation of fake cryptocurrencies, bank websites and investment schemes. Can you share examples of these new scams?

LISA WYVER: We're seeing a lot of cryptocurrency investment scams, typically on social media platforms. There are usually false endorsements attached from trusted people and organisations and there might be some initial returns, but the customer is gradually manipulated to pay out more and more money. In the scams we're seeing, the particulars are new, but they boil down to the same things we've seen in the past. The

"We're seeing a lot of cryptocurrency investment scams, typically on social media platforms. The customer is gradually manipulated to pay out more and more money."

– Lisa Wyver

criminal is trying to build trust with the victim or to stress them and make them panic. Then, the criminal uses that trust or panic to harvest the victim's details or get them to make the payments themselves.

GERARD MCDONNELL: While the initial concept for scams has stayed the same, the sophistication and the style of scam attacks have changed over time, particularly since the pandemic. There are some quite sophisticated efforts going on around the region.
One extreme example is a fake cryptocurrency that was being advertised in Saudi Arabia called the CryptoRiyal. It pretended to be a cryptocurrency funding Neom, which is a big development in Saudi Arabia, so it's a source of national pride for the locals, and the young locals particularly. CryptoRiyal played on that sense of national pride and the urgency to do something for their country, but also to be part of cryptocurrency and the wave of quick money coming into the world. CryptoRiyal came from a shell company in Singapore, and it caused inter-country issues. So, we're not just talking about scam attacks fooling people but complicated money laundering schemes through shell companies going on as well.
Another scam that was quite popular in this region is "crazy rich" Indonesians in Jakarta – a couple of young guys who were getting rich through a trading app, became celebrities because they were driving around in Lamborghinis and flashing all their money. They became almost household names. Then, they were caught overnight because it was all a fake scheme where they were inspiring people to invest in the fake money arrangement that was making them rich. So, they shifted from designer suits to orange prison suits.

HOW SCAM CENTERS WORK

DELANEY: Gerard, let's dive into the operations of these schemes. Where are they coming from, who's being recruited and how do they work?

MCDONNELL: In this region particularly, we see whole centers dedicated to scam attacks. These centers have been built up in special economic zones, which are on the borders, particularly in countries like China, Laos or Myanmar, but even off border in Cambodia, where they were originally casino areas for physical gambling. During the pandemic,

that stopped immediately. Then, it grew into online gambling casinos that were controlled by the countries and shut down. So they shifted to creating these scam centers.

The centers have blocks of flats in these special economic zones with small rooms where people are focused on carrying out scam attacks, like Macau scams. In this scam the scammer pretends to be an official telling you that you have a fine or some kind of financial obligation, and if you make a payment quickly you'll be out of trouble. There are also romance scams and job scams, and they're very targeted. They use a lot of local knowledge. They quite often involve human trafficking, where people are forced from other countries, particularly Thailand and Indonesia, and human-trafficked into either perpetrating the scams or helping orchestrate the scams with technologists. IT staff are also being human-trafficked and forced into labour in these zones.

The special economic zones are lawless. They have so much autonomy that even the local and regional police forces cannot enter them. They're starting to get a lot of international attention with human rights organisations now. The scam centers are connected to cryptocurrency schemes as well. The two have grown together. So, they already have a route to steal money from people and launder it through the cryptocurrency schemes or persuade people to invest in them.

WYVER: With the growing number of scam centers, criminals need places to facilitate money movement, so we're seeing a lot of recruitment for money mules. The criminals are taking advantage of people's financial difficulties. They're putting ads on job websites or social media or sending phishing emails, and they're offering people an opportunity to make some easy money. In some instances, the criminals scam the money mules into handing over their details, and they're becoming money mules without even knowing it. In the U.K., a growing amount of older account holders are now being recruited. They are more attractive to the criminals because they typically have more established accounts with the banks, and it's usually less suspicious when you see larger transfers happening from those accounts.

THE ROLE OF BANKS

DELANEY: Gerard, what responsibility do banks hold in the prevention of these crimes?

MCDONNELL: It's a real challenge because they're not the victims per se; it is the banking customers who've been fooled into doing this. Two types of fraud happen as a result of scam attacks. The first type is third-party account takeover. This is where somebody has been fooled into giving up their credentials, and the fraudsters then use those credentials to take over the person's bank account and steal the money from it. The second type is called authorised push payments. This is much trickier, because customers are fooled into making the payments themselves to what they believe is a worthy cause. In both cases, the

banks could argue that it's the customer's fault that they have been fooled into either giving up their credentials or making the payments.

It's been a challenge for many years to work out where the fault lies beyond the consumer. In the last few years, regulators have started to step in a lot more. We had two big incidents in Singapore and the Philippines in 2021 and early 2022, where hundreds of accounts were taken over as a result of a very fierce scam attack. Lots of money was stolen and moved into cryptocurrency accounts. In both of those cases, the regulators stepped up hard and put pressure on the banks. So now, the banks are being driven to potentially reimburse customers who are victims of account takeover.

In Singapore, a bank had to place $300 million in funds to mitigate the risk of these scam attacks until they believed they were in a position to defend the customers more. Of course, the only way they could defend the customers is by using technology. The use of AI and machine learning is interfering with transactions that are believed to be fraudulent. So, banks are being drawn into the fight by the regulators and sometimes by their own corporate social responsibility. And they're in an ideal position to interfere with the account or with the payments using technology. That's the key change I'm seeing.

NEW REGULATIONS

DELANEY: Lisa, what forthcoming regulations must financial institutions observe?

WYVER: In the U.K., the Payment Systems Regulator is bringing in some new requirements that will give the victims of these scams more protection. A number of banks in the U.K. are already voluntarily reimbursing customers under the Contingent Reimbursement Model. With these new requirements, all banks will be forced to reimburse the victims that fall in scope of the new regulations.

And reimbursement will be split fifty-fifty between the sending bank and the receiving bank. That is supposed to come into effect

"Banks are being drawn into the fight by the regulators and sometimes by their own corporate social responsibility. And they're in an ideal position to interfere with the account or with the payments using technology."

– Gerard McDonnell

next year. In Australia, the minister of financial services indicated that the country wants to force the banks to provide more appropriate compensation for victims. Australia is also looking at potentially doing something similar to the U.K.

MCDONNELL: This new fifty-fifty split concept that the U.K. has introduced was also on the back of quite a big scandal from an elderly customer of Lloyd's who lost over 150,000 pounds making a payment to somebody they believed was a worthy cause and turned out not to be. The bank was forced to make a repayment based on the grounds that the payer was vulnerable. So, now banks have to profile their customers to assess vulnerability. The regulators and the banks all around the world are watching how this fifty-fifty split concept is going and when it's going to come into their region.

The regulators are driving some big changes at the moment. Singapore has put a lot of pressure on banks. And the Philippines is driving banks to look at both money laundering and fraud because typically in a scam attack, a lot of money is stolen and then a laundering pattern emerges. The country wants banks to join the data together – join the dots – and see the bigger perspective. Saudi Arabia is driving banks with a very aggressive fraud maturity level requirement that was passed in June this year. The banks have to use technology to look at mule account activity and at the bigger picture to assess risk across the spectrum much more widely.

SCAM DETECTION CHALLENGES

DELANEY: Lisa, where are financial institutions most challenged when it comes to detecting these schemes?

WYVER: One of the main challenges is the lack of data, and that could be because of data silos. The information's available in the bank, but it's in different systems, held by different departments. Nobody's seeing the full picture. It could also be lack of channel-specific data, such as user biometrics, digital data and session data, which are key in

"Identifying where the money goes can dramatically improve your accuracy in identifying money that is being stolen. Getting a bigger picture can improve a machine's ability to detect fraud by up to 10 times."

– Gerard McDonnell

trying to validate remote interactions and in detecting scams. There are also challenges with skills and experience. Even if you have all of the data, you need to know how and when to use it. There can even be challenges in confirming the fraud once you've detected it. The customers are confident in the payments they're making. They don't think they're being scammed, so they're not going to confirm that for you.

AML AND ANTI-FRAUD SILOS

DELANEY: Gerard, Lisa mentioned data silos. Why do the teams in AML and anti-fraud departments still often work in silos, and what problems does this create?

MCDONNELL: Anti-Money Laundering departments are driven by regulatory demands and their objective is to comply with those regulations and to stop money laundering. Their role is not to interfere with the transaction but just to report a suspicious transaction to the regulators. So, their job is focused on compliance.

The fraud department is driven to be intrusive and to stop transactions on the fly. It uses a different approach and a different technique to detect and prevent fraud. The different approaches and the business drivers behind them result in there being two silos.

Identifying where the money goes can dramatically improve your accuracy in identifying money that is being stolen. Getting a bigger picture can improve a machine's ability to detect fraud by up to 10 times. And banks have a lot of data. Yes, there is a limitation with their internal data today, but they have the opportunity to take data from external sources. And device intelligence providers and company intelligence providers can enrich that data much more. Using that extra intelligence can dramatically improve the ability to detect fraud in real time and interfere with the transaction. So, more data and more views over a longer range dramatically improve the ability to detect everything and stop it in real time.

'JOINING THE DOTS'

DELANEY: Lisa, when looking at detecting and preventing these crimes, how can financial institutions better join the dots for more effective scam detection? And what methods do you see banks currently using?

WYVER: More data is definitely key. By sharing data across your organisation and adding in biometrics and digital data, you can make sure that you see a full view of the customer activity and all the potential risks. At SAS, we have completed a data study with two data providers. The first one was focused on biometric data, and the second one was focused on digital data. We just used the data out of the box and looked at the individual event, and we found that you could get 34% fraud detection rates just by using basic data points. That's pretty good.

We then put some analytics on top of that, which meant using that data, building features, incorporating data across the portfolio, and no longer just looking at that single event but at all the behavior in the past. With that, we added another 26% of detected fraud, making it 60% overall. The next key piece once you have all that data is building profiles using predictive analytics. Look at your customer, how they transact, what devices they're using and how they're using those devices, and use predictive analytics to anticipate potential fraud and enhance your decisioning processes.

A lot of the banks we work with are looking at unusual customer activity to see if there is an increase in the values of transactions or if there are new beneficiaries involved. There's more emphasis on deposit monitoring. They're looking at mule account propensity scoring and including more device intelligence in their rules and models. They're looking at simple things, like if your customer typically logs in with the latest iPhone and then suddenly the logins are coming in with an older version. Even that can indicate it might not be your customer.

A lot of banks are building up financial crime investigation units that look at financial crimes that are bankwide; they're combining their fraud investigations and their AML efforts. With all of that data, they can use link analysis to better connect all the fraud cases, look for more suspicious money laundering patterns, find things to identify high-risk customers, and use all of that as feedback to make their detection rules better.

Some banks are looking more into sharing intelligence via consortiums. The Fraud Exchange Reporting Platform in Australia allows the sending and receiving banks to share information quickly. That means they can stop further payments and try and recover funds more quickly. And the U.K. has confirmation of payee, which allows you to check your payee details and make sure that they're validated, giving you more confidence in that payment. These consortiums have great

"Make sure that you have a robust fraud reporting process. Ensure you have a system that enables you to use your data and analytics and customer profiles to make decisions in real time and take action to stop scam payments."

– Lisa Wyver

value because they allow the banks to achieve a lot more than they could on their own.

MCDONNELL: The whole becomes greater than the sum of the parts when we get to a more collaborative environment where multiple banks are sharing information. I see interest in this, as well as opposition to it. The whole idea of a consortium is to share more knowledge. The banks want it, but they're also nervous about sharing information. They need a mechanism to share it securely, maintain privacy and respect all the government regulations about protecting people's identity.

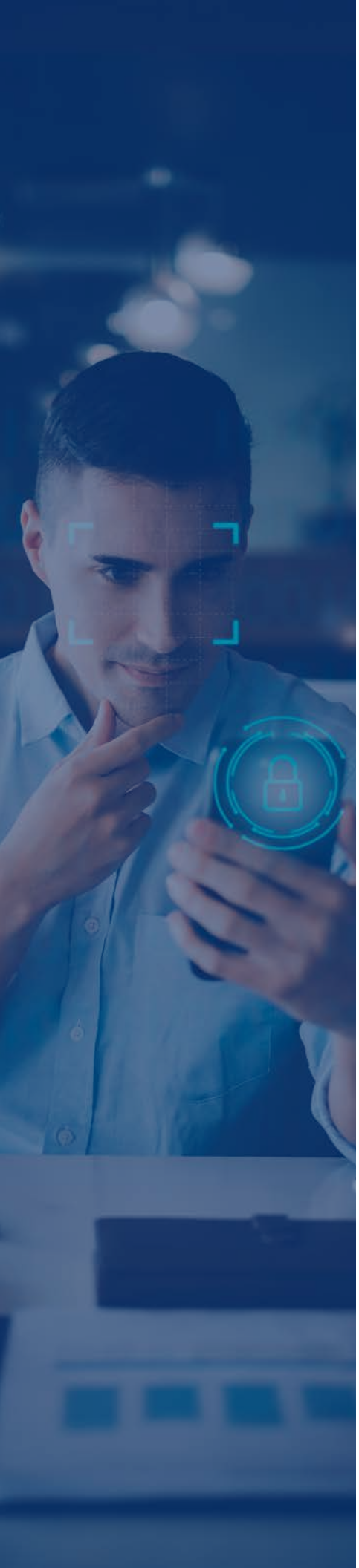
There are ways of doing this, and there are third-party organisations that help with it. So, the interest is there, and the value that they can get out of it is huge. It's another big step forward. I see it really happening in the next three to five years. And when it happens, it will beef up the ability to protect our consumers.

ADVICE TO FINANCIAL INSTITUTIONS

DELANEY: Lisa and Gerard, what additional advice can you offer financial institutions that are looking to develop strong anti-fraud capabilities and strategies?

WYVER: Make sure that you have a robust fraud reporting process. Being able to have accurate and reliable fraud reporting is an important piece of being able to drive good insights from your data. Ensure you have a system that enables you to use your data and analytics and customer profiles to make decisions in real time and take action to stop scam payments.

MCDONNELL: Do fraud maturity assessments to look at how ready your bank is to protect its consumers against scam attacks. Make sure the bank has access to all the data and has the processes and corporate policies in place to interfere as quickly as possible.



WHY SAS FRAUD MANAGEMENT?

Make faster, better-informed risk-based decisions across your organisation.

Our end-to-end fraud detection and prevention solution supports multiple channels and lines of business, enabling enterprisewide monitoring from a single platform. The solution simplifies data integration, enabling you to combine all internal, external and third-party data to create a better predictive model tuned to your organisation's needs. Bringing together this data on a single technology platform gives you the flexibility to scale up or out as your business changes and respond faster to new threats as they arise.

Find fraud faster and reduce revenue loss.

Stay on top of shifting tactics and new fraud schemes. Embedded machine learning methods detect and adapt to changing behavior patterns, resulting in more effective, robust models. Key technology components let you easily spot anomalies for each customer. In-memory processing delivers high-throughput, low-latency response times – even in high-volume environments – enabling you to score 100% of transactions in real time. Our patented signature-based approach captures customer behaviour data from multiple sources and analyses it for patterns and inconsistencies every time a transaction is processed.

Keep customer satisfaction high.

Better fraud detection capabilities and faster response times lead to fewer false positives, which translates to less customer inconvenience. When fraudulent behaviour is detected, alerts are scored and prioritised, enabling immediate customer self-service, or fast review and assessment, reducing the chances of wrongly declined transactions that would adversely affect the customer journey.

Learn more at: www.sas.com/en_au/software/fraud-management.html

ABOUT THE PANELISTS

LISA WYVER

Wyver provides fraud expertise to drive the enhancement, presales and business implementation of the SAS banking fraud solution globally with both current and potential customers. Prior to joining SAS in 2016, she spent over six years at HSBC, where she held a variety of roles in fraud analytics.

GERARD MCDONNELL

McDonnell has over 25 years of experience providing software solutions for fraud and security clients, particularly in the finance sector and governments in many areas around the world. Prior to joining SAS, he held various regional management roles for security technology companies such as Oracle, Sun Microsystems, Cross Match Technologies and Novell.

About SAS®

SAS® is the leader in analytics. Through innovative software and services, we empower and inspire customers around the world to transform data into intelligence. SAS® Anti-Money Laundering is a proven platform that takes the fight on money laundering and terrorist financing to the next level with AI, machine learning, intelligent automation and advanced network visualization. We help your organisation meet growing global compliance demands, enable better prevention and ensure superior detection and protection. SAS® gives you THE POWER TO KNOW.

About intel®

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io