CCMA Contact Centre Management Association

Supported by smartnumbers

Turning Your Contact Centre into a Proactive Crime Prevention Hub

Fraud is one of the most significant threats facing organisations, and the contact centre provides an attractive point of entry for fraudsters. This Good Practice Guide offers practical, actionable instructions to help organisations start the process of transforming their contact centres from reactive fraud targets into proactive intelligence hubs that can detect and disrupt organised crime, before it causes harm.

Criminal fraud continues to pose substantial risks to organisations, representing 40% of total crime across England and Wales.[1] Today's fraudsters operate with increasing complexity, deploying organised networks that systematically target multiple enterprises through every accessible channel to exploit operational weaknesses.

Contact centres present particularly appealing access points for criminals, offering opportunities to harvest sensitive data, validate compromised credentials and manipulate employees through social engineering to reveal information or carry out transactions.

Through adopting a strategic shift from reacting to isolated incidents to monitoring and disrupting entire criminal operations, contact centres can spot fraudulent behaviour much earlier in the process and provide superior customer protection.

Based on established methodologies from prominent organisations, this guide demonstrates how to combine advanced call metadata analysis, call patterns and cross-industry intelligence sharing with cultural and process changes - to establish proactive crime prevention capabilities.

What's the Urgency?

Criminal fraud activity continues expanding in both volume and complexity:

- £1.7 billion (and increasing) is extracted from UK consumers annually via authorised and unauthorised payment fraud. There's been a 1,400% surge in documented incidents over the past decade.[2]
- Criminal organisations routinely target numerous organisations, such as financial providers, airlines and telcos, simultaneously - frequently testing account security before launching comprehensive fraud attempts.
- Contact centre representatives face sophisticated social engineering attacks designed to extract confidential information or execute unauthorised account changes. Internal intelligence from several organisations reveals that significant fraud incidents frequently involve contact centre touchpoints, even if the fraud takes place online.[3]
- Criminals deploy spoofed or withheld IDs to conceal their identities, making it harder to validate whether calls are suspicious. AI and automation tools are making it easier to launch attacks at scale, for example by executing multiple, brief calls to automated systems such as IVRs (Interactive Voice Response) to verify compromised credentials.

An Opportunity for Contact Centres?

Contact centres represent both potential security gaps and strategic opportunities. With appropriate technology, procedures and organisational culture, they can transform into valuable intelligence sources for detecting and preventing fraud earlier in the criminal process. For instance:

- **Recognising suspicious calls** before IVR or advisor engagement, via automated risk analysis.
- **Connecting separate fraud incidents** and the phone numbers used to identify criminal organisations operating across various customer accounts.
- **Revealing concealed threats** and exposing callers operating behind withheld or spoofed numbers.
- **Preserving customer trust** while implementing enhanced verification for high-risk calls.
- **Preparing frontline colleagues to respond decisively** when confronting questionable caller behaviour.
- **Facilitating secure, rapid intelligence distribution** between internal departments and other organisations.

Getting Started

Developing effective fraud prevention capabilities begins with forming appropriate multi-disciplinary teams.

It's vital to unite stakeholders from fraud prevention, contact centre, technology and compliance teams, to define clear project scope and success metrics.

After establishing alignment with stakeholders, concentrate on assessing current security exposures. For example, examine historical fraud incident data, including associated phone numbers, and document typical fraudster contact centre access methods and the fraud types they are known for. Make sure your deny lists are up to date with numbers from fraud teams in other departments.

This groundwork enables contact centres to identify and focus on high-risk situations, including identifying systematic testing of account details within IVR systems, take prompt action.

A CCMA Good Practice Guide

Effectiveness requires strengthening frontline capabilities and leaning on internal and external fraud intelligence. Create straightforward escalation processes, enabling your frontline colleagues to confidently recognise and address suspicious interactions.

Concurrently, engage with industry intelligence-sharing networks and technology platforms that enable collaboration with other organisations and access to their insights regarding active fraudster methods and developing threats.

Implementation Considerations

It is recommended to evaluate new technology strategies through controlled pilot programmes, enabling rapid value demonstration, monitoring both financial protection metrics and operational improvements such as enhanced frontline assurance.

- **Stakeholder Coordination.** Clearly outline objectives, responsibilities and oversight with your vested teams.
- **System Integration.** Confirm any fraud detection tools integrate effectively with your telephony, CRM and risk assessment platforms.
- **Organisational Transformation.** Develop analytical thinking approaches and establish intelligence-sharing as core operational practice.
- **Ongoing Enhancement.** Consistently evaluate fraud trends and modify protective measures to maintain advantage over evolving criminal methods.

Tackling fraud requires a shift from reactive to proactive thinking. Through combining call analytics, proactive risk identification and integrated operational workflows, your contact centre can become the central hub for tackling fraud.

Proactive Fraud Prevention: A Nine Step Approach

1. Undertake Risk Assessment

Use call metadata to identify blocklist matches, even if a number is spoofed or withheld, and abnormal calling behaviours before a call is answered. This provides early threat warnings enabling preventative measures without affecting legitimate customers.

2. Monitor Reconnaissance Activity

Observe call patterns, for example, multiple, brief calls or irregular navigation of automated systems (such as IVR) to indicate suspicious activity. Early detection enables account protection before fraudulent transactions can occur.

3. Look Beyond Individual Incidents

Connect phone numbers, voice characteristics and tactics to develop comprehensive fraudster profiles.
This reveals the scope of criminal activity and can help identify connections between seemingly separate attacks.

4. Integrate Frontline Systems

Incorporate real-time call risk indicators and known criminal profiles into customer management or transaction platforms, enabling appropriate frontline advisor responses during active calls.

5. Establish Specialist Response Teams

Create dedicated fraud teams to evaluate alerts, validate threats and orchestrate rapid cross-departmental responses.
These teams maintain and enhance fraudster profiles for continual circulation and review.

6. Enable Industry Collaboration

Work with your IT and cybersecurity leaders to establish pathways to exchange timely, actionable information with partner organisations.
This can help prevent criminals from exploiting multiple institutions undetected.

7. Balance Security and Customer Experience

Apply enhanced verification exclusively for high-risk communications while simplifying authentication for standard interactions.
Communicate additional security measures clearly to customers.

8. Empower the Frontline

Deliver ongoing training covering emerging criminal tactics, communication and social engineering strategies and escalation protocols - ensuring frontline advisors feel confident to address suspicious behaviour.

9. Monitor, Improve and Promote

Measure prevented losses, criminal network disruption, reduced telephony-based fraud and customer satisfaction levels.
Use insights to enhance detection algorithms and operational procedures. Promote the impact your approach is having on both your customers and the business – as well as any success metrics, including financial savings.

[1] National Crime Agency (2025). The Threat from Fraud. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
[2] UK Finance (2025). Annual Fraud Report 2025. https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release
[3] UK Finance (2025). Annual Fraud Report 2025. https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2025