FourNet®

Using Data to Spot and Stop Fraud in the Contact Centre

Why Contact Centres are the Ideal Target for Fraudsters

The scale of the problem

01

40%

Of all crime in the UK

61%

Of fraud interacts with a contact centre

79%

B2B organisations reporting attempted fraud

35%

Increase in account take over last year

£1.2bn

Reported Cost of Fraud

14%

Estimate of actual fraud reported

Fragmented Defense : Why Scammers Succeed

Silo 1 ***NETWORK***	**The Network Silo:** Traditional network firewalls have no visibility into caller *intent* or *context*. They can block numbers, but not sophisticated, spoofed, or novel threats.
Silo 2 ***IVR***	**The IVR Silo:** The IVR (Interactive Voice Response) system likely treats every caller with the same level of suspicion. It has no pre-call context, forcing genuine clients to endure high-friction authentication processes, while attackers can simply probe the system
Silo 3 ***Agent***	**The Agent Silo:** The agent is "blind." When a call is connected, they have no way of knowing if the caller is a high-value, legitimate client or a known / suspected fraudster deep into a social engineering script. They are forced to become interrogators, which damages the customer relationship.
Silo 4 ***QA***	**The QA Silo:** The Quality Assurance team is looking for a needle in a haystack. With manual, random sampling, they may review less than 2% of calls, making it statistically impossible to find the 1-in-500 malicious calls that matter

The problem is not a deficiency in tools, but a critical deficiency in data-sharing between them. The attacker knows:-

- ***the IVR is "dumb,“***
- ***the agent is "blind,"***
- ***the QA approach is "random."***

The core of an effective strategy is to connect these silos with a single thread of real-time intelligence in data-sharing between them.

The “Fraud Formula” structured approach fraudsters will target you with

02

1. Reconnaissance	PII from breaches, social media, public websites
2. Target Selection	Pick high value and / or data rich accounts
3. Preparation	Scripts, spoof numbers, fake emails, mules
4. Initial Contact	First test of script and techniques
5. Verification Bypass	Social Engineer Agent
6. Execution	Change account setting, payments & transfers
7. Covering Tracks	Change and delete details and collect money from mules

Conversational cues that help you spot fraudulent activity

03

FourNet®

1

Declaring vulnerabilities

2

Urgency & Pressure Tactics

3

Change Of Account Details followed by sensitive transaction

4

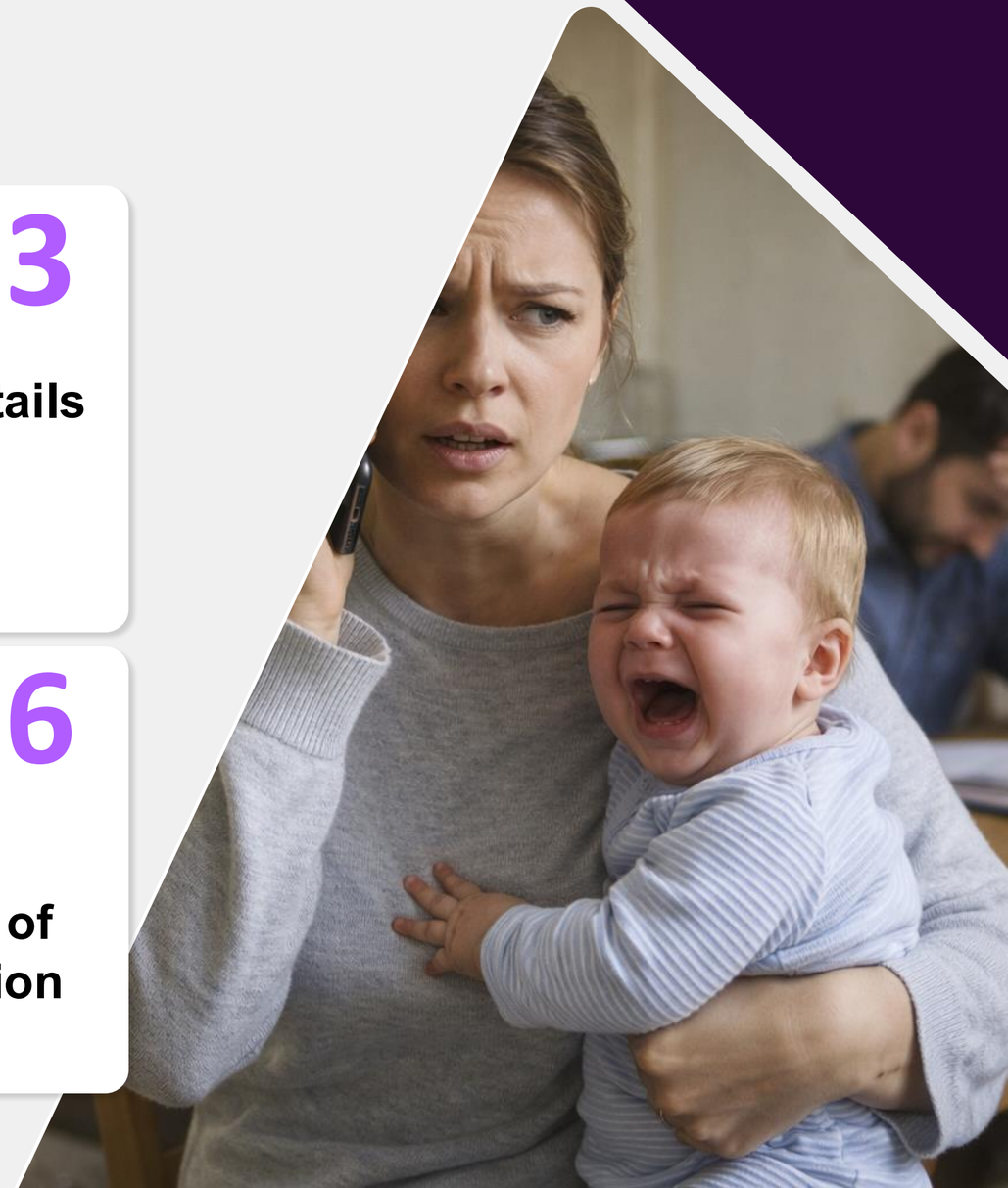
Hesitation and unnatural cadence

5

Use of Background Noise… crying babies

6

Attempts to take control of the verification process



Detection techniques

Investigation 1 ***Scam Signatures***	**We can build a "fraud dictionary" based on the known tactics of the B2B attackers.** • **What we look for:** This includes not just obvious terms like "account takeover" or "unauthorized access" , but also more subtle "scam signature" phrases. These are the specific, repeated questions used in the reconnaissance phase, such as "Can you just confirm the administrator's name?" or "What's the B2B payment address you have on file?" • **Why it works:** This immediately flags calls that match the known B2B fraud campaign, prioritizing them for manual review and allowing you to flag the associated accounts for enhanced monitoring.

Investigation 2
Social Engineering
	This technique looks at how people are speaking and just not what they are saying.
	• **What we look for:** We analyze transcripts for "linguistic cues" associated with manipulation. This includes:
	  • **Urgency Cues:** Phrases like "I need this fixed immediately" or "This is an emergency".
	  • **Ambiguous or Vague Language:** Repeated use of vague terms or a high density of probing, "ambiguous questions" designed to confuse the agent and extract data.
	• **Why it works:** This helps find sophisticated attackers who avoid specific keywords. A call with high urgency cues, low agent-talk time, and a high density of questions is a classic high-risk pattern.

Investigation 3 ***Sentiment & Emotion***	**Emotional Tones Can Reveal High Stress Events** • **What we look for:** We can scan all calls and tag them for specific emotional markers. We would flag calls with high levels of "customer frustration," "vocal stress," or "anger". We can also identify calls where the agent sounds stressed or uncertain. • **Why it works:** This creates two target groups. First, a spike in "customer" frustration can pinpoint a legitimate B2B client who *discovered* a fraud attempt and was trying to report it. Second, it can identify agents who were being pressured by a social engineering attack, allowing for a more targeted review of those interactions..
Investigation 4 ***Cross-Call Anomalies***	**Look beyond singular interactions to spot persistent account takeover attempts** • **What we look for:** We analyze the call logs for patterns and trends associated with fraudulent behaviour. The key indicator here is "repeated requests for account changes across multiple calls". An account that called five times in two days, spoke to three different agents, and asked about account details each time is a massive red flag. • **Why it works:** This tactic directly identifies the "Reconnaissance" and "Set Up" phases of the fraud lifecycle. It finds compromised accounts by their *behavioral footprint*, even if any single call was not obviously fraudulent.

How you can use Speech Analytics to defend your contact centre

Benefit 1
Streamline QA Effort

Tripwire for Potential Scammer Detection

This automation is your first line of defence. You can configure these **automated workflows to act as a "tripwire" for scammer-related behaviour**. For example, you can set rules to automatically flag and escalate any interaction that contains:

- High-risk keywords or customer behaviours identified in the Policy Section
- High-risk agent behaviour: Muting the call for an extended period, or an agent not following a required compliance script.

Instead of hoping to manually find a suspicious call automatically send the "smoking gun" directly to a manager for immediate review.

Benefit 2
Increase Evaluation Coverage

100% Coverage Means No Suspicious Conversation Slips Through The Cracks

- **Detecting Vulnerability:** AI can identify signs of **customer vulnerability** (e.g., a customer sounding confused, panicked, or distressed). This is a powerful dual-use feature. You can use it to protect customers, but also to flag interactions where a scammer might be *preying on* a vulnerable person.
- **Spotting Anomalies:** By analyzing all interactions, the AI establishes a baseline for "normal" agent and customer behaviour. It can then automatically flag significant deviations—such as an agent skipping key compliance phrases or a customer exhibiting unusual urgency combined with specific keywords ***manipulating agents.***

Benefit 3
Enable Compliance Reporting

Automate Compliance and Notify Managers to Allow Errors to Be Corrected Satisfying Regulator Needs

- **Immediate High-Risk Alerts:** You can configure the system to send **instant alerts to supervisors** the moment a high-risk interaction is detected (e.g., a call combines "panicked" customer sentiment with the keyword "bank transfer").
- **Pinpointing Non-Compliant Behavior:** Scammers, whether internal or external, actively avoid compliance. By auto-failing interactions that miss required identity verification steps or disclosures, you can instantly pinpoint agents who are either cutting corners or actively bypassing security protocols.

Benefit 4
Continuous Improvement

Train Your Agents to be A Human Firewall For Scammers

- **Identifying "Social Engineering" Patterns:** By analyzing all flagged interactions, you can identify the new scripts and tactics scammers are using. You can then build these "scammer personas" and tactics directly into your agent training and coaching modules
- **Proactive Agent Support:** You can use the platform to identify agents who are "too helpful"—for example, agents who are consistently trying to find workarounds for security policies to "help" a customer. The data allows you to coach these agents on *why* the security policies are in place, making them more resilient to social engineering attacks.

FourNet®

Register interest for Speech Analytics Assessment

Survey at the end of the webinar

Data cues that help you spot fraudulent activity

04

FourNet®

1

Short calls + high repeat rate

2

Callback patterns

3

Invalid or mismatched contact details

4

Failed authentication clustering

5

Unusual time of day

6

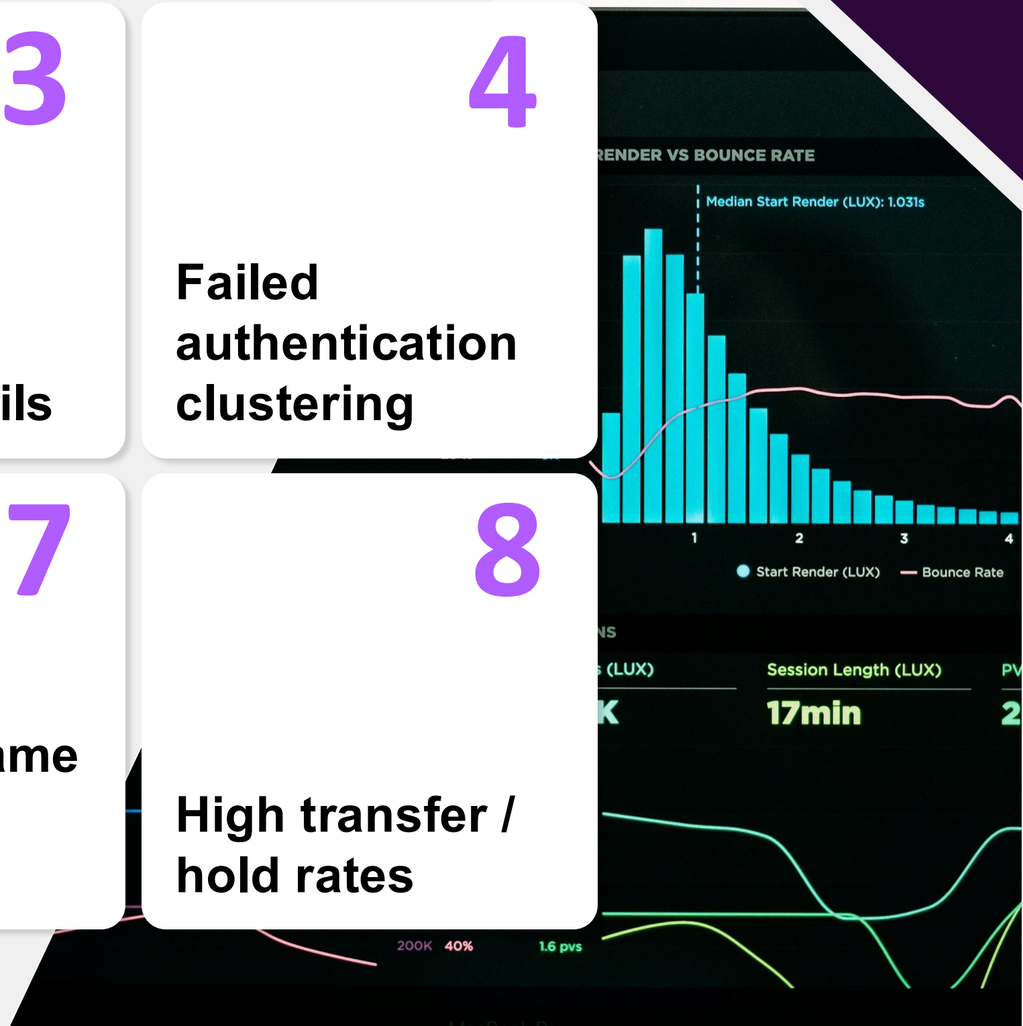
Channel hopping

7

Multiple identities, same device or number

8

High transfer / hold rates



FourNet®

Register interest for Data Queries to Spot Fraud

Survey at the end of the webinar

Effective ID&V in IVR’s

05

1. Automated, Consistent ID&V in the IVR
2. Multi-Factor Authentication Without an Agent
3. Real-Time Risk Detection & Adaptive Routing
4. Continuous Threat Learning
5. Randomisation of Questions

Preventing scammers reaching the call centre

06

1 **Network Level Call Screening**	SmartNumbers Protect inspects every inbound call in the telecoms network before it reaches your IVR, analysing origin, routing patterns, spoofing indicators and number reputation to spot suspicious activity early
2 **Advanced Spoofing Detection**	It identifies when callers are presenting falsified or manipulated numbers by checking signalling data, network metadata and mismatched call paths—instantly flagging or blocking spoofed calls.
3 **Real Time Risk Scoring & Routing**	Each call receives a dynamic risk score, allowing genuine customers through while diverting or step-up-verifying risky calls, ensuring fraudsters never reach frontline teams.
4 **Consortium Level Data**	Cross-checks the calling number against a shared, dynamic database of confirmed fraudsters identified by other major UK organizations (banks, insurers, telcos). 52% of scammers target multiple organisations making consortium data valuable.
5 **Continuous Threat Data**	SmartNumbers Protect constantly updates its detection models using industry-wide fraud intelligence and live attack patterns, adapting automatically to new tactics.

That’s not me!

07

1. Have a Profile / Account ?	60 Second OSINT Profile - Relationships & Tone of Voice
2. Posted about Your Pet?	Pet’s names are often security questions
3. Happy Birthday?	DOB and in particular year is key information, also can identify maiden names.
4. At The Airport?	Highlights off-grid moment for SIM-SWAP fraud.
5. Published a Video?	30 Seconds of audio to create a 95% accurate voice clone
6. Pictures of Yourself?	Creation of Deep Fakes that can trick “Proof of Life”
7. Checked In?	Location can be used to verify transactions. Location services can also reveal in photos.

FourNet®

Register interest for Scamming Risk Assessment

Survey at the end of the webinar

FourNet®

Thank you for attending