Fraud and the Contact Centre: What Can You Trust?

Autumn 2025

CCMA Contact Centre Management Association

Supported by smartnumbers

CCMA Leadership Series | **Fraud**

CCMA Leadership Forum Series

The Leadership Series is the documented output from the CCMA's series of Leadership Forum roundtables. These 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 their industry - and to consider how to continue innovating and adding value for the benefit of the customer, colleagues, and the business.

Leadership Forum Attendees

James Forsyth, Head of Fraud, Bupa UK

Phil Quickenden, Head of Customer and Registrations Services, Camden Council

Caitlin Neary, Director, Global Contact Centre, Dorchester Collection

Claire Carroll, Head of Service Operations, Hargreaves Lansdown

James Revell, Customer Experience and Contact Centre Director

Nic Hartley, VP Seller Operations, Motorway

Paul Whymark, Chief Operating Officer, Sensée

Marco Ndrecaj, Director of Contact Centre Services, Sopra Steria

How Prevalent is Contact Centre Fraud?

In an age where seeing is no longer believing, a vital question is being asked societally: who - and what - can you trust? From the rise of deepfakes to the increasingly sophisticated use of artificial intelligence (AI) and social engineering, fraudsters are seemingly able to tap into ever-increasingly complex and innovative ways to commit fraudulent activities.

However, as discovered during this Leadership Forum discussion, the contact centre continues to provide an opportunity for fraudsters to attack with some surprisingly routine methods too.

The contact centre is considered a weakness by fraudsters. Contact centres can represent the 'path of least resistance' for criminal networks targeting businesses. Leaders stated that while their organisations invest heavily in securing digital channels, voice remains comparatively under-invested. Fraudsters can exploit this imbalance, knowing that contact centres are often designed to prioritise customer experience versus overzealous security protocols.

Change of address requests remain a major red flag. High-risk customer journeys, particularly change of address and phone number requests, continue to be primary fraud approaches. These routine interactions provide fraudsters with account takeover opportunities that can have devastating consequences.

Fraudsters often possess enough stolen data to pass standard identification procedures. The rise in organisational data breaches and phishing has led to an increase in fraudsters obtaining enough personal details to bypass standard identity checks with some organisations, allowing them to impersonate victims to gain access to accounts, open new lines of credit or apply for benefits.

Trust continues to be a two-way street. Leaders said their organisations face a balancing act between customer experience and fraud prevention. Maintaining customer trust requires careful calibration. Overly suspicious approaches can damage legitimate relationships, while excessive trust enables exploitation. It was agreed the most effective strategies were those that aimed to remove fraud detection responsibility from frontline advisors through technology and specialist teams.

AI gives fraudsters more scale. AI technologies enable criminals to operate at industrial scale, processing significantly more targets per hour than traditional methods. Deepfake technology and sophisticated social engineering techniques make detection increasingly difficult. However, AI also offers defensive opportunities, with some leaders stating their organisations deployed automated fraud detection systems trained to spot suspicious patterns and behaviours.

Taking action can be a major challenge. Even when fraud is detected, organisational responses can occasionally lag. Leaders stated that success requires clear escalation procedures that protect both customers and frontline colleagues.

The Evolving Threat Landscape

The sophistication of fraud has escalated dramatically. Where manual fraud operations might have reached five victims hourly, AI-assisted techniques now enable fifteen or more. This acceleration isn't limited to volume – the quality and credibility of attacks have improved correspondingly, with deepfake technology and sophisticated social engineering making detection increasingly difficult.

Some criminal operations involve careful reconnaissance phases, with criminals often beginning in Interactive Voice Response (IVR) systems to test stolen credentials before engaging human advisors. IVR can often be a 'fraudster's best friend', providing opportunity to validate information without human scrutiny.

Contact centre leaders are acutely aware of the challenge and pitfalls presented to them by fraudsters, even when they're not directly involved.

"We're a BPO (Business Process Outsourcing) with a number of clients in financial services," said Paul Whymark, Chief Operating Officer, Sensée.

"The amount of fraud we're hearing about now is huge but we're lucky that our clients are at the forefront of tackling these issues. That doesn't mean we can be complacent in any way. Fraud can occur both externally and internally and is a worldwide operation, so you have to stay alert and informed."

Organised groups coordinate attacks across multiple organisations simultaneously, demonstrating that fraudsters aren't industry loyal. The same networks targeting banks are exploiting retailers, energy providers, public sector bodies and hospitality firms. And while sophisticated methods of attack are on the increase, rudimentary approaches remain commonplace too.

In the hotel industry, for instance, while the overall volume of criminal activity targeting contact centres can be relatively low, there are still regular attempts by fraudsters to exploit these channels.

Common tactics include callers trying to obtain information about guests, which poses significant data protection challenges. Fraudsters may impersonate guests, their staff, or third parties in an effort to bypass verification processes.

These situations can be particularly sensitive when dealing with high-value reservations or high-profile individuals. Robust training and strict identification procedures are essential to protect guests, prevent reservation fraud, and maintain the highest standards of data security.

In sectors such as financial services and insurance, the issue of fraud is multidimensional. "Like most insurers, we've seen an increase in customer fraud – usually they are fictitious claims and reimbursement requests," said James Forsyth, Head of Fraud, Bupa UK.

"We believe this is driven by the increasing NHS pressures and cost of living challenges. This means that a very small minority of customers who do need treatment take out policies with the intention of claiming fraudulently. As an insurance company we have controls in place and these have improved, meaning we're identifying more fraud. But it is an area of concern and risk."

A Challenge on All Fronts

The scope of organised fraud can be substantial. One leader reported that at one point their organisation had detecting a single coordinated group comprising 63 individuals operating systematically across their channels. The challenge of taking action against such networks – even once detected – remains significant due to legal complexity, resource constraints and the speed at which criminal operations adapt.

Internal fraud presents an equally concerning dimension too. Leaders reported cases of criminal 'plants' successfully completing training programs before switching identity at go-live, or new recruits specifically hired to facilitate fraud from within contact centres. In financial services, instances have emerged of internal actors making fraudulent account clearances, while other sectors report wrongful dismissal claims involving AI-generated supporting documentation.

The challenge intensifies with remote working arrangements, which create additional security vulnerabilities that criminal networks might exploit. Remote environments can complicate verification of colleague identity, monitoring of security protocols and enforcement of multi-factor authentication requirements.

Understanding the 'Fraud Cycle'

A key discussion point at this Leadership Forum was that seemingly routine interactions provide account takeover opportunities. The fraud cycle follows predictable patterns: data breaches and phishing attacks enable criminals to build customer profiles, which facilitate account takeovers, which enable money laundering and goods acquisition. Fraudsters harvest information through multiple small interactions – a phone number here, an address confirmation there – building comprehensive profiles over time.

The risk exposure is significant, so organisations have to establish which customer journeys present the highest risk and apply appropriate controls, whilst also protecting the customer experience. Contact centre leaders state they are acutely aware that every interaction represents potential information exchange that could enable future fraud.

Balancing Trust and Security

Contact centre leaders face persistent tension between maintaining customer trust and implementing robust fraud prevention. The philosophical challenge runs deep.

"We empower people in customer care roles to say "yes" but we also empower them to be vigilant and to know when it's OK to say "no"," said James Forsyth. However, this shift creates cultural challenges and could effect legitimate customer relationships if applied without nuance.

Other organisations have taken alternative approaches, deliberately choosing trust-first strategies. "I'm trusting and very proud of winning awards for our Voice of the Customer programme because we ripped up the rulebook and we believe our customers," noted Claire Carroll, Head of Service Operations, Hargreaves Lansdown. "You have to believe the customer. We have to get better on the back-end systems and allow the frontline to have the belief that the customer is always telling the truth."

Phil Quickenden, Head of Customer and Registrations Services at Camden Council said that as a public sector organisation, there was a natural tension borne out of over-policing fraudulent activity. "Our moral duty is to protect the public purse, but counterbalancing that we're protecting the public purse by not overspending on [security] checks we don't need to do. It's a very tight balance for us," he said.

The AI Conundrum

The consensus among leaders is increasingly clear: fraud detection responsibility should not rest primarily with frontline advisors. These colleagues are trained to deliver exceptional customer service, not to interrogate customer authenticity. As Hargreaves Lansdown's Carroll emphasised, "I don't want the responsibility to sit with my frontline colleagues".

Effective strategies remove this burden through technology investment and specialist team deployment. Traffic light systems that highlight at-risk transactions, back-end alerts identifying suspicious patterns and routing high-risk interactions to trained specialists protect both customers and frontline colleagues.

And while AI presents dangers for organisations, it also presents the opportunity to use it to protect customers.

While criminals leverage it for deepfakes and scaled operations, organisations can deploy it defensively to identify repeat patterns, spot behavioural cues and detect anomalies at industrial scale.

Some public sector organisations now employ Agentic AI trained to security standards matching human colleagues, with virtual bots handling straightforward queries and flagging suspicious activity. "An AI can spot cues," explained Marco Ndrecaj, Director of Contact Centre Services, Sopra Steria, which is an organisation that processes £32bn in public sector supplier payments annually, making it an ongoing target for attempted fraud.

A Renewed Focus on Telephony

The fundamental question remains stark: do organisations truly know who is calling into their business? With investment ratios heavily favouring digital channels, contact centre security arguably requires a renewed focus. "Businesses are in trouble if they are completely ignoring the contact centre as a potential target," added Sensée's Whymark.

Addressing this imbalance requires dedicated resources, specialist capabilities and leadership recognising that voice channels demand security investment that matches the risk exposure.

Avoid Being the 'Slowest Gazelle'

What advice do contact centre leaders give to their peers looking at how to tackle fraud?

"Payment integrity controls are everyone's responsibility. Stay aware of what to look out for and accept that fraud is happening. This isn't new, it's just different in its approach."
James Forsyth, Head of Fraud, Bupa UK

"Finding the right balance on the trust continuum is crucial. While fraud's impact may seem distant from contact centres, we're actually a clear target. Contact centres have a vital role in addressing fraud."
Phil Quickenden, Head of Customer & Registrations Services, Camden Council

"Educate yourself by understanding fraud patterns in other industries. This helps you anticipate and prepare for what's likely to emerge in your own sector later."
Caitlin Neary, Director, Global Contact Centre, Dorchester Collection

"Fraud prevention should be AI and tech-driven. We can't place more burden on our advisors. Instead, give them the technology and freedom to do their jobs effectively.
Claire Carroll, Head of Service Operations, Hargreaves Lansdown

"Build better defences, but expect smarter criminals. Keep frontline teams informed and establish fraud detection experts within your teams. Don't be complacent – criminals seek the easiest targets."
James Revell, Customer Experience & Contact Centre Director

"Hire the right people and prioritise security as your first defence. Focus on data and pattern detection – you can't expect advisors to catch everything manually. What protections do you have?"
Nic Hartley, VP Seller Operations, Motorway

"Fraud hides among legitimate transactions using sophisticated methods. Criminals target the path of least resistance. You just need to avoid being the 'slowest gazelle'. This threat is constant and real."
Paul Whymark, Chief Operating Officer, Sensée

"Fraud isn't new, but investment in it is growing. Know your people, build individual capabilities to distinguish normal from abnormal transactions and implement quality checks to future-proof operations."
Marco Ndrecaj, Director of Contact Centre Services, Sopra Steria

About the CCMA

For more than 30 years, the CCMA has been dedicated to supporting contact centre leaders. We push ourselves to do more for our thriving membership base, which is the largest community of industry professionals in the UK.

The CCMA was founded with the goal of sharing best practice and networking to improve skills and knowledge in order to progress contact centre operations – and we live by that to this day.

We give those who work in contact centres the chance to discuss ideas and share experiences through member-only Special Interest Groups and online and in-person events. Member organisations are invited to become Accredited through the Contact Centre Standards Framework and get independent guidance on where they can improve. There is the opportunity to compare operations against industry standards and 25+ KPIs, via our annual CCMA Benchmark.

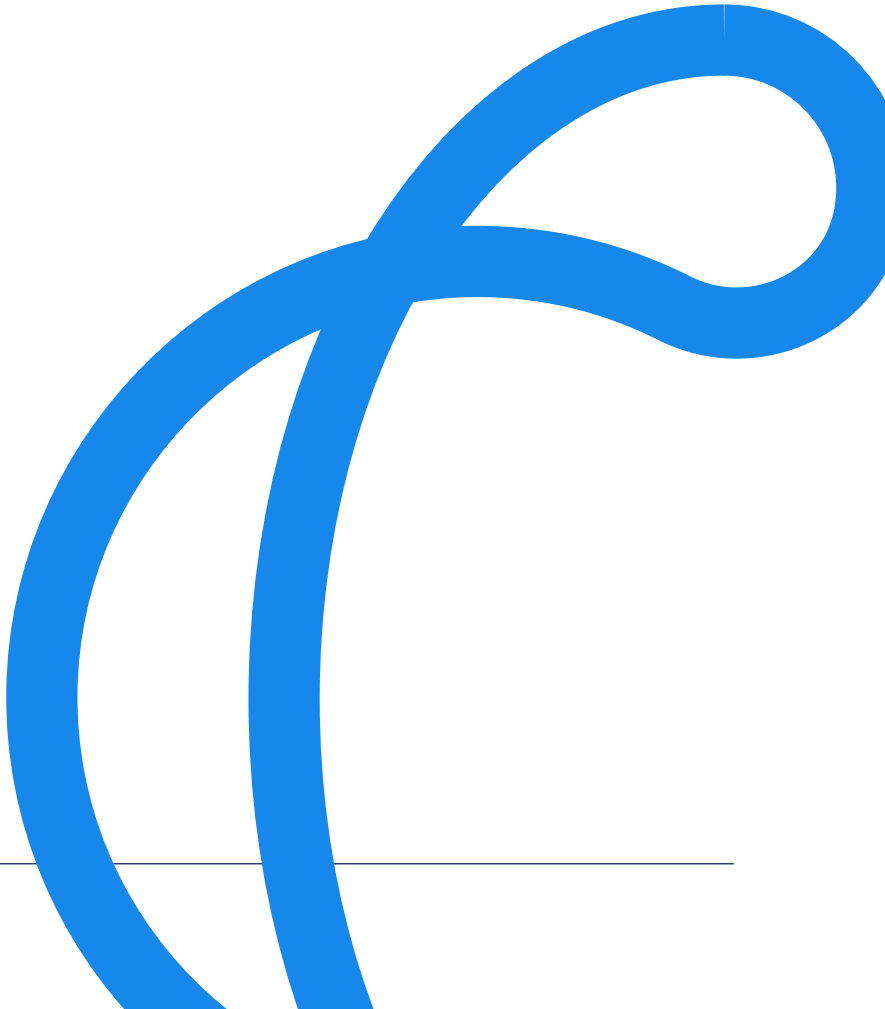
Our training arm, CCMA Academy gives contact centre professionals at all levels a structured learning opportunity to support both personal and professional development for the benefit of their operations. We also celebrate the progress our industry is making through the UK National Contact Centres Awards. Those that win go on to share their stories through channels such as the UK National Contact Centre Conference, Best Practice Visits and CareerTalk, while also providing input into our Special Interest Groups and other events.

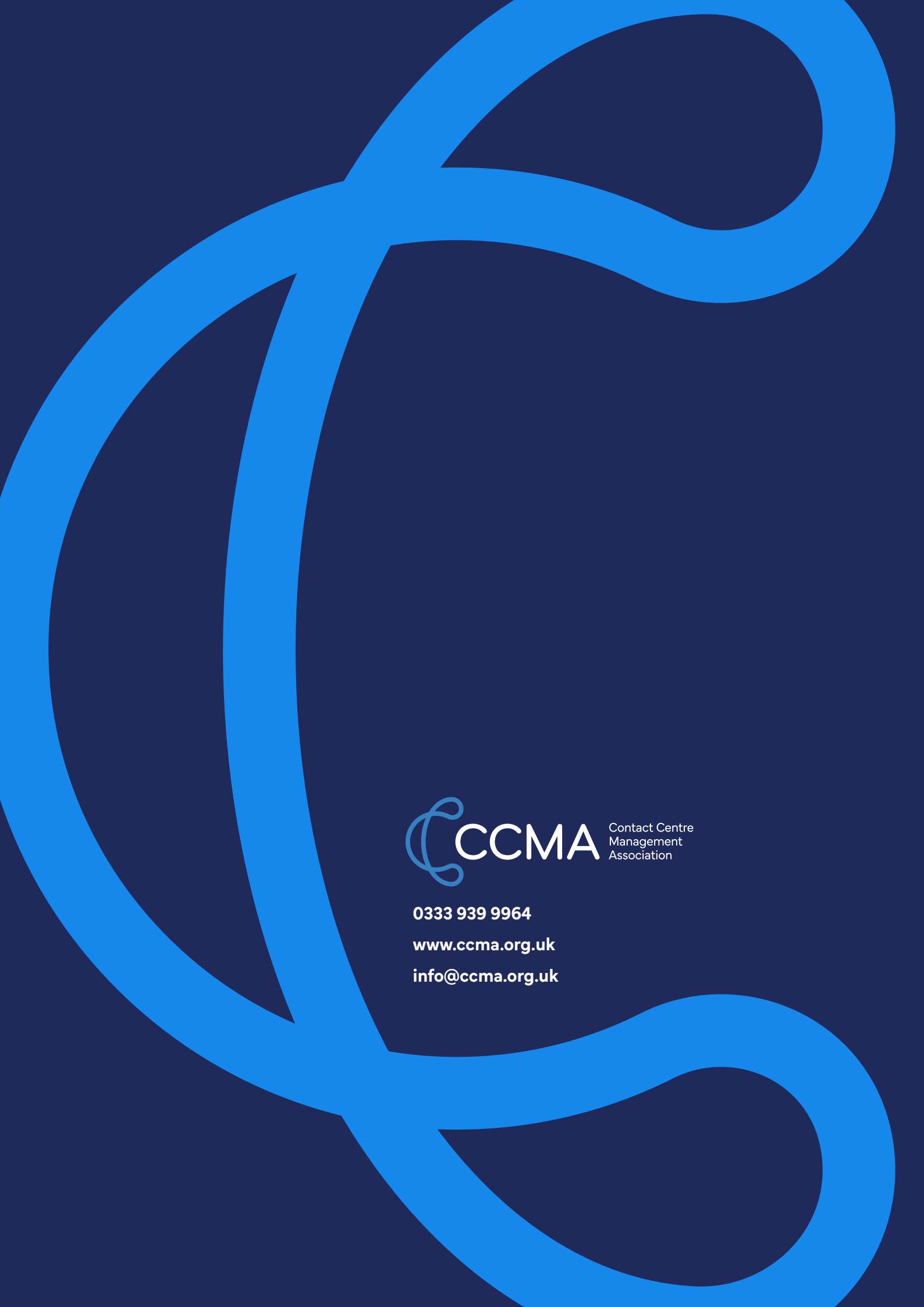
www.ccma.org.uk

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. Smartnumbers assigns a risk score to incoming calls before answering by analysing call data, caller behaviour and confirmed fraudsters identified by other members. Through the Smartnumbers Consortium, members share intelligence in real time on the fraudsters they know, enabling them to play an essential role in disrupting organised crime.

www.smartnumbers.com





0333 939 9964

www.ccma.org.uk

info@ccma.org.uk