Contact Centre Security Report 2023

The hidden fraud lurking in the shadows

smartnumbers

Introduction:

About the research

The Contact Centre Security Report 2023 report is our first annual contact centre fraud review, where we have analysed our extensive primary data on calls made to our customers' contact centres to provide insight into caller patterns and behaviour.

Operating some of the biggest contact centres, our customers receive hundreds of millions of calls every year. Smartnumbers monitors and assesses each call for its relative security risk. As part of the process, our platform flags tens of thousands of suspicious calls each month. Closer inspection of these calls helps us identify ways for contact centres to better recognise fraud and streamline the customer experience in the process.

Our primary aim with this research is to provide year on year insight into changing fraud patterns and actionable advice for contact centre leaders and security teams that can improve contact centre security.

We're delighted to be able to share the results of our 2023 analysis.

Section 1:

Contact centres play a key role in the fight against fraud

Protecting contact centres is essential if we are to combat fraud across the board and risk assessment of incoming calls is the way to do it

It's time to spot fraud before it happens and the contact centre is the place to do it. According to UK Government statistics, fraud accounts for 40% of all crime and costs the UK a staggering £7 billion annually. And according to Datos Insights (previously Aite Group), almost two-thirds (61%) of that fraud touches the contact centre at some stage.

At Smartnumbers, we've long known the contact centre is vulnerable: often neglected by wider anti-fraud measures, it has become the first touchpoint in a much broader fraud lifecycle. For a complete picture of fraud in any organisation, a clear view of fraudulent activity in the contact centre is essential.

Fraud tactics in the contact centre may vary from one individual to the next, but the patterns are unmistakable – and they target both Interactive Voice Response (IVR) and agent calls.

What can be done? The problem for contact centre leaders and fraud prevention teams has always been balancing recognising and dealing with high-risk, suspicious calls with compliance obligations and ensuring a positive customer experience.

The good news is that there are ways to provide you with an early warning system before calls even touch your infrastructure. Read on to find out more about the risks faced by contact centres and what can be done.

Contact centre security report 2023:

Key research findings

Our research draws from the Smartnumbers platform and analysis of the data it collected from the previous 12 months' calls to our customers' contact centres.

Here, we identified a range of different call types and patterns of behaviour, a significant number of which were of concern. This is what we found:

1

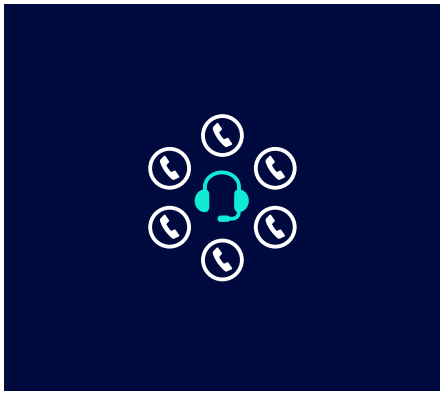
1 in 500 calls to the contact centre were flagged as 'suspicious'

When numbers are withheld or spoofed, or there is a large number of redials in quick succession, we consider these calls to be suspicious. We found as many as 1 in 500 calls to the contact centre like this.

2

58% of calls originating from withheld numbers show signs of fraudulent activity

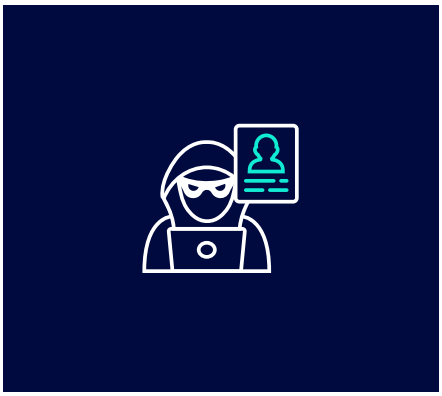
There are many reasons why numbers are withheld and they are not always bad. But since the majority (58%) of the withheld number calls we analysed showed signs of fraud, we consider withheld numbers to be of high risk to the contact centre.



3

80% of inbound calls to the contact centre are from mobile phones

There has been a shift in how customers communicate and mobile phones are now the preferred means. Mobiles are far more likely than a landline to represent a 1-2-1 relationship and those numbers are kept longer too. This creates an opportunity to deliver personalised customer experiences leveraging the mobile phone number as the unique identifier.



4

Just 3 in 10,000 of spoofed number calls are suspicious

While there is growing fear of number spoofing, our research found that the vast majority of spoofed calls - where there is a mismatch between the Presentation Caller Line Identity (CLI) and Network Caller Line Identity - are legitimate. In reality, fraudsters will manipulate both the Network CLI and Presentation CLI, unfortunately making them much more difficult to detect using a mismatch cue.

5

Almost 35% of suspicious calls are flagged due to anomalies in caller behaviour

Caller behaviour – calls from unusual locations or large numbers of repeated redials in quick succession, for example – is the biggest indicator of fraudulent calls and is a factor in almost 35% of those flagged. These kinds of calls cannot be identified without artificial intelligence.

6

52% of identified fraudsters target multiple contact centres across different sectors

In 52% of cases, we discovered the same fraudster details targeting more than one contact centre, often in more than one sector. It goes to show that sharing information helps build a more comprehensive view of fraud and suspicious activity.

Section 2:

Fraudsters are using the phone more than you realise

With all the focus on increasing cybersecurity and educating customers about online scams, you'd be forgiven for thinking contact centre fraud is not a risk. In fact fraudsters are using contact centres more than you realise

It's true, actual telephony fraud is relatively rare. It is not so common for fraudsters to call a contact centre and directly access a customer account by phone and steal their money. It happens and it's an issue, but it's just the tip of the iceberg when it comes to contact centre fraud.

Our data shows that as many as 1 in 500 calls to a contact centre could be from fraudsters and those fraudsters can make on average 26 calls before initiating their attack. And while each of those calls may not always lead directly to a customer being defrauded, they help active fraudsters build a picture of a contact centre's defences and security practices.

10%

increase in calls reaching the contact centre from a mobile device in the past 5 years alone

Fraudsters use the telephony channel for a few critical tasks in the fraud cycle:

Reconnaissance: Collecting and validating stolen customer information to use to commit fraud in other channels, for example. Or monitoring compromised accounts to see when regular large payments are normally received, so that fund transfers can be timed accordingly. Or gathering personal data from a Local Authority record or confirming they are a customer of yours so that they can send a spoofed text message.

Preparation: Carrying out tasks that enable fraud elsewhere, such as adding a name to a utilities bill which can be used for identity theft elsewhere. Or changing an address on a bank account.

Most of this kind of fraudulent activity in the contact centre is hidden or not noticed due to the subtle and apparently low-risk nature of each engagement. It is also often carried out by bots calling over and over to test out which number and data combinations work in the IVR, without making it through to an account or agent. But the signs are there and can be spotted if you know what you are looking for and you have the right technology to do so.

As cybersecurity becomes more robust and public awareness of scams grows, we will see growing exploitation of the telephony channel from fraudsters. Securing this channel therefore provides a huge opportunity to prevent downstream fraud not only in the contact centre, but across all customer channels.

With increased mobile phone usage we're well placed to tackle fraud in contact centres

The key to combatting fraud in the contact centre is to spot suspicious calls before they are answered, and with increased mobile phone usage and technology to flag spoofed or withheld numbers, *this is getting easier.*

Our research found that the majority of today's legitimate callers to a contact centre have a couple of things in common: they rarely call from withheld numbers and the vast majority call in from a mobile. And when it comes to spotting the fraudsters amongst the real customers, this is good news.

Ofcom research[1] shows that by 2021, smartphone take-up was at 88.7% and our own data echoes this with a nearly 10% increase in calls reaching the contact centre from a mobile device in the past 5 years.

The simplicity of mobile number portability and the dwindling use of landlines in the home mean that a mobile number is a much more reliable unique customer identifier as it is tied directly to customer accounts – something that was impossible with shared and frequently changing landline numbers.

This represents a significant opportunity for the contact centre to streamline security processes and customer authentication based on the number being used to make a call.

For example, by making use of mobile phone numbers as a way to help identify legitimate customers, contact centres can eliminate friction in the authentication process.

Collection and maintenance of accurate customer data, including mobile numbers, therefore should be a key priority for improving security and providing better customer experience.

26 calls

made by fraudsters before an attack, on average.

Are spoofed numbers a risk?

Spoofing is not illegal in the UK, but it is an issue. While not a leading indicator of fraud, it does make it difficult to fully trust the number you see. And as more organisations rely on mobile numbers to identify customers, it is inevitable that fraudsters will evolve their tactics to include number spoofing.

And although our data shows that fraudsters don't waste much effort spoofing numbers today, with just 3 in 10,000 spoofed number calls flagged as suspicious, it is important to have the right checks in place.

Detection of spoofed numbers is tricky and requires knowledge of the thousands of legitimate routes calls can take into your organisation and a technology solution with the ability to compare them using machine learning techniques.

The ability to spot and flag callers using spoofed numbers before a call is answered, alerting contact centre agents to handle these calls carefully, is essential to fully mitigate the spoofing risk.

[1] www.ofcom.org.uk/__data/assets/pdf_file/0017/232082/mobile-spectrum-demand-discussion-paper.pdf

Section 3:

Beating the fraudsters: how to secure your contact centre

If an organisation is serious about combatting fraud and building customer trust, then it needs to deploy technology to secure the contact centre

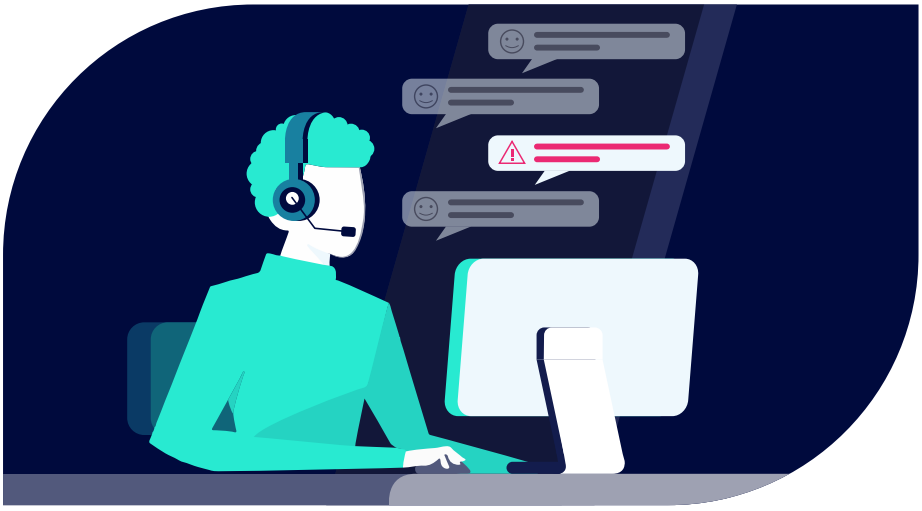
We found that suspicious calls fall into four groups, each of which can be addressed in distinct ways.

01	24%	Known fraudster: presenting number
02	24%	Known fraudster: hiding number
03	17%	Consortium match
04	34%	Suspicious behaviour

01

Known fraudster: presenting number

The fraudsters that keep coming back and do not attempt to hide who they are. Our research and ongoing work with contact centres has highlighted that not all fraudsters are highly sophisticated criminal masterminds. This group equates to 1 in 4 of suspicious calls to the contact centre. They can easily be recognised, making it relatively simple to automatically flag and block the numbers they use.



Known fraudsters equate to *1 in 4* of suspicious calls to the contact centre.

02

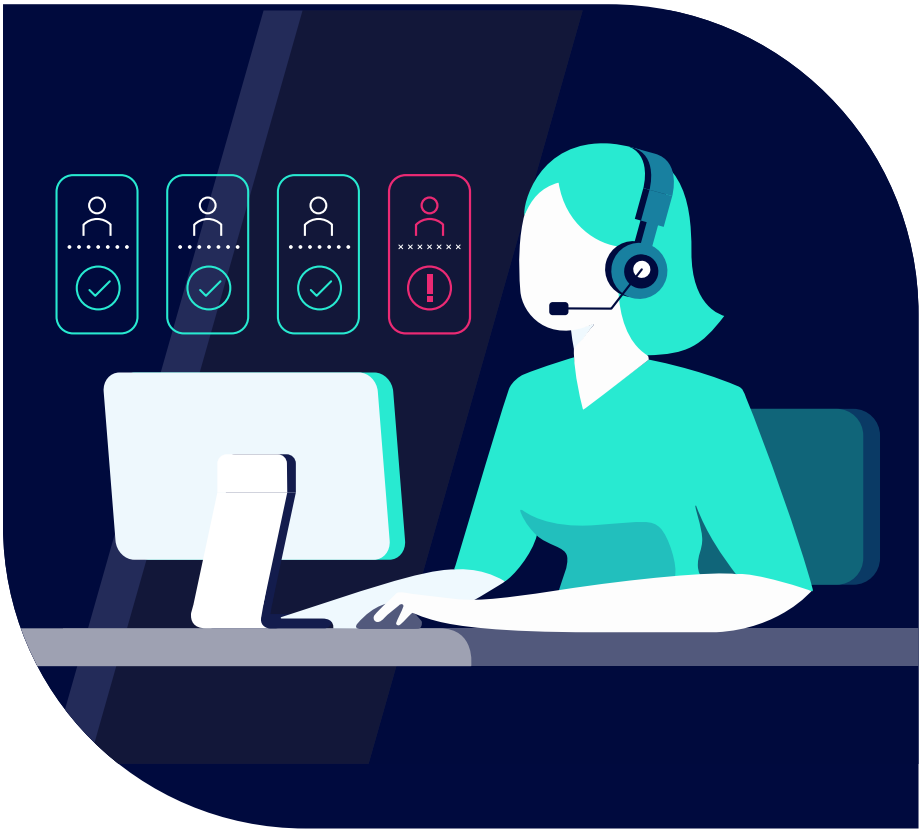
Known fraudster: hiding number

Our research identified that more than 58% of suspicious calls come from withheld numbers and represent a high risk to the organisation.

Unfortunately, the solution is not as simple as denying these calls - plenty of genuine customers also withhold their numbers when calling. But with this knowledge, contact centres must treat withheld number calls with increased scrutiny.

How you can address this risk:

- ☑ The challenge is that the originating number is protected data and, to protect the privacy of genuine customers, telcos can't provide access. But you can work with your telecommunications provider to establish a process to block or alert you to calls originating from withheld numbers you have previously associated with fraud.



Hidden number calls equate to another *1 in 4* of suspicious calls to the contact centre.

03

Consortium match

Consortium match numbers are calls from numbers flagged by other contact centres. Fraudsters will target multiple…. Fraudsters will target multiple organisations simultaneously as they gather information for a fraud attack and maximise their returns. They make multiple calls from multiple phones throughout the day to multiple contact centres and multiple types of company in their quest for a weak link or opportunity.

For example, to tackle a bank's 2FA, a fraudster might convince a mobile operator to fraudulently change a victim's SIM card so they get sent the code by the bank. Or within the same sector, a fraudster might focus effort on one bank until they get caught, regroup and try another bank a few days later.

Of the fraudulent calls we identified, in 52% of cases we discovered the same fraudsters targeting more than one contact centre, often in more than one sector. And nearly 1 in 5 suspicious calls we identified was from a fraudster identified by another contact centre, but which had not been identified by the organisation they were calling.

Contact centres therefore must work together across industries to strengthen the chain and ensure there is no weak link.

How you can address this risk:

- ☑ Collaboration is essential. Work with peers, industry bodies and law enforcement to share phone numbers used by fraudsters and other intelligence about how criminals are operating.

  Smartnumbers' consortium of customers and partners provides the community to do this. Consortium members share data, analysis and insights that can assist all parties in exposing fraud and known fraudsters. By working together and pooling knowledge, everyone can combat fraud.

Leveraging AI/ML to boost security

AI and machine learning tools can be used to spot and flag suspicious behaviour and activity – and this can help you authenticate genuine customers too. Smart tools and technology are turning the tide in the fight against fraud.

04

Suspicious behaviour

Our research highlighted that 1 in 3 of all suspicious calls were identified based on behavioural cues, such as frequency of calling. Learning and adapting to new or unusual caller activity, requires contact centres to monitor caller behaviour patterns as well as the numbers they used. These types of calls are difficult to spot and require the use of machine learning technology to identify and flag unusual caller patterns.

Case study:

Leading retail bank fights fraud with Smartnumbers

Tackling contact centre fraud plays a key role in combatting fraud across ALL customer channels, keeping customers' personal data and accounts safe. And with Consumer Duty regulation requiring banks to deliver good outcomes for their customers – that means customer trust and a slick experience is top of the agenda too.

The challenge

The downside of a successful automated telephone service is that a significant proportion of callers don't speak to an agent, making it difficult to use conventional (human) fraud detection methods to identify suspicious callers.

Top that with an increase in social engineering (the art of manipulating someone into revealing information) when calls do reach time-pressed call agents, and the contact centre is a weak spot in any organisation's fraud defences.

This bank's post-fraud investigation team had identified their automated (IVR) service as a particular weakness that needed to be addressed. But they also saw the IVR as a way maintain and improve customer service, so the bank sought ways to mitigate the risk without limiting access for genuine customers.

The bank also wanted to find ways relieve pressure and improve wellbeing for call agents and find other ways to improve customer experience.

The solution

The bank deployed Smartnumbers Protect to enhance its contact centre security processes and reporting.

Smartnumbers' cloud-based platform uses AI to analyse and assign a risk indicator to incoming calls to the bank's contact centre before they are answered. The platform does this by checking the carrier-level caller details for risk indicators such as numbers already identified as fraudulent by Smartnumbers' customers, withheld numbers or unusual caller behaviour such as a high number of calls in close succession.

Suspicious calls are flagged as high risk can be blocked or managed by specialist teams. And calls from genuine customers are flagged as low risk and can be fast-tracked with minimal authentication steps to the IVR or an agent. Machine learning within the platform keeps track of caller data and fraudster behaviour and adapts its risk indicators as the criminals change their approach.

As a Smartnumbers customer, the bank also becomes a member of the Smartnumbers Consortium – a collaborative community of customers and partners working together to track and share data on active fraudsters.

The fraud and customer service teams at the bank can now:

1. Identify and manage signs of fraud in the contact centre without impacting customer experience
2. Prevent downstream fraud across multiple channels: card, online, APP and telephony
3. Deliver better customer service for genuine customers with seamless authentication and reduced call queuing and handling times
4. Relieve the pressure on call agents to spot fraud, improving productivity and wellbeing
5. Achieve 8x ROI by preventing fraud losses and increasing contact centre efficiency
6. Gather insights and share intelligence on confirmed fraudsters with consortium of other contact centre leaders

"With Smartnumbers, the Bank has reduced friction in the customer journey and delivered *immense ROI* by preventing fraud losses in multiple channels, including card, online, telephony and APP fraud."

Customer, Bank

Conclusion:

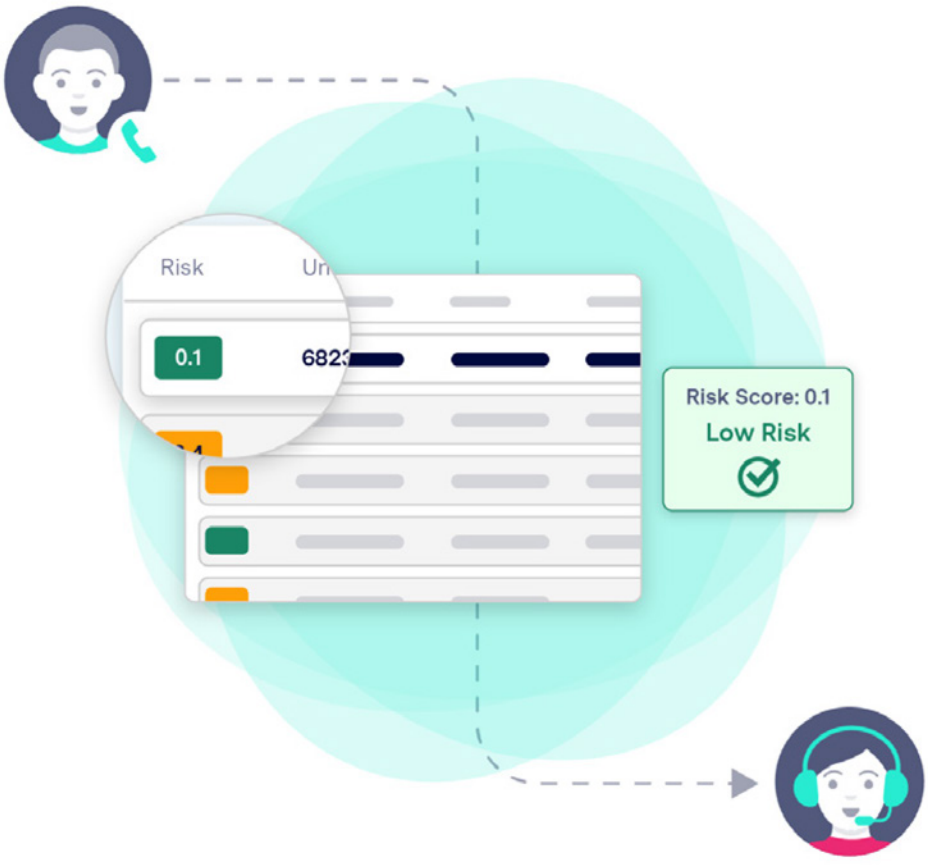
Working together to fight fraud

As cybersecurity becomes more robust and public awareness of scams grows, we will see growing exploitation of the telephony channel from fraudsters.

Our research has made it clear that there is a hidden but easily identifiable world of fraudster activity in the contact centre. With easily deployable practices and immediately actionable insight, much of this activity can be eradicated. But awareness of the problem must be established first.

We hope this research and report inspires you to review your approach to fraud in your organisation. By deploying intelligent tools and technologies in the contact centre, you can make a serious difference to your customers' security.

Tackling fraud together is the only way to *beat it*.



We make voice communications safer. Contact us for more information.

Telephone
+44 20 3379 9000

Email
info@smartnumbers.com

Web
smartnumbers.com