



Technology's role in reducing fraud and risk in banking and financial services

Panel event report



Introduction

Managing fraud and risk has always been important to banking and financial services firms, but that importance is rising as the global threat environment evolves. With new technologies, adversaries and criminal techniques emerging regularly and regulations increasing in response, it's a complex scenario to navigate.

At BT, we're in the same position; our networks and contact centres are targeted every day. We already defend ourselves and our customers from over 200,000 cyber attacks each month and expect that number to grow.

We're all in this together, so we're working with banks and financial services organisations, and an ecosystem of innovative technology partners, to identify new fraud techniques and knit together multiple layers of security to minimise holes in the defence.

Our recent event brought together a collective of attendees from banking and financial services organisations, cyber security firms, and our own experts to explore technology's role in reducing fraud and risk in banking and financial services, and this paper summarises what we covered.

Contents

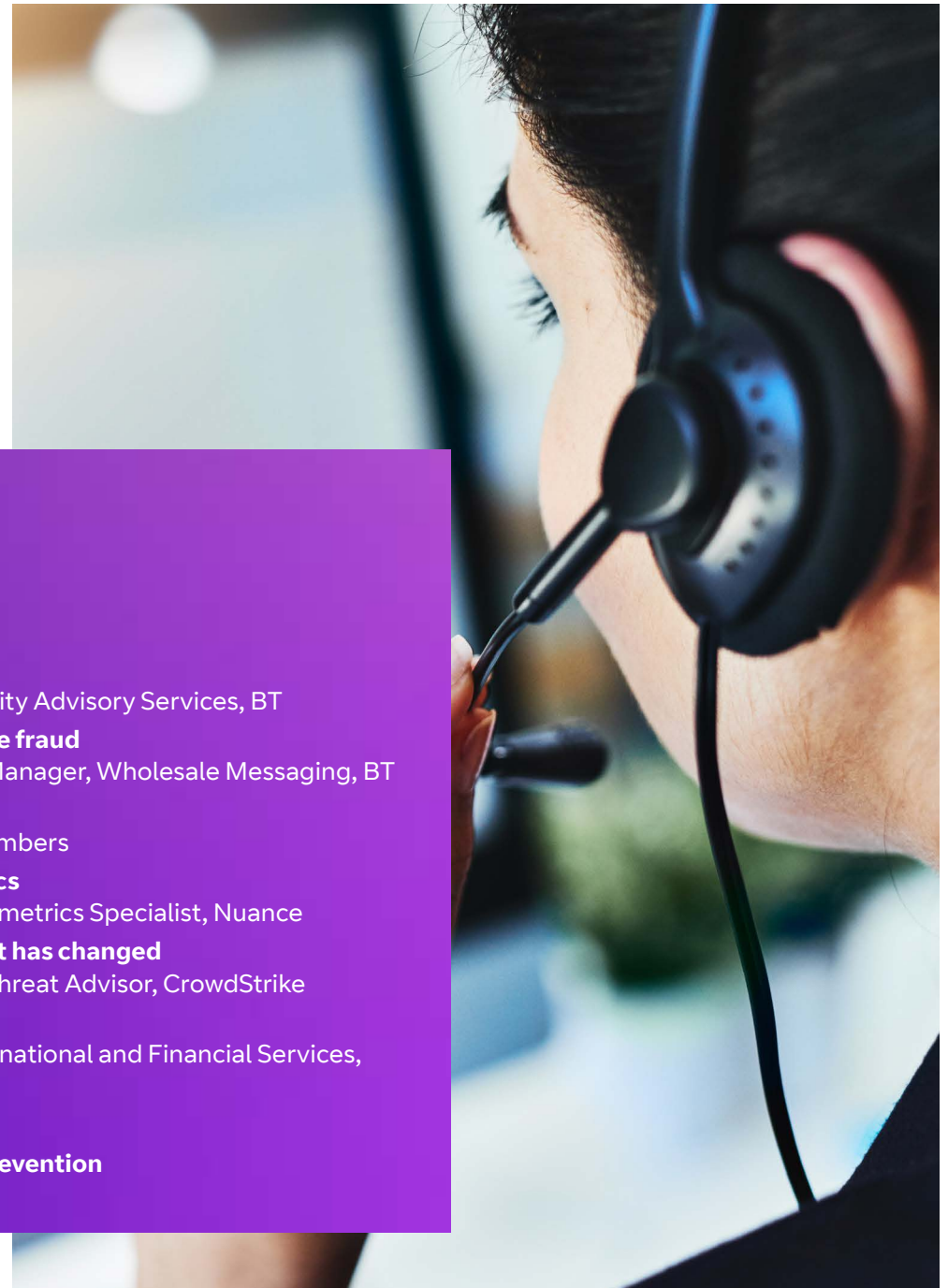
Key insights

Presentation summaries

- **Fraud and risk – the BT view**
Lee Stephens, Director, Security Advisory Services, BT
- **BT innovations to help reduce fraud**
Anna Smith, Senior Product Manager, Wholesale Messaging, BT
- **Is your contact centre safe?**
Jamie Melling, CEO, Smartnumbers
- **Tackling fraud with biometrics**
Ian McGuire, Security and Biometrics Specialist, Nuance
- **How the modern cyber threat has changed**
Christian Heggen, Strategic Threat Advisor, CrowdStrike
- **Cyber risk quantification**
Adam Winter, Senior VP, International and Financial Services, Safe Security

Q&A session summary

An ecosystem approach to fraud prevention



Key insights

Our panel delved into the fraud landscape for financial services firms, exploring the impacts of new technologies, adversaries, criminal techniques and regulations. The following key insights emerged:

1 The SMS channel is being used more and more for business messaging as consumers move to other channels for their personal conversations.

4 The messaging market is fragmented, with a flow of new entrants. As yet, there are no clearly defined roles for channels because consumers are undecided as to which channels are appropriate for inbound and / or outbound business contact.

7 The messaging market is projected to grow rapidly due to the breadth of channels and their ability to carry richer content, although the reach of Rich Communication Services (RCS) remains a challenge.

2 Using voice prints as a fraud prevention tool is progressing, but is held back by data regulations that prevent full data sharing.

5 Fraud is migrating to the contact centre but, due to technology limitations, the risk is often hidden. Events such as fraudsters gathering data from the Interactive Voice Response (IVR) to help social engineer contact centre agents or to defraud citizens as part of an APP scam often go undetected.

8 Voice print recognition is a reliable technology due to the process of embedding watermarks into the audio recordings. Plus, deepfakes remain unconvincing and easy to detect.

3 Fraud prevention tool providers are now able to share phone data with the appropriate authorities if it's linked to a criminal investigation.

6 Attacks targeting employees to get the credentials that unlock access to the organisation remain a significant source of fraud. Technology exists to give organisations visibility and alerts when employee, customer and supplier information is obtained.

9 The key to better fraud management and prevention is pan-industry cooperation, supported by data regulation frameworks that allow the sharing of information between organisations.

Presentation summaries

During our event, each speaker presented key insights from their area of expertise. Here, we've captured each panel member's key learnings and summarise their take on technology's role in fraud prevention and risk management.

Fraud and risk – the BT view

Lee Stephens,
Director, Security Advisory Services,
BT

The current financial services fraud and risk environment, though sprawling and complex, can be split into three focus areas:

- **consumer fraud** – the use of more sophisticated tactics to target consumers is exacerbated by hybrid working and digital contact centres; the contact centre is involved in 61% of fraud losses
- **employee fraud** – the growth in connected devices and work-anywhere culture is changing how risks are assessed and monitored
- **cyber risk** – a broad range of cyber threats needs to be contained and quantified so cyber exposure can be calculated in monetary terms.

What's the current state of play?

Many financial services institutions rely on a fragmented view of the puzzle and multiple solutions to provide their response – and those solutions can fall short in today's threat landscape. Consumer authentication processes such as PINs and security questions can be hacked and, despite some progress in introducing biometrics and machine learning, BT analysis of internal calling data shows that customers still waste 1.5bn minutes per year being authenticated. Employee authentication largely focuses on usernames and passwords, which deliver poor security, a sub-optimal user experience and increased support costs. Organisations are looking for ways to introduce robust privilege management and role-based controls without stopping people from doing their jobs.

In the cyber arena, organisations know layering security solutions is key to an effective cyber risk response. However, current 'risk matrices' often use ordinal scoring (low, medium, high) rather than quantitative, statistical methods; or they focus on specific controls instead of the organisation holistically. Plus, many risk quantification methods rely on 'expert' opinion rather than statistical fact.

Reframing fraud and risk defences

As part of our ambition to help our customers and society 'connect for good' we're committed to being part of the solution to fraud and digital risk. We believe the best defence is a multi-layered, fully integrated approach, creating a unique, collaborative partnership with customers and partners to address and combat fraud from all angles.

Our approach enables financial services organisations to access an anti-fraud and security portfolio that supports capabilities in:

- enhanced caller authentication and fraud detection
- advanced voice biometrics
- enhanced identity and access management
- a Zero Trust approach to authentication
- advanced detection and remediation of security breaches
- objective risk quantification using data science.

BT innovations to help reduce fraud

Anna Smith,
Senior Product Manager, Wholesale Messaging, BT

Our messaging security team works with a wide range of internal BT stakeholders on messaging and customer security, working closely on SMS smishing and fraud with key external agencies, including the National Cyber Security Centre, UK Finance, DCPCU, MEF, Google and GSMA.

SMS has significant value as a highly effective messaging format in terms of business engagement rates. To maintain trust in SMS in the face of increased smishing we've stepped up our focus on the route the message is using to enter the network and what the actual content is.

Detect and block

Our new AI-driven firewall has made a significant change in identifying messages before they reach our customers and put them at risk. Already, the firewall has blocked 30,000 numbers, 41 million messages due to the URL and 132 million messages on content, leading to a 90% decrease in complaints.

Driving the shift from reactive to proactive protection

In collaboration with our direct partners, we'll be running a series of trials and proof of concepts covering:

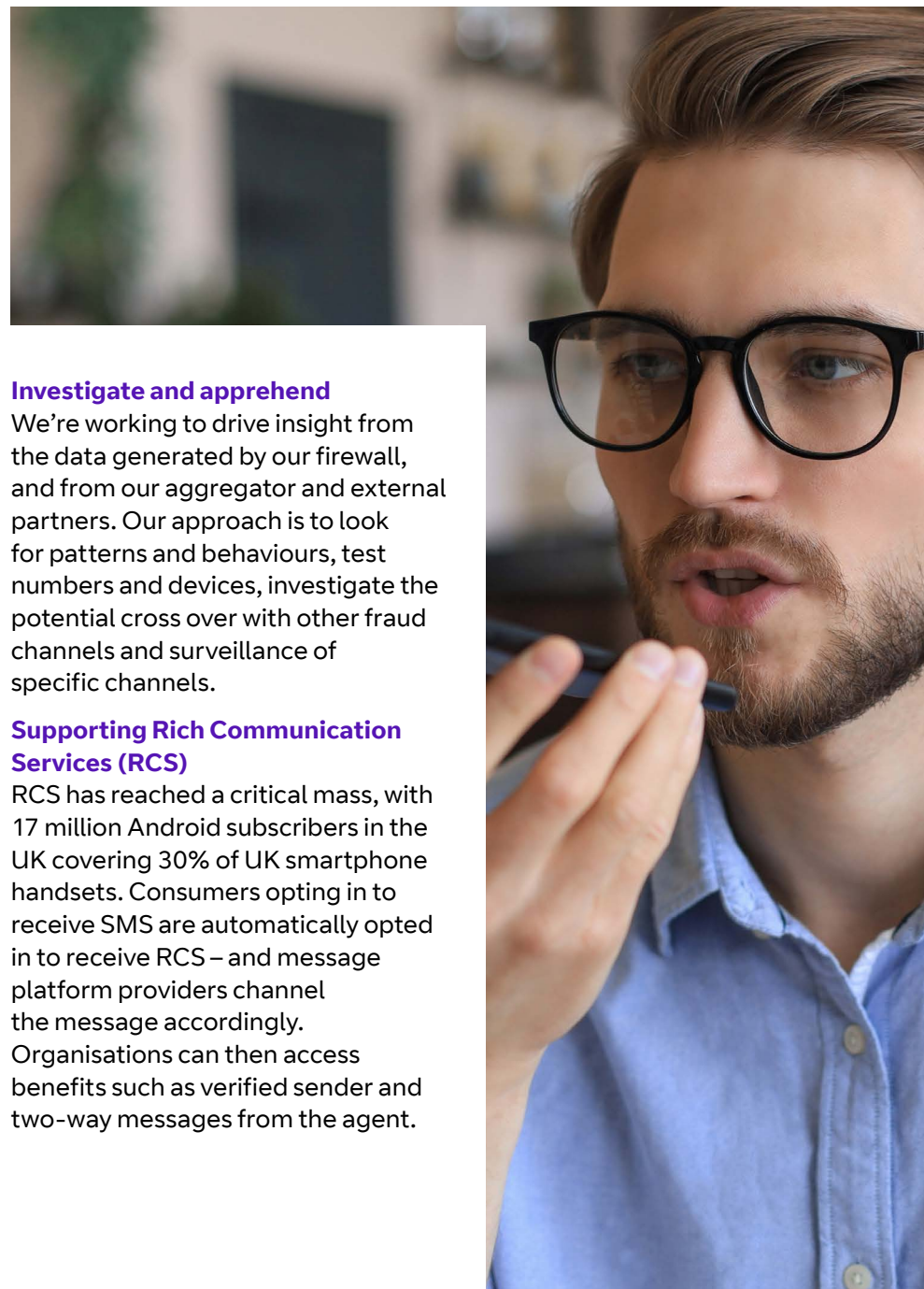
- new sender ID rules
- allowing special characters by exception only
- tailoring security to 'trusted' or 'general' sender categories
- firewall blocking based on set sender ID / URL combinations
- automated blocking based on URL age and risk factors
- tackling SIM farms by identifying SIMs keeping under limits, such as inbound vs outbound SMS, call and data usage.

Investigate and apprehend

We're working to drive insight from the data generated by our firewall, and from our aggregator and external partners. Our approach is to look for patterns and behaviours, test numbers and devices, investigate the potential cross over with other fraud channels and surveillance of specific channels.

Supporting Rich Communication Services (RCS)

RCS has reached a critical mass, with 17 million Android subscribers in the UK covering 30% of UK smartphone handsets. Consumers opting in to receive SMS are automatically opted in to receive RCS – and message platform providers channel the message accordingly. Organisations can then access benefits such as verified sender and two-way messages from the agent.





Is your contact centre safe?

Jamie Melling,
CEO, Smartnumbers

Observed contact centre fraud is only the tip of the iceberg

The latest figures from UK Finance put [fraud loss due to telephone banking at £7.9 million in the first six months of 2022 alone](#). However, most of the fraud due to contact centre vulnerabilities is hidden because reported telephone fraud only includes data where criminals use compromised bank details to gain access to the victim's telephone bank account and transfer money away.

Hidden fraud includes reconnaissance activity where fraudsters validate compromised details or monitor compromised accounts to time the extraction. Alternatively, fraudsters exploit IVR vulnerabilities to gather additional data that can be used in other types of fraud. They hide their identity by manipulating their phone number - either by spoofing or withholding their number.

The make-up of IVR fraud

Smartnumbers has analysed millions of calls to identify the signs of organised fraud attacks. On average, 1 in 500 calls into the IVR are from a fraudster and fraudsters make an average of 26 calls leading up to a final attack. The majority (59%) of fraudster calls are from a withheld number and more than 40% of IVR attacks are from a known fraudster.

Prevent fraud in the contact centre with Smartnumbers

First, pre-answer analysis assigns a risk score to the call before it even arrives at the IVR, using multiple tools including analysing call behaviour, call signalling, or flagging fraudster numbers highlighted by other customers. Then post-call analysis helps to identify, investigate and prevent future fraud by highlighting suspicious calls that need investigation. Smartnumbers can also follow up and provide more detailed information on calls flagged as risky from another system, such as Nuance Gatekeeper.

Tackling fraud with biometrics

Ian McGuire,
Security and Biometrics
Specialist, Nuance

The one constant in fraud is the human behind the fraud, so Nuance focuses on tracking the fraudster's voice. This frustrates fraudsters and also adds extra costs to their business model, forcing investment in a network of unknown individuals to make the calls.

Nuance has the power to break the fraud lifecycle early, often at only the second step – reconnaissance – where attacks previously went undetected. It also focuses on disrupting the set-up and monetise stages, to prevent any money being accessed or moved. Real data shows that Nuance's fraud detection breaks down as 48% at reconnaissance, 13% at set-up and 39% at the monetise stage. This translates into significant savings for banks: in 2022, a large UK bank's Nuance system prevented £249m of attempted fraud.

Nuance uses four main techniques:

- **real-time and offline watchlist detection** – comparing incoming calls with known fraudster voice prints. The effectiveness of this will increase when data sharing issues between organisations are resolved
- **historical search** – finding past fraud events committed by a particular fraudster to identify repeated fraud attempts from a single known fraudster. This also works across messaging channels, using conversation pattern analysis
- **clustering** – comparing all audio within a timeframe to find similarities that could be possible fraudsters. Key times to apply clustering include enrolment, authentication mismatches, opt-outs, locked-out accounts and high-risk calls
- **data mining** – large sample analysis to spot previously undiscovered fraudsters and to help predict when fraud attacks are going to happen.

The six-stage fraud lifecycle

1.

Data acquisition

Dark web, phishing, smishing, vishing, corrupting employees, mail intercepts, cyber breaches, device takeovers.

2.

Reconnaissance

Access via phone or online, validating data, obtaining more data (balance, recent transactions, etc.), checking finance hygiene, determining the best attack.

3.

Setup

Creating a new payee, ordering replacement card / PIN, PIN reminder, reset login details, internal funds transfer, initiate loan / overdraft application.

4.

Monetise

Make payment / balance transfer - banks view this as 'cashing out'.

5.

Laundering

Move funds between 'clean' accounts, move offshore (and back), use of mule accounts.

6.

Cash-out

Fraudsters obtain the money.



How the modern cyber threat has changed

Christian Heggen,
Strategic Threat Advisor, CrowdStrike

As malware, tooling, and infrastructure shift over time, threat intelligence needs to understand the motivations, techniques, and tools of distinct adversarial individuals and groups. This threat intelligence forms the basis of a proactive security posture that puts organisations one step ahead of the ever-changing threat landscape.

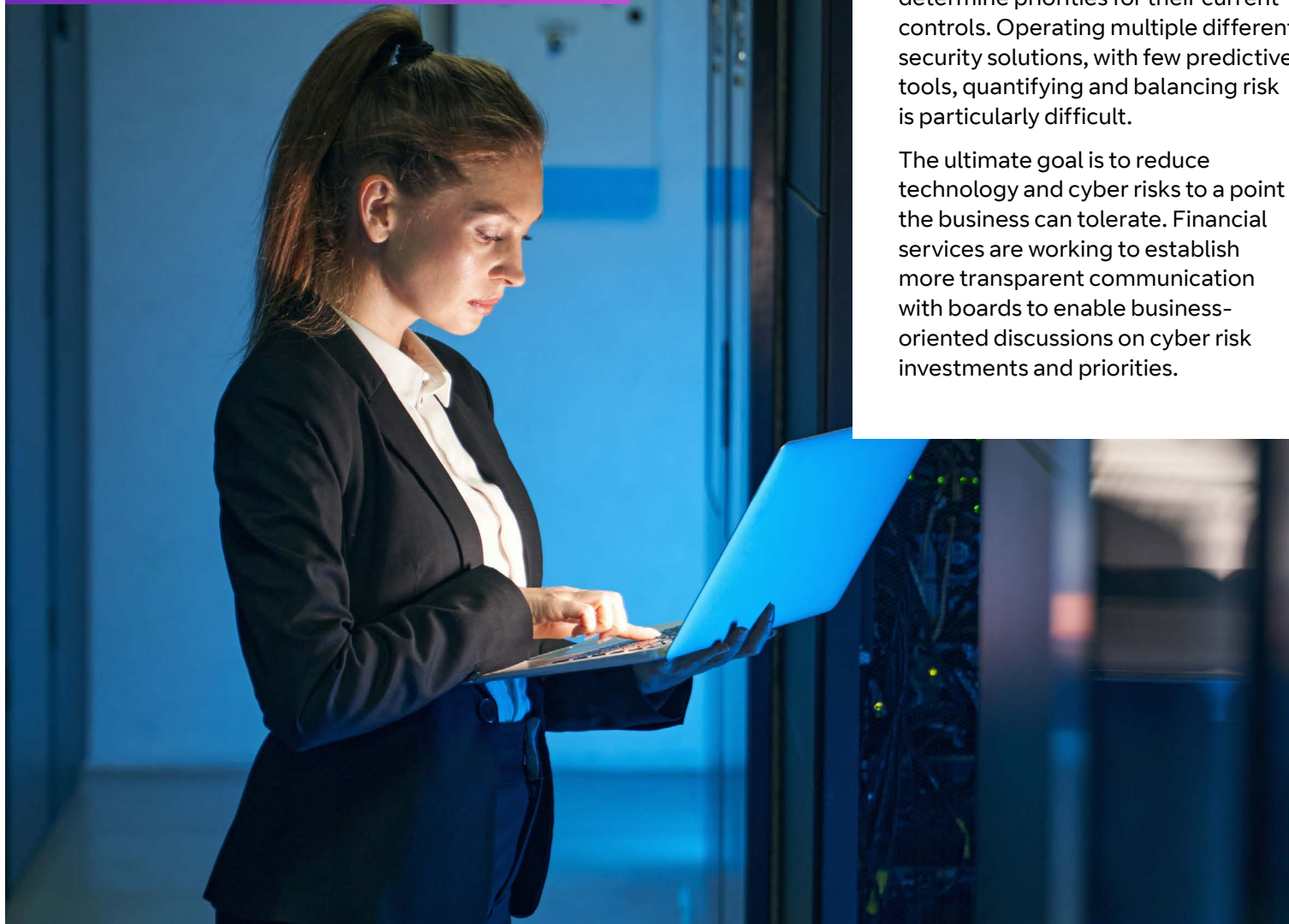
Our internal data indicates that, since 2019, eCrime has increased by over 700%, with most incidents carried out by financially motivated cyber criminals working in ecosystems. Rather than a distinct group, these ecosystems comprise large numbers of individuals with varying specialisations – from access brokers to malware developers to Ransomware-as-a-Service – all collaborating to conduct more efficient operations. Because they're agile and dispersed, ecosystems reduce the risk of being caught and increase potential profits.

The typical eCrime sequence for a successful ransomware operation can include various actors and might play out as follows:

- 1. Access broker:** helping adversaries to launch attacks faster, access brokers identify targets and sell their credentials – enabling cyber attackers to gain access to the victim's environment.
- 2. Malware downloader / banking trojan:** the adversary purchasing the access then downloads either malware or banking trojans into the victim's environment, typically allowing for backdoor access.
- 3. Lateral movement:** often referred to as 'living off the land', many criminal actors use legitimate tools and processes on the victim's network to blend in with normal network traffic, so they don't trigger any internal alerts.
- 4. Data exfiltration:** once they've located sensitive data, the adversary will exfiltrate the data from the victim's network.
- 5. Ransomware deployment:** the adversary then deploys ransomware to lock the victim's machine.
- 6. Money laundering:** after receiving ransom payments, the adversary monetises these using currency washing or mixing services.

Cyber risk quantification

Adam Winter,
Senior VP, International and Financial
Services, Safe Security



In recent years, focus has transitioned from cyber security to cyber risk. In an environment where macro-economic conditions are slowing and regulators are turning their attention to risk statements, financial institutions are moving to risk management frameworks to determine priorities for their current controls. Operating multiple different security solutions, with few predictive tools, quantifying and balancing risk is particularly difficult.

The ultimate goal is to reduce technology and cyber risks to a point the business can tolerate. Financial services are working to establish more transparent communication with boards to enable business-oriented discussions on cyber risk investments and priorities.

Many financial institutions already have aspects of a risk appetite framework in place but lack an end-to-end structure that's fully linked to control objectives. Developing, understanding, enforcing, and executing a framework requires good data, extensive monitoring, and coordination across business, technology, and second line of defence functions.

Today, cyber risk is measured and managed in three ways: outside-in threat intelligence based on risk posture monitoring, siloed telemetry from 10-30 cyber security tools, and inside-out questionnaire-based risk posture audits. A nexus of all three together via an integrated and real-time SaaS platform enables:

- real-time visibility of cyber risk at enterprise, group, and individual asset level
- intelligent prioritisation recommending actions for the risks that matter most
- consistent communication across enterprise and committees like the board and IT department
- articulate ROI for both past cyber security investments and future budgets
- rationalised risk transfer that incentivises enhanced security postures for better insurance premiums.

Q&A session

With fraud and risk firmly entrenched as a strategic priority for all financial services organisations, our expert panel explored the current threat landscape and how to bring about positive change. Here we summarise how our specialist partners from Nuance, Smartnumbers, CrowdStrike and Safe Security, as well as our internal experts from BT, answered the questions of the day.

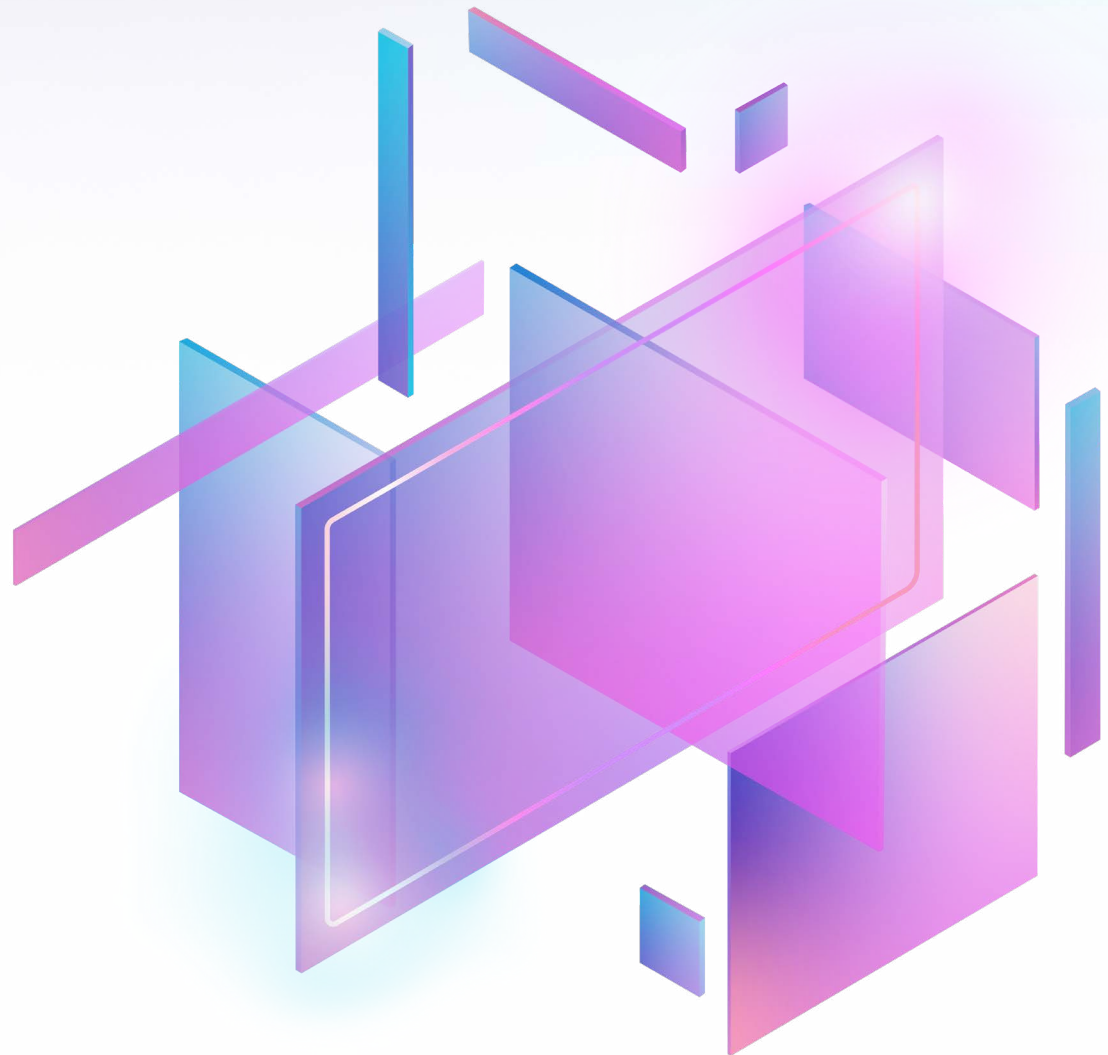
Messaging fraud

What can we do to satisfy regulators and get new innovations incorporated into regulation? From a banking point of view, SMS is often perceived as untrustworthy and unsafe. What can we proactively do to get trust back in SMS?

The key will be in coming together with other mobile network operators in working groups to push for change in the messaging arena.

SMS is still very strong and will continue to be a key form of business messaging. Downloading apps works in many use cases, particularly banking, but it's unlikely consumers are going to get the app of every business that touches them, so not all messages are going to be notifications via apps. WhatsApp has problems with reach and security, and the reach of Rich Communication Services (RCS) remain a challenge, with Android adopting RCS but Apple resisting. It will be worth watching to see how the EU's Digital Markets Act could change this by requiring interoperability.

The more banking and financial services firms can feed information about what they want to see, the more operators can use this to feed into the working groups and make a difference to the use and value of SMS.





Why shouldn't we have sender ID registry in the UK?

There's been some debate over where SMS is going and the effect of introducing sender ID registration, and a threat that Ofcom will come in and demand a registry like in France and Singapore. This is unlikely to happen in the near future because retrofitting sender ID would be costly. It could possibly prove so costly and cause so much friction that it pushes people away from SMS, particularly small businesses, removing any registration benefits. Regulation may come in to enforce sender ID registration, but it's not a decision that would be taken lightly.

How will messaging evolve in 2023?

The big shift to watch right now is the fragmentation of the messaging market, as new channels offer wider benefits to both consumers and businesses. The question with channels such as WhatsApp for Business and Facebook for Business is: will consumers want to use what they see as personal channels to receive business messages? A split may develop between consumers wanting to use these channels for inbound contact but resisting their use for outbound contact. Consumers want to be able to use the channel of their choice, which is increasing the importance of the omnichannel messaging platform.

The messaging market is projected to grow rapidly due to the breadth of channels and their ability to carry richer content, enabling more engaging conversations and the use of chatbots to answer certain queries - but a strong part of that is still going to be SMS.

What does the roadmap look like for data sharing? Can we get to the point where the investigation teams of banks, BT, and EE collaborate?

Getting a clear picture will involve bringing together information from a lot of teams within BT and EE. Accessing certain elements of data is challenging, due to data protection rules and the requirement to justify why access is needed. Teams need to work hard to get the necessary permissions and talk to mobile network operators about ways to share information between firewalls. Today is about taking action to push this forward.

“Our ambition as an innovative messaging team is to get permissions to access data that's currently protected and find ways of sharing it so all interested parties can collaborate to find a robust solution to fraud. We'd like to lead the way on working with the regulations to move the industry forward.”

Anna Smith - Senior Product Manager,
Wholesale Messaging, BT

Contact centre fraud

There are restrictions around sharing voice prints, yet clearly this would benefit everyone. How do we address that?

The good news is that the more organisations move towards cloud solutions the easier it gets technically to share audio files. The issue with sharing fraudster voices is that an attack often involves a fraudster giving a customer's data (PIN, postcode, etc). The bank can share the fraudster's voice, but can't share a person's data, so has to redact some of the call. It makes sense that financial institutions will only invest in this if they see a return on it.

The regulator is also relevant to this point. Last year a project launched using voice prints for age verification to prevent minors accessing 18-rated games and content. Technically, organisations have the capabilities for this, but what's slowing them down is accessing children's data to test a solution's effectiveness. The protection around gathering children's data is onerous, with multiple regulators involved. What's needed is for regulators to sort these access questions out together.

Could that be inverted, and a voiceprint used to determine an age which is less fraught in terms of regulation?

Yes, Nuance has also explored inverting this technology to identify older people who, generationally, tend to be more vulnerable to cyber crime. With Telefonica in Spain during the pandemic they developed a system that prioritised access to services for those over 70 and achieved over 75% accuracy. The problem with younger age groups is that people's voices change quite dramatically, certainly boys' voices do, so there are issues around collecting enough data to accurately model it.

How has Smartnumbers found dealing with regulations?

From Smartnumbers' perspective, it's all about the telephone number, and they're classed as personal information. Operators have had to argue long and hard with the regulator for adjustments to this personal information classification to allow operators to share information to protect customers. As a result, operators can now share phone data that's linked to a criminal investigation with the correct authorities at the press of a button.

We've talked about Smartnumbers' capabilities in the operator role – how well does Smartnumbers work outside the UK?

Smartnumbers uses partnerships as a route to compliant delivery, developing a variety of deployment models to meet the requirements of different geographies and using BT's international network to make BT-Smartnumbers joint services easy to access. Smartnumbers' systems are structured so that local data rules are applied, keeping signalling data within that country's borders.

“We can spin up an AWS instance within a region so that the data never leaves its country of origin. We're keeping pace with regulations as they emerge.”

Jamie Melling – CEO, Smartnumbers

Deepfakes are highly topical – how are they going to impact the voice biometrics world?

There are concerns about deepfakes, and the Microsoft research project, DALL·E, that needs only three seconds of audio to be able to replicate a voice comes up a lot as a potential issue. But the risks of deepfakes are overstated at the moment. Even with nation state-backed resources, the recent deepfake of President Zelensky was unconvincing. Ethical organisations creating synthetic voice are embedding watermarks into the audio that are only detectable at a spectral level. Biometric engines can identify deepfakes through the absence of watermarks, as well as the high degree of audio processing a deepfake goes through makes it unnaturally clean.

“We've never seen a real-world successful deepfake attack because there are easier ways to attack a customer. Currently, deepfakes aren't viable attacks and won't be for at least five years.”

Ian McGuire – Security and Biometrics Specialist, Nuance

Cyber threat and risk

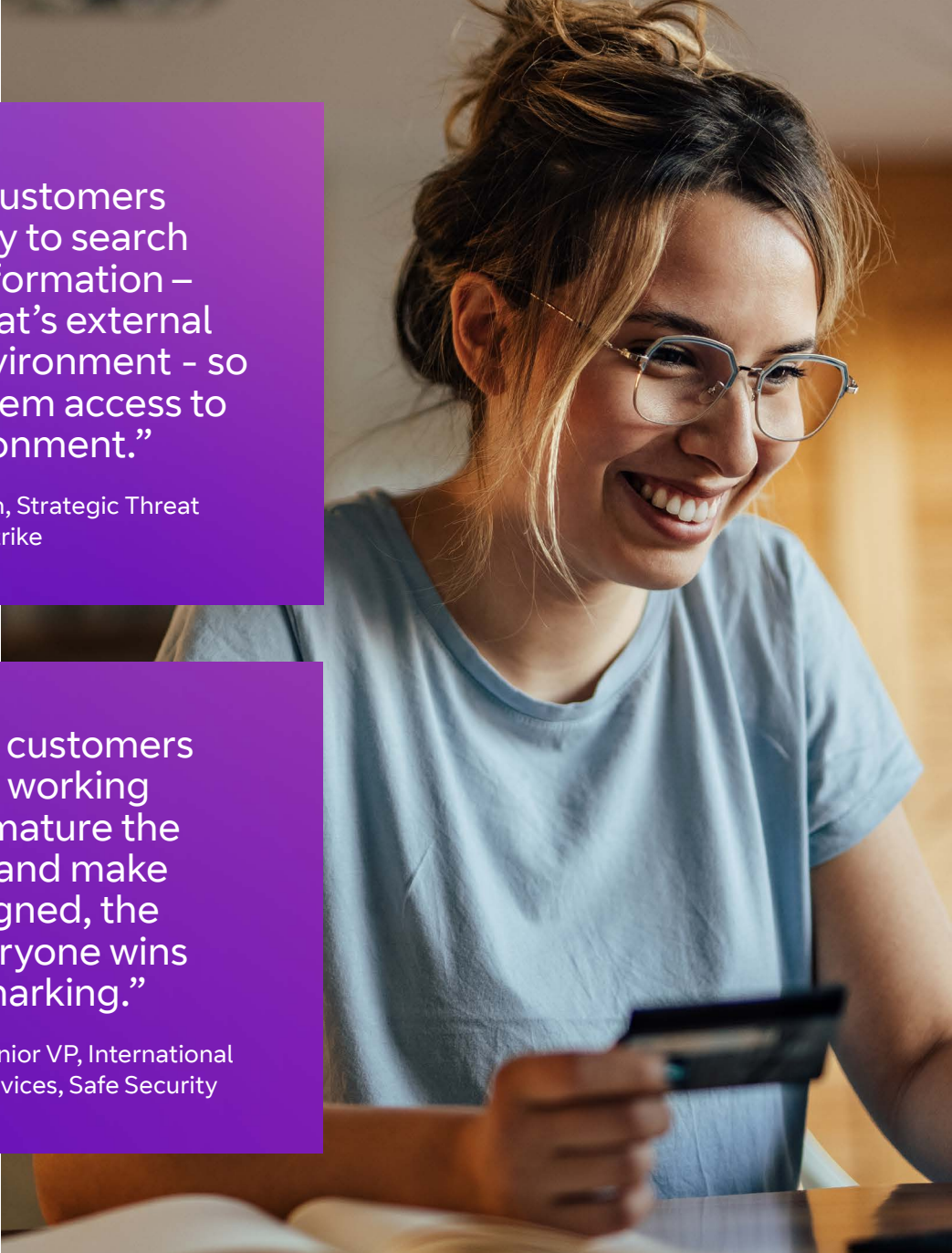
Thinking about access brokers and the information that's out there, how can organisations prevent cyber-enabled fraud from happening?

A significant amount of fraud is the result of attacks that target an organisation's employees to get hold of credentials that they can leverage to access the organisation's environment. So much of this information is sold and re-sold on the dark web - organisations just don't have visibility of it. Organisations like CrowdStrike are developing tools and structures to give firms that visibility and information on their employees, customers, third-party suppliers - notifying organisations as information is obtained.

In terms of Safe, is there an opportunity to adopt a standard system to assess risk, bringing down the cost of insuring against risk?

To achieve a standard system, without being forced to by regulations, an industry body needs to push real-time risk quantification forward by creating a bridge between parties. The key point is, how to align schemes of classification (or taxonomies) with events - because if this can be achieved, then financial services clients can exchange information.

Safe Security, for example, is currently exploring ways to align their risk taxonomy with the standard, as well as with cyber risk taxonomies, to build a model. They're also working with rating agencies because cyber risk is intrinsically linked to credit risk.



“We give customers the visibility to search for their information – visibility that's external to their environment - so they can stem access to their environment.”

Christian Heggen, Strategic Threat Advisor, CrowdStrike

“The more customers we can get working with us to mature the taxonomy and make sure it's aligned, the better. Everyone wins on benchmarking.”

Adam Winter, Senior VP, International and Financial Services, Safe Security

BT's plans and innovation

It's clear BT is working with a number of banking and financial services customers on fraud and risk strategies – what makes these customers choose to work with BT?

At BT, our focus is on connecting different cloud-based services together and providing customers with easy access to the result. Our teams have also worked with innovation partners to produce new technology that's unique to our implementations.

The work doesn't stop there. Currently, we're exploring a range of projects with customers and partners designed to help tackle fraud and risk in banking and financial services.

From sharing the voice prints of bad actors across the industry in a controlled and focused way, to broadening the use of the partner capabilities to help consumers recognise when they're being targeted, our teams are pushing boundaries. They're also using data that combines activity on our network with information from banks collaboratively, to find new ways of detecting and preventing scam calls from reaching consumers.

To follow this up, we're launching a pan-industry forum to explore the results with executives from banking, insurance, telcos, regulators and law enforcement to drive greater and more focused collaboration between organisations.

“The ‘why choose BT’ reasoning is all about our work with a lot of other partners, making sure everyone’s efforts all join together and connect into a single story. We also always have our compliance and ethical hats on - we’ve debated every move with our lawyers and in-country experts which gives trustworthy assurances.”

Kerry Johnson, Product Manager
– AI for Customer Experience, BT





An ecosystem approach to fraud prevention

We're taking action to better manage fraud across the whole of society, working with our industry partners to broaden the conversation beyond solutions and networks. It's in partnership that we'll be able to bring isolated projects together to create compliant pan-industry solutions.

We're already part of a working group exploring voice print sharing, and we'll continue to run industry-wide forums that bring together all banks with UK interests, regulators such as Ofcom and the FCA, and crime teams to propel progress.

[You can find out more about how our ecosystem of innovative partners blends the latest technologies in fraud detection and mitigation on our webpage.](#)

We will be offering a virtual version of this event shortly. If you'd like to join in online, then [register your interest here.](#)

Partner biographies



Smartnumbers is a caller authentication and fraud detection solution that prevents fraud in the contact centre. It identifies suspicious calls while still in the network and authenticates legitimate customers before they even reach an agent.

Smartnumbers helps to provide a seamless and efficient customer experience and detects fraudulent calls at the source, covering both prevention and optimised authentication. It's also cloud-based, which simplifies call recording and enables businesses to scale their strategy.



Nuance is a leading provider of speech and imaging technology solutions that help businesses to improve their customer engagement and prevent fraudulent activities. Nuance's Intelligent Fraud Prevention solution provides AI-based fraud detection across multiple channels and touchpoints, including phone, web, and mobile.

Intelligent Fraud Prevention draws upon voice biometrics, behavioural biometrics, device recognition, and more, to detect both known and unknown types of fraud and adapt to new threats and attack patterns in real-time. This allows businesses to prevent fraud before it occurs, reduce losses, and improve the customer experience.



CrowdStrike offers the world's most advanced cloud-native platform that secures the most critical areas of enterprise risk – endpoints and cloud workloads, identity, and data – to keep customers ahead of today's adversaries and stop breaches.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft and enriched telemetry from across the enterprise. This delivers hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritised observability of vulnerabilities – all through a single, lightweight agent.



Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

© British Telecommunications plc 2023. Registered office: One Braham, Braham Street, London, England E1 8EE. Registered in England No. 1800000.

February 2023