Preventing fraud in the contact centre

A best practice guide

smartnumbers

Contents

Foreword

Fraud continues to account for around 40% of all crime in England and Wales, with UK Finance reporting 2.97 million confirmed cases and £1.17 billion being stolen from consumers in 2023.
The scale of the issue is well known.

Less well known is the role contact centres play in carrying out this crime, even when the actual fraud transaction takes place in another channel.

In this guide we'll take a closer look at the kinds of fraudulent activity we see taking place in contact centres and the relevance of this insight for combating this crime across all channels and in all sectors.

of all crime is fraud

2.97m

confirmed cases

£1.17bn

stolen in the UK

Fraud and the contact centre

Fraudsters exploit the contact centre because it is a weak spot in an organisation's defences.

This vulnerability is partly because it often sits outside the scope of typical online defences, and also because the contact centre is a point of human interaction where humans can be manipulated.

Fraudster activity

Fraudsters carry out a number of different activities in the contact centre depending on the stage of their attack, including:

Reconnaissance

Validating and enriching the stolen information they have gathered by exploiting weaknesses in IVR systems or manipulating contact centre agents to divulge information. This is known as the reconnaissance stage of an attack.

Based on telephony data from Smartnumbers customers, this accounts for 28% of fraudulent behaviour in contact centres.

Set Up

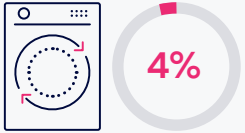
Making amendments to a victim's account, such as changing contact details, by using the data they have acquired to pass security checks with contact centre agents. This is known as the set-up stage and prepares the account for future fraudulent activity.

For our customers, this relates to 59% of fraudulent behaviour discovered in the contact centre.

Cash Out

Creating fraudulent applications in order to gain access to funds.

This is the cash-out stage and accounts for 9% of the fraudulent behaviour seen in the contact centre.



Laundering

Checking when stolen funds have cleared before transferring them elsewhere. For this money laundering stage, fraudsters exploit both automated and non-automated mechanisms, using security vulnerabilities in call centres to manipulate accounts and carry out financial fraud.

This accounts for 4% of fraudulent behaviour in the contact centre.

These activities are not isolated incidents - carrying out these attacks is a often a full time job for fraudsters.

They continuously target multiple accounts, across multiple organisations, over and again.

Fraud networks

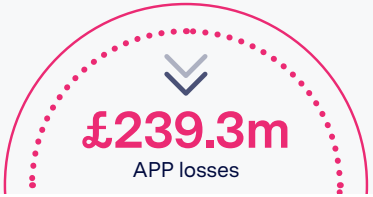
It is also important to remember that the information fraudsters gather, and the actions they carry out in the contact centre, may not always lead to a financial loss within the contact centre itself.

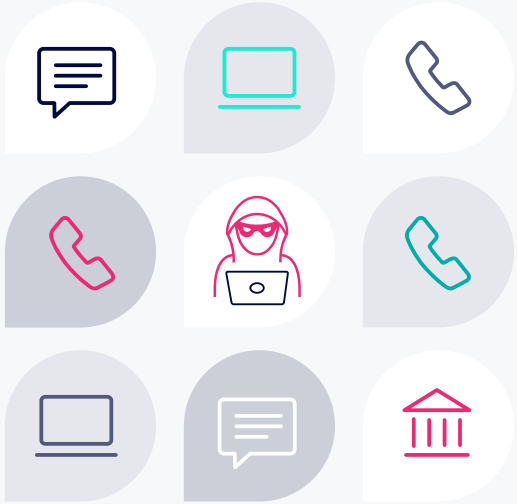
These activities may be part of a wider fraud operation that is completed in another customer channel, or within another organisation.

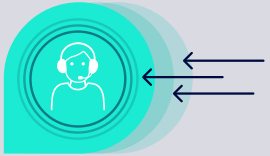
For example, additional data gathered during reconnaissance activity targeting one retail bank contact centre, may be used to open a new digital account with a different bank, or apply for an insurance product at a different organisation using a stolen identity. And sometimes the goal is simply to sell the data on again.

Stolen data may also be used as part of complex scams that convince the account holders themselves to divulge further personal information and/or voluntarily transfer money to the fraudster. In banking terms, this is known as Authorised Push Payment (APP) fraud and amounted to £239.3 million in APP losses in England and Wales in 2023 according to UK Finance.

In the case of APP fraud in the contact centre, it is therefore important to be on the alert not only for fraudster activity, but also the account holder operating under the fraudster's spell.







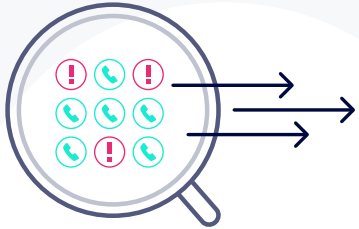
The purpose of this guide is to help those seeking to protect their organisations from fraudsters by securing contact centres.

We outline the vulnerabilities, describe various techniques that can be used to prevent them and recommend best practice guidelines for effective treatment.

Three essential considerations

Ahead of putting in place any treatment strategies, there are three key points that organisations should consider up front to ensure they put themselves in the best position to detect fraudsters.

01

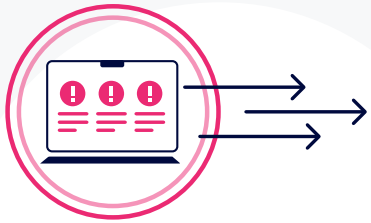


Identify withheld numbers

Fraudsters often use withheld numbers to avoid detection (based on our data, this amounts to 43% of fraudulent calls).

The ability to link withheld calls from the same individual is key to tracking the impact of repeat fraudsters.

02

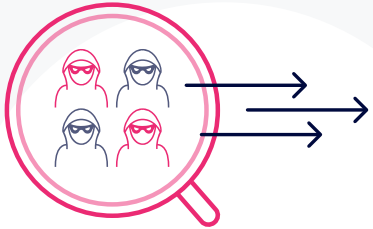


Harness denylist intelligence

Fraudsters reuse the same phone number for multiple attacks across multiple accounts or organisations.

So maintaining a denylist of phone numbers associated with fraudsters can help to identify repeat offenders.

03



Track behavioural patterns

Fraudsters have behavioural patterns that can give away their intent, such as lots of short calls into an IVR.

Access to data from systems such as IVRs to assess caller intent is a key starting point when investigating fraud.

Data prerequisites

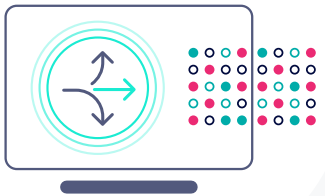
To effectively detect and treat fraud at the reconnaissance stage, fraud professionals need access to four key data points:

01

Call metadata

Core metadata about the call such as the start/end time, phone number and dialled number.

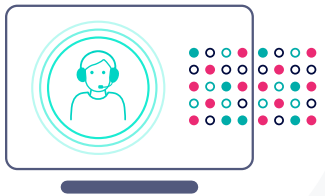
02



IVR data

Data about the route that a caller attempted to take through an IVR, which account holder they targeted and what they ended up doing.

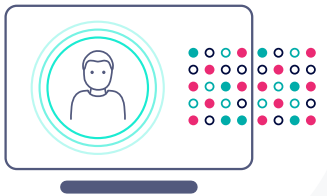
03



Agent call data

Data about what happened on the agent answered call such as call recordings and agent notes.

04



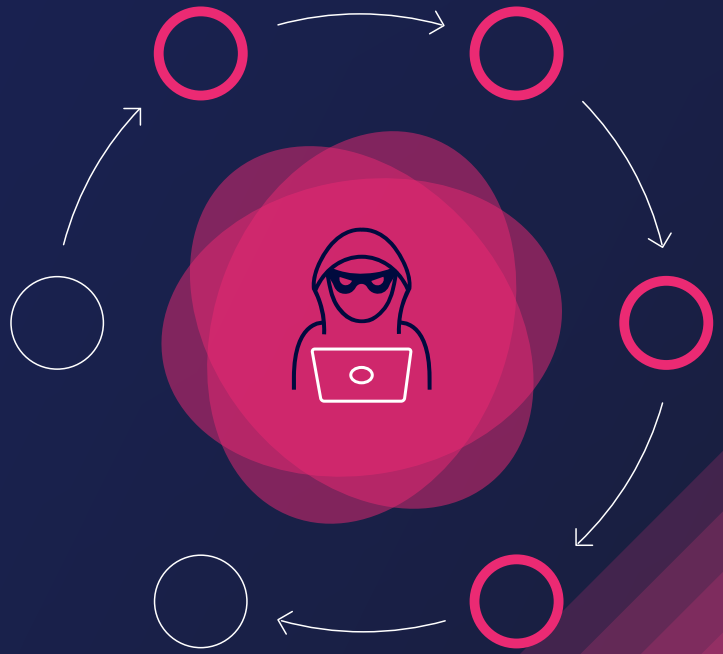
CRM data

Data about the customer and their account(s) including recent transactions.

Introducing the Fraud Lifecyle

Together, the different stages of a fraud attack, from data gathering to accessing clean funds, are known as the Fraud Lifecycle.

In our experience, a typical timescale from call to cashout could be up to 9 months, which indicates the opportunity to stop fraud in the early stages.



Lifecyle walkthrough

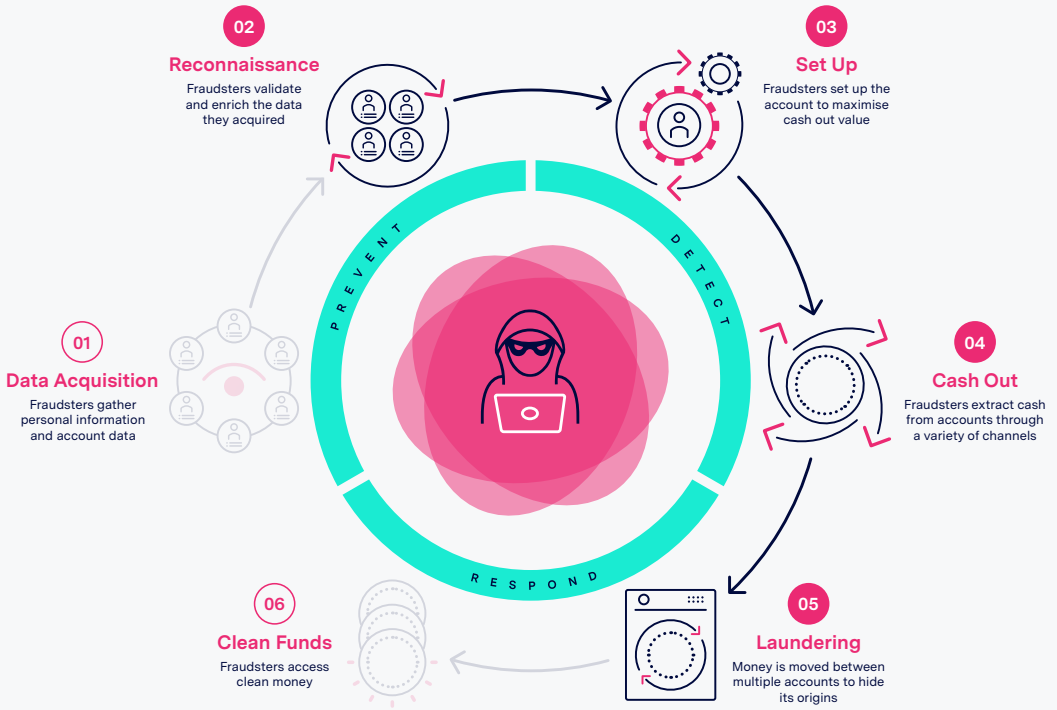
This section of the guide outlines each stage of the lifecycle where fraudsters are known to exploit the contact centre.

Each stage defines the fraudster's intent, the contact centre mechanisms they typically exploit to achieve their goals, potential treatment strategies that can be applied, key defence implementation details and best practice guidelines for preventing fraud at this stage.

Every organisation is different and will investigate fraud in different ways. The key is to gather as much intelligence as possible in order to better understand fraud tactics and to drive fraud strategy across the organisation.

In this guide we focus on the stages of the lifecycle which commonly touch the contact centre:

- 02 Reconnaissance
- 03 Set Up
- 04 Cash Out
- 05 Laundering



Reconnaissance

02

Fraudster intent

At this stage, the fraudster seeks to validate and enrich information about the victim that they have previously stolen or acquired. For example, if they have access to stolen card data on the darknet, the fraudster could use the IVR of a retail bank to validate that the card is active and that any credentials that they have already are valid. Then, they could attempt to gain access to the balance on the account to use later in their attack.

The final stage of the fraud transaction may be initiated in the contact centre, or it could take place elsewhere. The data may also be used to create a convincing scam that targets the account holder directly.

Mechanism

Fraudsters exploit both IVRs and contact centre agents at this stage:

IVRs:
Leveraging self-serve capabilities on the IVR to validate data they have and trying out different combinations in order to enrich their data. This is sometimes done manually, or at scale using a bot to automate.

Agents:
Using social engineering techniques to trick agents into validating information and divulging more details that they can use later in their attack.

Best practice recommendations

Treatment

There are three potential treatment strategies that can be applied at this stage:

Respond:
Safeguard the account & monitor

- Put a marker on the account to ensure that future high risk activity is prevented and any suspicious behaviour on the account is flagged

RECOMMENDED

Route:
Transfer to specialist ops team

- Re-route the call to an operational fraud team that is equipped to navigate the risk without tipping off the fraudster

Prevent:
Prevent the call from taking place

- Actively cut off the call so that the transaction cannot take place

Process

There are automated and manual processes that can be implemented at this stage:

Automated steps:

- Automatically safeguard & monitor the customer account

Manual steps:

- Specialist ops team investigates & safeguards account
- Review IVR intent (assess behaviour, route and velocity of the caller)
- Listen to the call
- Review account activity (recent changes or transactions)
- Provide feedback data for machine learning and consortium (decision, type, methods, denylist)

03

Set Up

Fraudster intent

At this stage, the fraudster passes through security and attempts to amend the victim's account to prepare it for their attack. By suppressing notifications, for example.

Mechanism

Fraudsters only exploit contact centre agents at this stage:

Agents:

Using social engineering techniques to encourage and pressurise agents into making unauthorised account changes such as new addresses or payees, even if it means bypassing standard procedure.

Best practice recommendations

Treatment

There are three potential treatment strategies that can be applied at this stage:

Respond:
Safeguard the account & monitor

- Put a marker on the account to ensure that future high risk activity is prevented and any suspicious behaviour on the account is flagged

RECOMMENDED

Route:
Transfer to specialist ops team

- Re-route the call to an operational fraud team that is equipped to navigate the risk without tipping off the fraudster

Prevent:
Prevent the call from taking place

- Actively cut off the call so that the transaction cannot take place

Process

There are automated and manual processes that can be implemented at this stage:

Automated steps:

- N/A

Manual steps:

- Specialist ops team investigates & safeguards account
- Listen to the call
- Review account activity (recent changes or transactions)
- Provide feedback data for ML and consortium (decision, type, methods, denylist)
- If it is an account takeover, undo any recent changes that have been made on the account
- If it is an application fraud, close the account

Cash Out

04

Fraudster intent

Fraudster carries out a financial event via the contact centre. (This scenario is normally associated with retail bank contact centres).

Mechanism

Fraudsters may exploit both IVRs and contact centre agents at this stage, transferring money between accounts or to a new payee.

Note: It is at the Cash Out stage where contact centres also need to be on the alert for genuine account holders acting under the spell of the fraudster, by checking for out-of-character behaviour and any flags on their account..

Best practice recommendations

Key data points:

To effectively detect and treat fraud at the Cash Out stage, fraud professionals needs access to four key data points:

Call metadata

Core metadata about the call such as the start/end time, phone number and dialled number.

IVR data

Data about the route that a caller attempted to take through an IVR, which account holder they targeted and what they ended up doing.

Agent call data

Data about what happened on the agent answered call such as call recording and agent notes.

CRM data

Data about the customer, their account including recent transactions.

Treatment

There are two potential treatment strategies that can be applied at this stage:

Route:
Transfer to specialist ops team

- Re-route the call to an operational fraud team that is equipped to navigate the risk without tipping off the fraudster

Prevent:
Prevent the call from taking place

- Actively cut off the call so that the transaction cannot take place

Process

There are automated and manual processes that can be implemented at this stage:

Automated steps:

- Feedback data

Manual steps:

- Specialist ops team investigates & safeguards account
- Review IVR intent (behaviour, route and velocity)
- Listen to call
- Review account activity (recent changes or transactions)
- Provide feedback data for ML and consortium (decision, type, methods, denylist)
- If it is an account takeover, undo any recent changes that have been made on the account
- If it is an application fraud, close the account

05

Laundering

Fraudster intent

Fraudster waits for stolen funds to be cleared before transferring onwards in order to clean the money.

Note: in the case of 'money mules' this could be the account holder themselves calling in. The key is to spot unusual activity, such as large sums of money or irregular deposits and withdrawals.

Mechanism

Fraudsters exploit both IVRs and contact centre agents at this stage:

IVRs:

Checks on the account balance to see if incoming funds have been cleared before sending them onwards.

Agents:

Checks on the account balance to see if incoming funds have been cleared before sending them onwards.

Best practice recommendations

Treatment

There are two potential treatment strategies that can be applied at this stage:

Respond:
Safeguard the account & monitor

- Put a marker on the account to ensure that future high risk activity is prevented and any behaviour on the account is flagged.
- Raise a suspicious activity request (SAR)

RECOMMENDED

Process

There are manual processes that can be implemented at this stage:

Manual steps:

Organisations are not allowed to tip off its criminal offence, however banks do freeze account/funds

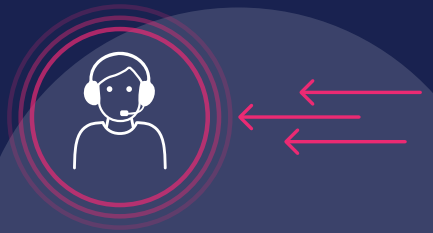
- Raise Suspicious Activity Request (SAR) – information: who/value
- SAR is raised to Financial Crime Teams
- Financial Crime Team will ensure regulation is followed
- If meets criteria, SAR will be raised to Nation Crime Agency
- When its decided to close the account and more £1000 in account a DAML (defence against money laundering) is needed. DAML requests consent from National Crime Agency (NCA) to pay customer the money back

Source: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/462-sars-faq-july-2020/file

Your three takeaways

Securing the contact centre is an essential part of protecting the entire organisation from fraud.

01

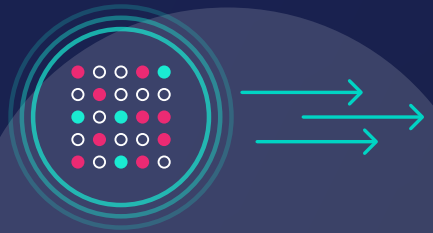


Spot early signs of fraud

With the right measures in place, organisations have the opportunity to spot signs of fraud in its early stages.

Counter fraud teams gain access to valuable information about fraudster tactics, which help inform fraud prevention approaches.

02



Share your data

As with any solution, the key to success is access to and visibility of data.

In the fight against fraud, telephony data (including call metadata, IVR activity and agent call data) is a powerful source of intelligence that can be used across an organisation. Without this, success will be limited.

03

Put processes in place

Armed with this data, and the ability to link it to customer accounts, organisations across sectors are able to put in place contact centre processes.

They can also develop a wider fraud prevention strategy that will enable them to combat fraud more effectively.

Fight fraud. Protect the contact centre.
Contact us for more information.

Telephone: +44 20 3379 9000

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers