call centre management association

Leadership Forum
Financial Services

Tackling the fraud epidemic in contact centres

Financial Services Leadership Forum attendees:

Matthew Addison, Chief Revenue Officer, Smartnumbers
Nick Andrews, Head of Customer Operations, Monzo Bank
Russell Atkins, Head of Customer Services, Starling Bank
Tim Burton, Chief Customer Officer, Smartnumbers
Alice Bush, Head of Operations, Takepayments
Mike Clark, Operations Director, IG Group
Jamie Crewe, Operations Manager, Close Brothers
Dean Docherty, Head of Fraud, Marcus by Goldman Sachs
Sean Gilholme, Head of Customer Service, Atom Bank
Leigh Hopwood, CEO, CCMA
Tracey Lawlor, Deputy Director of Banking Operations, Starling Bank
Mandy McCormack, Head of Risk and Control Direct AIB, Allied Irish Bank
Danielle Sack, Head of Fraud Operations, TSB
Mark Williams, Head of Financial Crime, Optimus Cards

Financial Services Leadership Forum

The Leadership Series is the documented output from CCMA's Leadership Forum meetings. These meetings take place at the House of Lords and provide an exclusive opportunity for senior contact centre leaders to explore the key factors driving change in the industry and to consider how to continue to innovate for the benefit of the customer, colleagues, and the business.

Supported by

smartnumbers

According to recent UK Government statistics, fraud now accounts for 40% of all crime – and costs the country around £7 billion annually. Fraudsters are also increasingly taking advantage of contact centres to access information and commit criminal offences, with research suggesting that around six out of ten fraud cases touch the contact centre in some way.

Fraud tactics clearly vary from one case to the next, but there are some common patterns. Fraudsters often use IVR systems to validate information such as recent transactions – which they can then use to conduct fraud more successfully through other channels. They also regularly contact banks to validate payments and remove existing fraudulent activity flags. Another method is to gain control of customer phone numbers via SIM swaps, enabling them to bypass multi-factor authentication when committing fraud through a mobile or an app.

One of the key reasons why contact centres have become vulnerable to these kinds of frauds is that the function often falls outside of traditional corporate anti-fraud measures. The introduction of a more integrated approach to Fraud and Anti Money Laundering (FRAML) is looking within organisations to address this, with FRAML best practice now seeing customer identification as a key first stage in addressing the issue. Regularly reviewing key information such as mobile device identities, customer behaviour, and cross-channel transactions will be a vital stage in highlighting potential money laundering and fraud vulnerabilities.

One of the other troubling developments is the rise in Authorised Push Payment or APP fraud, where criminals trick victims into making fraudulent payments. And contact centres play a key role here too. Whether it's validating and harvesting personal data by attacking the IVR or employing smart social engineering fraud techniques when speaking with the contact centre frontline, fraudsters clearly see non-digital channels such as the contact centre as a good way to prepare for an APP attack.

To gain a sense of how today's Financial Services sector is addressing the challenge, Leigh Hopwood, the CCMA's CEO, asked customer service and fraud/risk leaders how their own organisations were working to combat the threat of fraud in contact centres.

How do you set about combatting contact centre fraud?

Monzo Bank's Nick Andrews believes that customer service teams need to be aware of the challenges that may come up when they are on a call. **"We have a really structured agent onboarding process, so that our people become familiar with fraud calls and understand how to approach them. However, they can still be quite daunting so we always have a floater – someone who's on call and available to agents and ready to provide them with the detailed technology knowledge and emotional support they might need. That's very re-assuring as we're a 24/7 operation and agents need to know there's help available."**

Alice Bush at Takepayments shared how they see some fraudulent activity play out: **"We get lots of people trying to call in and change details. They perhaps email first with no suspicions, then around three weeks later they'll call in to change a trading address which is more notable – particularly when you then look at how many changes there have been."**

IG Group's Mike Clark felt that it was important to always think about who has access to which systems. **"Line managers need to be looking at requests for access and calling it out if it doesn't seem right – even if this means having uncomfortable conversations."** Danielle Sack from TSB added: **"alerts are really powerful providing they are easily visible – it also helps to have stringent alerting for vulnerable customers. Additionally, it always makes sense to look at what else is happening out there that might signify unusual behaviour – making comparisons with branch networks, for example."**

Tactics for addressing contact centre fraud are also evolving. According to Tim Burton at Smartnumbers: **"many firms have used intelligent routing to divert fraud calls to a different group of people. Now there's a move towards flagging these calls and letting them progress, so we can collect more information before we deal with them."**

What fraud types are you dealing with at the moment?

At Allied Irish Bank's Direct AIB operation, Mandy McCormack reports **"a noticeable increase in mobile top-up fraud attempts – often for quite small amounts. The use of secure customer IDs is an important control in helping to support customers in preventing the attempts being successful. We're also seeing that customers are now much more confident in coming forward and reporting fraud which is great to see."**

Danielle Sack at TSB notices an increase in transactions means more are being flagged as fraud and triggering alerts: **"a lot of 'me-to-me' transactions happening at the moment, with money shifting from current to savings to another account. Another area is the decline in cash and a massive increase in the volumes of debit card usage, with greater plastic usage inevitably leading to more fraud alerts and customer friction."**

Nick Andrews at Monzo said **"fraudsters always seem to be one step ahead and, sadly, if they get access to a customer's phone it's hard to stop them. Recent cases include persuading customers to delete our app and then getting them to download a very convincing fake app that gives them access."** Within TSB's complex transactions team, Danielle looks to use video banking to help prevent higher value scams where possible – **"it can make a difference when trying to break the spell or prevent a fraudster''**

Tim Burton also referred to 'mousetrapping' – **"that's giving**

fraudsters a code that takes them to a phone line that they don't control – leaving them no choice but to reveal themselves in a non-digital way."

What difference has the introduction of PSR regulations made?

With the UK Payment Systems Regulator (PSR) implementing a 50:50 shared liability split between sending and receiving institutions for victims of APP fraud, there has clearly been an impact across the financial services sector.

Tracy Lawlor from Starling Bank sees PSR as **"a major shift – in that it introduces significant obligations for firms. It also means that any payment meeting a certain pattern, or a particular shift will come into consideration (as potential fraud)."** Danielle Sack considers PSR to be a more consistent approach across the industry: **"whether you're first, second or third in the APP fraud chain, the scam started at the first place. Why should the third place be solely liable?"**

For Nick Andrews, there are some concerns though: **"we're seeing a trend of people not always understanding how to look after themselves or what precautions they can take. The consequence is that they depend on the assurance of being able to reclaim their money through their bank(s). We need to ensure that we support people with better education and better technology, where possible."** Mandy McCormack from AIB Bank agrees, saying **"people are now much more confident in coming forward if they have been the subject of fraud – we're certainly seeing customer more confident and comfortable in reporting fraud."**

How does it work in practice – should teams be working together?

Mark Williams from Optimus Cards asked: **"In terms of bringing customer service and fraud together, would it be best for fraud teams to work alongside colleagues in the contact centre?"** Mandy McCormack said **"our Risk & Innovation team sits within AIB Bank's contact centre, giving our advisors access to the skills of a centralised financial crime team.**

Starling Bank's Russell Atkins felt: **"it's important that we're doing everything we can to help advisors – especially as calls are getting more complex and our contact centres are the first point of contact when it comes to managing fraud. Both customers and advisors need better protection, but that's hard if you've got a disjointed structure in place."** Mark Williams agreed, saying: **"we need our contact centre people to start thinking like fraud investigators and, in doing so, help protect the business from potential fraud."**

"We're always focused on making the customer journey

as easy as possible, and our advisors are of course fixated on getting things right for CSAT, NPS and customer reviews, so we know that interruptions and any additional friction won't always be welcome," added Alice Bush from Takepayments. **"Ensuring fraud prevention can be frustrating for customer service teams, but we need to recognise that by not being challenging enough we're potentially exposing customers to fraud."**

What's happening with AI? Is it being used yet to support fraud and risk management?

Sean Gilholme from Atom Bank said: **"AI has the potential to really help in tracking fraud – by picking up on spend locations, frequency, or value – and using that information to highlight any anomalies. It's important to make use of the data you've got, but also to make sure that any actions taken only add friction to the customer journey at the right times."**

"There's no doubt that fraudsters will be seizing the AI opportunity, and we need to make sure as an industry that we're operating on the same level."

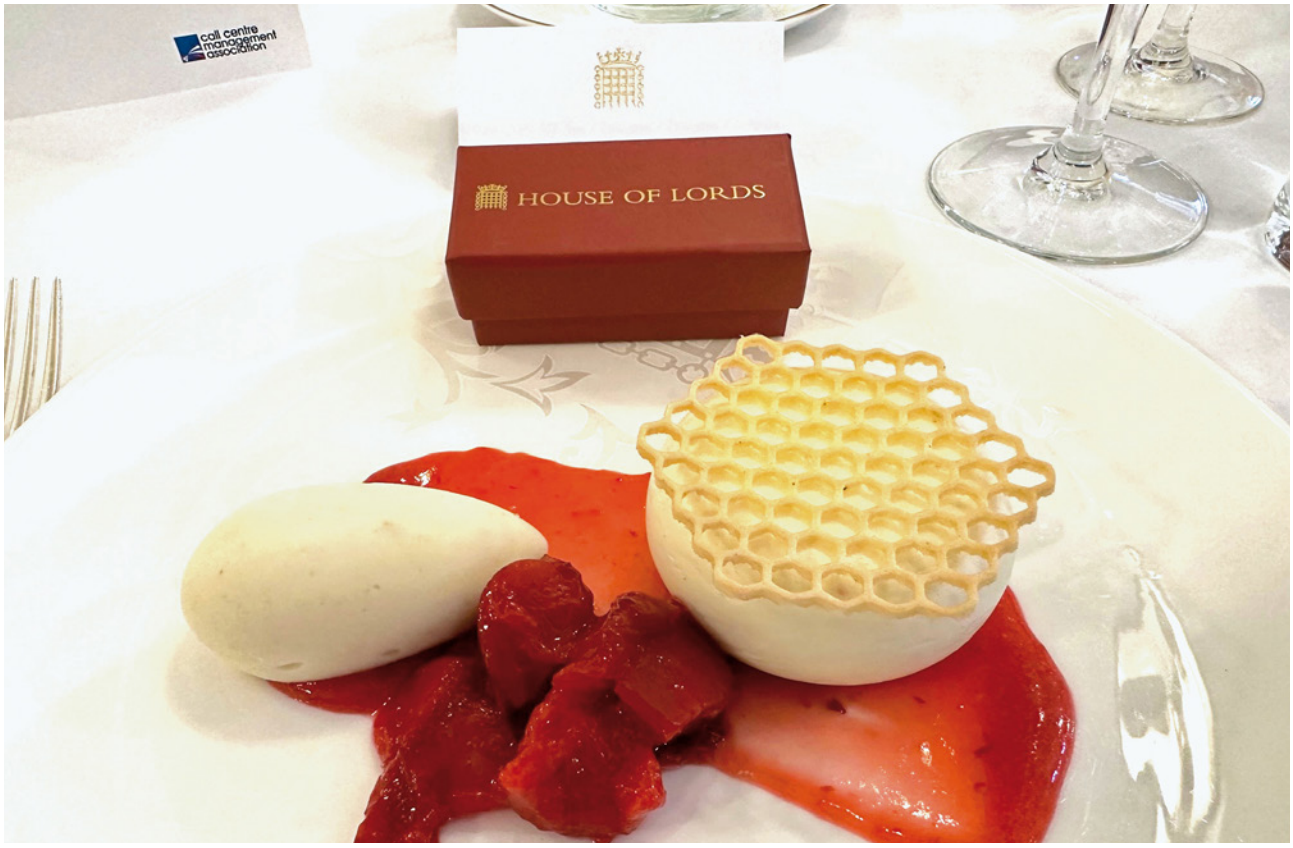
"At IG Group we've been trialling a ChatGPT-based AI model that we've been using to help our advisors get a sense of what AI could offer, and they have been getting closer to the process by scoring responses" explained Mike Clark. "**I'm sure we'll be adding AI to our toolset, but we're only really at the very early stages."**

What other innovations do you see coming up that could be helpful?

We also asked forum attendees whether there were any specific innovations emerging that could be helpful in helping contact centres to address their fraud challenges. Sean Gilholme felt that **"there was a need to improve the technology around monitoring customer interactions and picking up on any anomalies that signalled potential fraud."**

For Mike Clark, the requirement was more about integration. **"We find that online teams know 'x', the payment people know 'y', while the contact centre focuses on 'z'. It would be great to have tools – no doubt AI-powered – that could bring all this together and help everyone to understand the different indicators of risk and what's happening across the wider business."**

Tim Burton also believed that financial services firms shouldn't overlook the value of enabling customers to act for themselves. **"Many financial service providers still want to keep services such as allowing customers to freeze and unfreeze their cards or manage overseas spending limits in-house. But why would a financial institution want to stop their customers from actively reducing risk?"**



What advice would you share around successfully balancing fraud and customer service objectives?

Wrapping up the conversation, Leigh Hopwood asked the group for any advice they would like to share with other leaders – particularly when it comes to successfully balancing fraud and customer service objectives:

- **Nick Andrews, Monzo Bank** – "Prevention is always better than the cure, so it's important to invest time up front. It's also smart to share best fraud prevention practices across the industry as we'll all benefit. And remember to speak to the frontline – they see it and feel it every single day."

- **Russell Atkins, Starling Bank** – "It's essential to keep on closing the gap between customer service and financial investigation teams – prevention and detection is a valuable service that is needed to support all our customers."

- **Tim Burton, Smartnumbers** – "Financial services organisations need to acknowledge that their cost of service models are very different now compared to five years ago – and this has led to conversations with lots of different people. Prevention is always better than later resolution – that means, for example, being able to ID mule accounts before a fraud occurs as 70% of cases move money within 15 minutes! I would also encourage CX and fraud teams to experiment with AI, but do it I in a safe and controlled space. One of the best potential AI applications should be agent empowerment, with passive safety nets that can protect against loss without agents having to spot the risk. That's important as the most critical interactions are still human to human."

- **Mandy McCormack, Allied Irish Bank** – "It's all about constant coaching and education, with the frontline CX and fraud investigation teams working together and continually learning from each other. We're now in a world where most of the easy conversations have gone, and fraud issues now sit at the heart of many of our more complex discussions."

- **Mark Williams, Optimus Cards** – "We see Customer Service and Financial Crime as intrinsically-linked and it works so much better if there's a close relationship between the two functions."

- **Tracey Lawlor, Starling Bank** - "We need to make sure that we always look at the customer journey and understand the downstream impact of the decisions that we're making on customer service and risk. Starting from the customer perspective, we need to be thinking of how less or more of the friction associated with risk is likely to affect customers and contact centre people."

- **Jamie Crewe, Close Brothers** – "We've got to keep on listening to customers and discovering exactly what they need to improve their experience."

- **Danielle Sack, TSB** – "There are a few areas that I feel are important. Equipping customer service colleagues with comprehensive training and a range of skills to deal with customers' needs whilst reducing the friction of multiple hand-offs. PSR shared liability will also have an impact here, driving a potential need to look at claims with two lenses, thus increasing the importance of quality training and competence. Firms will need to balance the demands of fraud prevention strategies versus supply to service this demand, allowing the business to prioritise speed to answer whilst customers are in a potential vulnerable situation. Finally, creating a culture of change and continuous improvement will help colleagues to meet these challenges."

- **Mike Clark, IG Group** – "Judging the right mix of customer service and friction can be a hard balance to find – but it's critical that you don't hold back on introducing controls into the equation when you know you've got risk."

- **Dean Docherty, Marcus by Goldman Sachs** - "While the PSR's 50-50 shared liability split may increase the operational burden on some financial services firms, we mustn't forget our responsibility to customers. The new generation of behavioural tools will continue to help in tackling fraud, and there's a huge amount to be gained by sharing data across the industry."

- **Alice Bush, Takepayments** - "Of course the focus needs to be on providing great CX, but don't be afraid of adding in extra friction to reduce fraud – lots of stress for the right reasons is OK."

- **Sean Gilholme, Atom Bank** – "Don't be complacent – we're working in an ever-evolving landscape with fraud. You might have a good defensive record, but that doesn't mean you can't get better at defending against fraud."

- **Matthew Addison, Smartnumbers** - "A greater focus on collaboration would make a huge difference. Sharing details of fraudsters will help strengthen prevention and provide increased protection for customers."

About the CCMA

For 30 years, the CCMA (Call Centre Management Association) has been the longest established contact centre industry body who are dedicated to supporting contact centre leaders across the UK.

Founded on the principles of sharing best practice and networking to improve skills and knowledge, the CCMA is a thriving community that represents leaders from a huge cross-section of the industry.

Membership of the largest contact centre community offers unique opportunities, such as free annual benchmarking of 25+ KPIs, access to become an Accredited Contact Centre with the Contact Centre Standards Framework, free entry into the UK National Contact Centre Awards, free tickets to the UK National Contact Centre Conference, invites to Executive Networking Dinners and Leadership Forums, and other exclusive events for members-only. Members also benefit from discounted training through the UK National Contact Centre Academy, the industry's training partner.

To support the industry further, the CCMA conducts regular original research for download, including the annual Voice of the Contact Centre Consumer research, the Evolution of the Contact Centre tracking the industry's progress and Good Practice Guides on a variety of topics.

www.ccma.org.uk

About Smartnumbers

We help companies in the fight against fraud.

Our solutions help protect organisations from downstream fraud by ensuring the contact centre stays secure.

Our cloud-based AI-powered platform - Smartnumbers Protect - analyses call signalling data, caller behaviour and data on known fraudsters shared by our customers to assign a risk rating to incoming calls. This helps contact centres prevent downstream fraud and improve customer experience for genuine callers.

Through the Smartnumbers Consortium, our community of customers and partners share intelligence in real time on the fraudsters they know. Organisations are also able to connect and collaborate through Smartnumbers Consortium events.

www.smartnumbers.com

call centre management association

0333 939 9964 | www.ccma.org.uk | info@ccma.org.uk