AI VS. SCAMS: LEVERAGING TECHNOLOGY TO SECURE THE FINANCIAL ECOSYSTEM

ISMG
INFORMATION SECURITY
MEDIA GROUP

ABOUT THE SPEAKERS

Keith Swanson

Keith Swanson, Director, Fraud and Financial Crime, Asia Pacific-Japan, SAS

Swanson works with customers, partners, advisors and colleagues to help identify and define strategies and tactics on how technology, coupled with people, processes and data, can drive improved outcomes across anti-fraud, anti-financial crimes, waste, error, abuse and program integrity initiatives. His engagement crosses geographies and industries, in the face of ever-increasing risks posed by fraudsters, scammers and digitally driven engagement and immediacy. Swanson's experience spans roles across companies, consulting and advisory firms, and IT service providers, including IT, operations, administration, marketing, analytics, management and project management. This breadth gives him a unique perspective on driving outcomes through IT, analytics, data and AI-led change, value and adoption.

Shane Burnett

Shane Burnett, Global Solutions Advisor, Risk, Fraud and Compliance, SAS

Burnett is an anti-fraud professional with more than 15 years of experience in the finance industry. He has worked with organisations across Australia, New Zealand, Saudi Arabia, Thailand, and India, providing expertise in designing and implementing fraud detection software and operational strategies across multiple channels. In his role with the global risk, fraud and compliance team at SAS, he continues to collaborate with leading financial institutions worldwide, focusing not only on technical solutions but also on best practices in financial crime prevention, team structure and process optimisation.

Suparna Goswami

Moderator: Suparna Goswami, Associate Editor, ISMG

Goswami has more than 10 years of experience in the field of journalism. She has covered a variety of beats including global macro economy, fintech, startups and other business trends. Before joining ISMG, she contributed for Forbes Asia, where she wrote about the Indian startup ecosystem. She has also worked with UK-based International Finance Magazine and leading Indian newspapers, such as DNA and Times of India.

As scams become more sophisticated and personalised, banks face a different kind of threat, one that targets people rather than systems. From authorised push payment (APP) fraud to social engineering and impersonation scams driving identity theft and account takeover, customers are being manipulated in ways traditional fraud controls can't always prevent or detect.

Reducing scam-related losses is not just a matter of financial protection, it's a business necessity. Each scam incident undermines customer confidence, increases operational strain, and risks long-term brand damage. In an environment where trust defines loyalty, the ability to safeguard customers from scams directly influences profitability, regulatory standing, and competitive strength. Banks that demonstrate proactive protection not only reduce losses but also differentiate themselves as responsible, trusted partners in their customers' financial lives.

To meet this challenge, leading banks are having to reconsider how they redefine their detection to proactive prevention strategies to protect themselves and their customers, much of this powered by artificial intelligence and advanced analytics. By combining real-time risk scoring, behavioural analysis, and human expertise, institutions can detect early signs of manipulation, intervene before losses occur, and protect customers without adding substantive friction to their experience. Proactive scam prevention is no longer optional, it's a strategic advantage that preserves trust, reduces losses, and secures the future of digital banking.

This e-Book is based on the webinar AI vs Scams: Harnessing Technology to Protect the Financial Ecosystem, which explores how AI and advanced analytics are transforming scam prevention, enhancing, not replacing, human expertise. Discover how forward-thinking institutions are staying ahead of scammers while strengthening trust and delivering exceptional customer experiences.

EVOLUTION OF FRAUD TACTICS

SUPARNA GOSWAMI: How have fraud tactics evolved in the last couple of years, and are they getting more sophisticated or just more scalable?

SHANE BURNETT: It was just over 30 years ago that the average household first gained access to the internet. Since then, technology has advanced at a rapid pace, creating new opportunities for criminals to exploit. As technology continues to evolve, and with the growing potential of artificial intelligence, fraudsters have developed increasingly sophisticated methods and techniques.

Scalability has been one of the key outcomes of this evolution, enabling fraudsters to reach larger groups of potential victims with ease, however the most significant shift is in the growing ingenuity and creativity of these scammers. Criminals are using adaptive, targeted and personalised approaches to circumvent standard security defences. This is resulting in more convincing fraud attempts and making it harder for both the public and fraud detection teams to identify threats. The rise of technology shows how easily fraudsters can exploit open-source tools.

Even casual users, including children can use free apps to create convincing deepfakes. And if kids can produce such content for fun in a short period of time, then criminals with greater motivation, resources and possible financial gain pose a more serious threat in an already high-risk digital landscape. These threats are not in the distant future; they are current realities. But it's not all doom and gloom. All these new evolving technologies are not just for the fraudsters. It also provides the financial services industry, with powerful tools to stay ahead. They enable investigation teams to better respond to new and emerging threats, efficiently manage historical patterns and workloads and dedicate more time to focus on what truly matters.

AI AND ML FOR FRAUD DETECTION

SUPARNA GOSWAMI: How are banks responding to these developments? How are financial organisations using AI and machine learning to detect fraud or abnormal behaviours in real time?

KEITH SWANSON: The reality is that many organisations have been using AI for combatting fraud for years. When we use the term applied or traditional AI, we often talk about using machine learning models to score transactions about the likelihood of fraud. As AI and machine learning have advanced in capability, banks have also moved to real-time behavioural profiling to understand what is normal or abnormal.

As we move from that past to where we are today, scale has materially changed what organisations can do. Scale has allowed banks to look at more than just financial transactions. With advancements in technology, banks can look at nonfinancial transactions, session data related to interactions, and financial transactions.

Where scale has allowed us to move forward, is around real-time detection versus scale-enabled real-time interdiction. You might be able to detect a risk or a potentially fraudulent transaction in real time, but in the past, you might not have been able to block that money or that transaction from occurring. Scale has now allowed organisations to apply AI and do the move to real-time interdiction.

In the past, when scoring transactions, we might have looked at a single event - for example, asking whether a $10,000 transaction was fraud or not. Today, we can assess it within the broader context of an online banking session. We can analyse behavioural patterns: Was there a failed login attempt? A password change? The addition of a new phone number for two-factor authentication? A new payee? And finally, the $10,000 transfer itself? When viewed together, these events paint a very different picture - one that suggests an account takeover and a fraudulent attempt, rather than a simple high-value transaction that should be assessed on its own data and merits.

The reality is that the evolution of AI, from its early applications to where we are today, has been a long-term focus for us at SAS. For years, we've helped organisations apply advanced analytics and AI techniques such as machine learning, neural networks and network link analysis. Now, we're working with them to harness the latest generation of AI, including generative and agentic AI. Much of our work centres on helping organisations solidify the use of traditional, applied AI and move toward the new possibilities emerging AI technologies offer, combining multiple AI techniques and enabling real-time interdiction at scale through modern technology.

"AI currently has limited understanding of nuanced human communication elements such as sarcasm or subtle emotional cues, which can be critical in detecting deception."

– Shane Burnett

LIMITATIONS OF AI IN SCAM DETECTION

SUPARNA GOSWAMI: We all know that AI is powerful, but it is not a silver bullet. What are the current limitations of AI in scam detection, and where is human oversight still very critical?

SHANE BURNETT: Current limitations of AI and scam detection primarily stem from the rapidly evolving nature of the scams themselves. Just like humans, AI systems experience a lag in adapting to new fraud tactics. When developing AI models, they're typically trained on specific features. If fraudsters change their tactics and methods, and the identifiers for these new tactics are not included in the training data, AI may struggle to identify them in a timely manner, if at all. AI currently has limited understanding of nuanced human communication elements such as sarcasm or subtle emotional cues, which can be critical in detecting deception.

While AI has made significant advancements and is highly effective at processing large volumes of data quickly, it still cannot fully replace human judgment. Human oversight and guidance remain essential in several key areas including, but not limited to, the generation of AI models, training processes, ongoing maintenance, validation of fraud detection and adjusting strategies to new types of events. Humans have a role in interpreting complex or ambiguous signals and ensuring that AI strategies stay current and effective in an everchanging threat landscape.

BALANCING AI AND OVERSIGHT IN SCAM DETECTION

SUPARNA GOSWAMI: How can you ensure a balance between AI and human oversight in scam detection?

KEITH SWANSON: The core reality of using AI is that it's not just defenders such as financial institutions who are leveraging it. Offenders, such as fraudsters and scammers, whether organised or singular in activity, are often able to advance faster than defenders. Unlike financial institutions, scam operations don't have to worry about governance, regulation or customer experience, all the factors that shape how we as regulated organisations responsibly use AI and which often necessitates having a human in the loop.

Offenders using AI will continue to innovate rapidly, finding new ways to exploit vulnerabilities and counter our defensive measures. As we think about how AI is applied and where human oversight remains essential, we also need to consider the broader ecosystem. That includes what organisations themselves can do, how other institutions involved in the customer experience can contribute, and what role regulators and governments can play in ensuring AI is applied effectively to help reduce scams.

CROSS-INDUSTRY COLLABORATION AGAINST SCAMS

SUPARNA GOSWAMI: For AI's effectiveness in fighting scams, no single entity can solve it alone. How can financial institutions collaborate across the ecosystem - including tech platforms, telecommunication companies and regulators to create a united AI-driven front against scams?

KEITH SWANSON: It's a challenge that we've been dealing with for years now. We've seen levels of collaboration in the industry, including public and private sector partnerships where information is shared between institutions and where allowed, with government bodies.

A good example of this is Australia's new Scams Prevention Framework, which is now being codified into regulation. The government has outlined shared obligations across multiple parties and institutions to help reduce scams and fraud, particularly financial institutions that handle transactions and move money. Equally important are telecommunications companies and digital media platforms, which often serve as the first point of contact for scammers targeting customers.

All these stakeholders are now within scope, required to share actionable intelligence, take coordinated and reasonable steps and demonstrate proportional responsibility for identifying, preventing and mitigating the impact of scams.

We have already seen significant collaboration developing alongside these efforts. Across the globe, many organisations and countries have implemented "confirmation of payee" or "verification of payee" technologies including regions like Asia-Pacific and Europe. These systems use cross-industry information to confirm that an account number matches the name on the account. This is critical because many legacy scams involve criminals presenting fraudulent accounts as legitimate, for instance, pretending to represent a payment to a trusted bank or company when, in fact, the account belongs to a criminal syndicate.

Organisations have been sharing data for years and this collaboration continues to grow, particularly through partnerships with reference data providers. These providers supply information such as compromised device data and other telemetry that helps organisations identify anomalies and other data points to say, "This isn't normal, this is not a device that we've normally seen our customer use in the past." We should have additional suspicion put forward in the AI and human-based detection methods that we use in combatting scams.

BUILDING STRONGER INDUSTRY COLLABORATION

SUPARNA GOSWAMI: What does effective collaboration across industries look like in building a stronger defence against scams?

SHANE BURNETT: The collaborative multi-industry approach is essential not just within banking but with other sectors to develop an effective strategy against scams. I would like to see the further development and selection of trusted representatives from key areas or industries to help create and develop universal strategies that have historically been more effective than everyone doing their own piecemeal approaches.

Reactive changes across industries often lead to siloed processes, data points, and the evolution of new regulations and tech solutions. All of these can sometimes be incompatible as a whole and create further issues and gaps leading to continued weaknesses and exposures that criminals can continue to exploit. From my experience, the most successful efforts include having well-defined approaches and a collective focus on the greater good. We need to develop a siege mentality against criminals, making it difficult for them to operate at all levels in all industries.

NEXT PHASE OF AI ARMS RACE

SUPARNA GOSWAMI: Scams are a global issue, with constant reports highlighting their growing impact. It often feels like an ongoing arms race between attackers and defenders. What's next in the battle between AI-powered scammers and AI-powered defenders?

SHANE BURNETT: The next move is very challenging. AI is advancing at such a rapid pace that staying ahead feels almost impossible at times. From a defender's perspective, we must maximise the value of our existing resources. As technology evolves, it's worth pausing to assess whether we're truly innovating or simply adding new layers of defence. In many cases, we may already have the right solutions in place, we just need to review our existing capabilities and use them more effectively.

To prepare for the future, organisations need to create flexible strategies and approach with a holistic view. At SAS, we have a broad portfolio of offerings and work with organisations to ensure we are solving a problem and not adding unnecessary layers.

EMERGING SCAMMER TACTICS AND DEFENSE

SUPARNA GOSWAMI: What new tactics do you expect from AI-driven scammers, and how should defenders prepare?

KEITH SWANSON: There are a few key points to highlight. Organisations have been using applied AI techniques for years in their roles as defenders in combatting scam and fraud attempts, but now they're exploring how generative and agentic AI can take those capabilities further. Much of this progress is happening in areas such as investigation and remediation, particularly in how organisations engage with customers. What's most important, is that as legacy exposures are identified and both traditional and emerging AI techniques are applied, organisations must ensure they can adapt and respond to new risks and attacks as quickly as the scammers attempt them.

One of the most common questions organisations face today is how to identify and combat deepfakes, both in interactions with people and in document verification. How can we be sure we're dealing with a real human and not an AI-generated persona? How do we confirm that the documents we receive, such as applications or other materials are genuine? The challenge now is finding effective ways to detect and counter AI-generated content by recognising when something has likely been, artificially, produced.

We have seen some powerful uses of AI and scam detection beyond the banking sector. In one case, a telecommunications company identified use of their services in helping facilitate investment scams as one of its highest exposure areas. By using AI to analyse customer interactions, the system detected patterns such as calls to their customers from newly registered phone numbers and unusually long call durations, often key indicators that individuals were being groomed for investment scams. The telecommunications company then shared this intelligence with banks, alerting them that certain customers might be at risk. This allowed the banks to use that information as an additional signal, for instance, flagging when a customer attempted a large transfer, such as a $20,000 payment to a new account and applying further AI analysis to determine if the activity was highly suspicious. Proactively, the bank can engage with the customer to help identify the genuine nature of intent, or whether the customer may be actively targeted by a scam.

CUSTOMER AWARENESS AND EDUCATION

SUPARNA GOSWAMI: What role does customer awareness play in preventing scams, and how can technology help deliver that education effectively?

SHANE BURNETT: Customer education is crucial in preventing scams, and technology can significantly enhance how this education is delivered. Traditionally, education efforts have been limited to static webpages or websites, which are rarely visited by the vulnerable groups, such as the elderly or those with limited computer knowledge. Education providers should focus on understanding the specific needs and behaviours of at-risk populations and tailoring their approach accordingly.

Different governments worldwide have websites where people can find more information about local and regional scams. In Australia, there is Scamwatch, the U.S. has the Federal Trade Commission (FTC), the U.K. has Action Fraud, and Southeast Asia has Global Anti-Scam Organisation.

By conducting some analyses using your own data or data and intelligence sources from these types of sites, we can develop automated educational tools that operate behind the scenes, analysing scam incidents and delivering targeted information to the appropriate peer groups in real-time. This approach ensures that education is both personalised and accessible using language and methods that resonate with the target audience. Respectful and clear communication is also extremely important.

Phrases like "dumbing down" are problematic. It implies a reduction in the quality and completeness of information. When explaining complex technology issues, you need to adjust the language to suit the level of understanding of the audience without oversimplifying or omitting important details. Effective customer education should always prioritise clarity and respect, ensuring that everyone receives the right information in a way that empowers them to recognise and avoid scams. Educating people so they don't get caught up in scams builds trust

in the organisation, and from an organisational perspective, it reduces overall costs.

MAKING EDUCATION REAL TIME

SUPARNA GOSWAMI: How can AI and new technologies make customer awareness more impactful in the real world?

KEITH SWANSON: Education is critical, but it must happen through the channels where potential victims engage. You typically wouldn't use TikTok videos to reach senior citizens. It's about matching the message to the right medium. Another key point is the shift toward real-time education. Organisations are now asking: How can we make real-time interaction part of our educational efforts? Historically, most awareness campaigns have relied in what I may call offline mediums, offline of the actual banking or payment activity, such as YouTube videos, TV commercials or Facebook ads. Today, the focus is moving toward integrating education directly into real-time interactions, where it can have the most immediate impact.

Most traditional education efforts happen outside the financial transaction itself. More organisations are asking: How can we use AI and real-time interaction to bring that education directly into customer experience? For example, if AI detects patterns suggesting that a customer may be the target of an investment scam, the system can trigger proactive messages during the interaction, such as, "Are you sure this transaction looks legitimate?" or "Please visit a branch to complete this transfer due to potential risk." This shift from offline to in-line education is a key development, enabling organisations to combine awareness and action in real time.

But it's important that we do not rely on education alone. For example, an organisation here in Asia-Pacific wanted to test the efficacy of scam awareness education. They defined a control group from their customer community, appropriately sampled using marketing techniques and segmentation, and they applied the test group.

"Education alone isn't enough. Reducing overall exposure requires a multi-pronged approach where education, detection and prevention, actioned through technology, people, process and data, all work together."

—Keith Swanson

The organisation then used offline (for banking or payment activities) communication channels, such as emails and SMS, or application-based videos, to educate its customers about typical scam exposures.

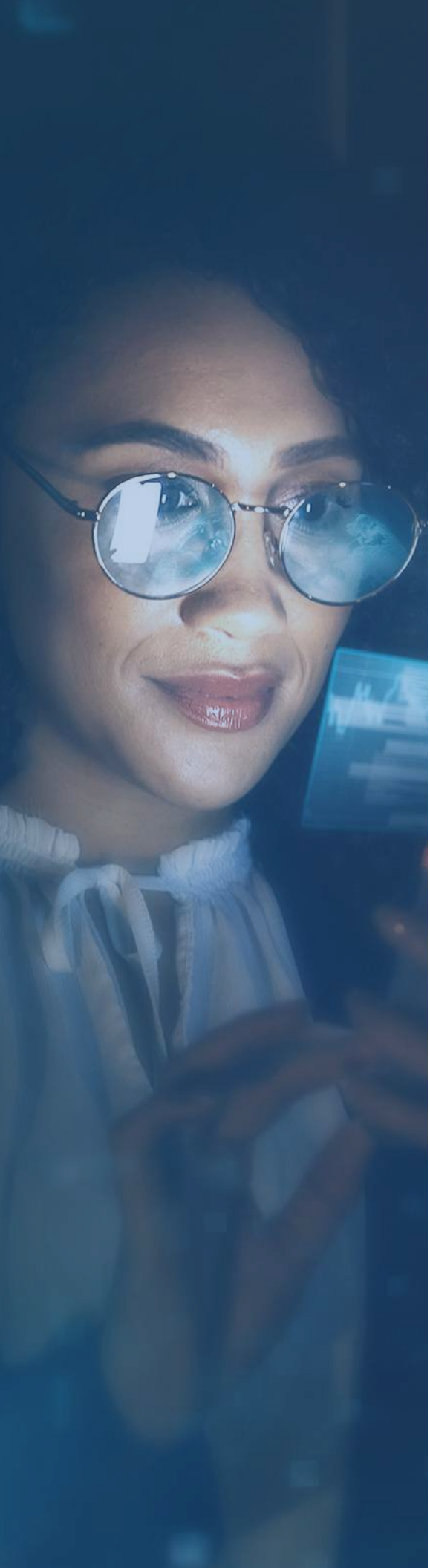
As expected, they saw a reduction in scams. But over time, the impact faded. As the test group either became fatigued by the education or was no longer exposed to it (such as 30 days past a communication), the levels of fraud and scams returned to those seen in the control group that received none of the anti-scam messaging. In short, education worked, but only temporarily. This highlights an important point: education alone isn't enough. Reducing overall exposure requires a multi-pronged approach where education, detection and prevention, actioned through technology, people, process and data, all work together.

EMERGING TECHNOLOGIES AND FUTURE STRATEGY

SUPARNA GOSWAMI: What emerging technologies hold the most promise against fraud, and what should financial institutions prioritise in their fraud prevention strategies over the next 12 to 24 months to move from reactive fraud controls to proactive scam prevention?

KEITH SWANSON: When we look at emerging technologies, much of the current focus is on combating deepfakes. The same generative AI techniques that scammers utilise are also being leveraged by defenders to detect deepfakes, whether they appear in human interactions or via documents.
As organisations consider how to use GenAI and agentic AI to enhance their defences, these discussions often centre on improving interdiction and remediation processes, the steps taken to stop scams or fraud during customer engagement. For example, Gen AI can assist investigators by suggesting key questions to ask a customer when they are contacted about an identified scam attempt, while agentic AI can help guide realtime customer interactions, prompting individuals for additional information needed to verify legitimacy or prevent fraud.

We often think of AI purely as a defensive tool, but some organisations are beginning to use it offensively, so to speak, as well. One such organisation asked an intriguing question:



“If scammers are using AI to target our customers, why can’t we use the same technology to target the scammers?” In this case, the organisation, working in collaboration with others, posed, “What if I could make a proactive call to a scam call centre acting like a customer and take up the scammer’s time?”
How does this approach help combat scams? The idea is simple: If a deepfake "customer" actioned via AI and systems can engage a scammer for 15 minutes, that's 15 minutes less they can spend targeting real victims. It's a creative way to turn a scammer´s own tactics against them. Ultimately, it remains an arms race, one that relies on a mix of techniques, from the applied AI we've used in the past to the GenAI and agentic AI shaping today and the future.

SHANE BURNETT: We first need to start by leveraging our existing assets and technologies to enhance our fraud prevention capabilities before adding blind layers. Emerging technologies such as advanced AI, machine learning, and behavioural analytics hold significant promise for shifting from a reactive to a proactive approach, if incorporated into a well thought-out strategy. Strategy is key. Organisations should be looking to create multi-layered strategies across the entire organisation, not just at the departmental level, breaking down silos and the political barriers that hinder agility. By doing so, they can develop a more comprehensive forward-looking approach that anticipates and mitigates emerging scams more effectively. This holistic stance is essential to stay ahead of evolving threats and avoid costly losses, ensuring a resilient and secure financial ecosystem in the next 12 to 24 months.

HOW CAN SAS HELP

Stopping scams requires speed, clarity and the ability to adjust as new tactics emerge. You need AI and machine learning to detect and prevent scam activity in real-time. Integrated analytics, alerting, investigation and automation help financial institutions prioritise risk and take action quickly without adding operational complexity. SAS® Viya® for banking is a cloud-native platform built to help banks and financial institutions tackle complex data and AI challenges.

FRAUD TYPES ADDRESSED

SAS supports detection and prevention across major fraud scam categories, including:

- Payment fraud.
- Account takeover and money mule activity.
- Identity verification and synthetic identity fraud.
- Application fraud.
- E-commerce fraud.

What sets SAS apart is the ability to unify fraud detection across channels, apply explainable AI to support compliance and adapt quickly as threats evolve.

DECISIONS YOU CAN TRUST

Our enterprise fraud management platform enables transparent decisions. Used by financial institutions worldwide, it combines internal and external data with AI and machine learning to identify a wide range of scam types as they occur, while clearly showing why actions are taken.

Key capabilities include:

- Real-time, AI-driven decisions with clear explanations.
- Forensic-grade investigation tools.
- Alert and case management.
- Business intelligence dashboards.
- Adaptive model management.
- Cross-channel and cross-border threat analysis.
- Data orchestration and enrichment.
- No-code/low-code user interfaces.

ABOUT SAS

SAS is a global leader in data and AI, serving more than 1,600 banking and financial services organisations in over 92 countries. More than 90 of the world's top 100 banks rely on SAS to make faster, smarter, and more transparent fraud decisions.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of its 38 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. Its 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 INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

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

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

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