Survey Report · December 2024

Contact Centres: The new frontier in fraud prevention

Contents

1

About the survey

Foreword

Fraud costs the UK economy billions. A focus on early signs of fraud in contact centres could help curb this growing threat.

For individual victims, fraud is felt when money is taken from their account, a charge is made to their card, or someone else uses their details to obtain a loan. Businesses also focus on financial loss – the 'cash-out' stage of the fraud life cycle. But, in fact, fraud begins much earlier, often with a call to a contact centre. Smartnumbers' in-house data shows that 28% of activity flagged by our systems is due to 'reconnaissance' attempts, while 59% is 'set-up' related.

These are vital parts of the process, when fraudsters validate stolen data or steal more information to prepare their attacks.

According to UKFinance, a trade association for the banking and financial services sector, the amount stolen through fraud in the UK in 2023 was £1.17 billion. Reducing that figure means we have to take seriously the wider role of contact centres in the fraud life cycle.

If businesses continue to measure and report fraud levels by financial transactions, rather than preventing customer data loss, they won't have a thorough understanding of what's going on and will miss critical insight for preventing fraud altogether.

To gain a clear picture of the scale of fraud that organisations are currently aware of in the contact centre, we partnered with Opinion Matters to conduct an independent survey.

We're delighted to share the findings with you.

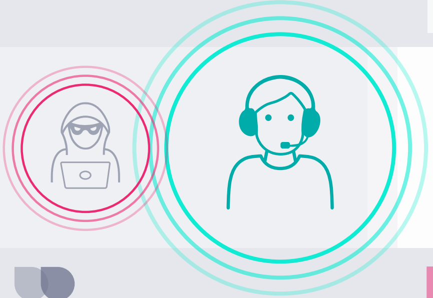
Jamie Melling
Smartnumbers
Chief Executive Officer

The amount stolen through fraud in the UK in 2023 was £1.17 billion.

Reducing that figure means we have to take seriously the wider role of contact centres in the fraud life cycle.

Survey quick guide

Contact centres: The new frontier in fraud prevention



Organisations need to stop focusing solely on the financial loss and start addressing data loss through reconnaissance, which are precursors to bigger fraud incidents.

Matthew Addison
Smartnumbers
Chief Revenue Officer

01 Early signs of fraud

Fraud is typically recognised at the point of financial loss. But fraud begins much earlier, often with a call to a contact centre. Activity flagged by Smartnumbers tells us:

28% Due to Reconnaissance attempts

59% Related to fraud Set Up

02 Missed fraud insight

When businesses measure and report fraud levels by financial transactions, rather than preventing customer data loss, they miss critical insight for preventing fraud altogether.

03 Fraud is widespread

More than **85%** of survey respondents report high fraud-related activity across all business sectors, with telephony channels being just as vulnerable as online or mobile channels.

+85%

04 Easy fraud targets

Travel sector respondents report particularly high fraud activity in both IVR (**66%**) and with contact centre agents (**55%**), suggesting fraudsters are constantly looking for softer targets.

66%

55%

05 Exploiting humans

The most common fraudster tactics are tricking agents (social engineering), reported by **40%** of respondents; and using devices to change the caller's voice, reported by **32%**.

40%

32%

06 Beware the bots

When businesses measure and report fraud levels by financial transactions, rather than preventing customer data loss, they miss critical insight for preventing fraud altogether.

07 Reactive fraud prevention

Fewer than half have automated fraud-detection methods in the contact centre, such as flagging incoming calls from blacklisted numbers (**44%**) or flagging incoming calls because of unusual behaviour (**39%**).

44%

39%

08 Data sharing is key

There is a hesitancy to share fraud intelligence – because of fears about data quality, giving away a competitive advantage or concerns about perception. But fraud threatens entire sectors, not just a few companies.

09 Moving beyond financial loss

A focus on preventing data leakage is key to avoiding larger financial losses overall. Counter-fraud teams, across all sectors, must prioritise the protection of customer data to make it harder for criminals to exploit such a vital resource.

Our methodology

What we wanted to discover

- Assess levels of fraudulent activity seen in contact centres vs other customer channels
- Understand most common types of fraudulent activity reported in contact centres
- Understand adoption levels of various counter-fraud tools and treatments
- Assess willingness to share intel within and across sectors
- Gain further understanding of reasons for not sharing data, when this is the case

Who we surveyed

Participants x250

Senior fraud professionals with decision-making responsibilities.

Sectors x4

Sector split:
Financial services; IT and Telecoms; Travel and Transport; and Retail.

Organisations 250+ people

Large organisations with with 250+ employees and contact centres that receive 30,000+ calls a month.

2

Survey findings

Fraud seen in all sectors

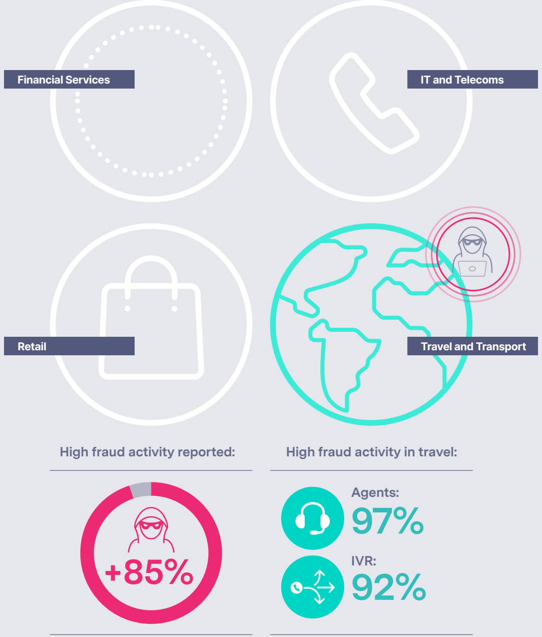
There's no doubt that fraudulent activity is widespread. The survey covered 250 UK-based senior decision-makers dealing with fraud in organisations with large contact centres in the financial services, retail, travel and telecoms sectors. More than 85% of respondents report high fraud-related activity across all business sectors, with telephony channels being just as vulnerable as online or mobile channels.

The research suggests that organisations do understand that contact centres are a target. "The awareness of vulnerabilities within contact centres across multiple sectors is a particularly interesting part of the survey results," says Matthew Addison, Chief Revenue Office at Sumartnumbers.

Certain industries, such as travel, report particularly high fraud activity in both interactive voice response (IVR) at nearly 97% and with contact centre agents (92%).

"Fraudsters are constantly looking for softer targets in sectors like retail or airlines, where they can conduct last-minute attacks such as fraudulent ticket purchases," says Tim Burton, chief product and success officer at Smartnumbers

He explains that, for example, cardholder validation by card issuers and passenger validation by airlines are not as joined up as they should be. Fraudsters exploit this by purchasing a last-minute flight using stolen financial details, or by modifying passenger information shortly before a flight takes off, leaving a narrow window for collaboration to spot the fraud.

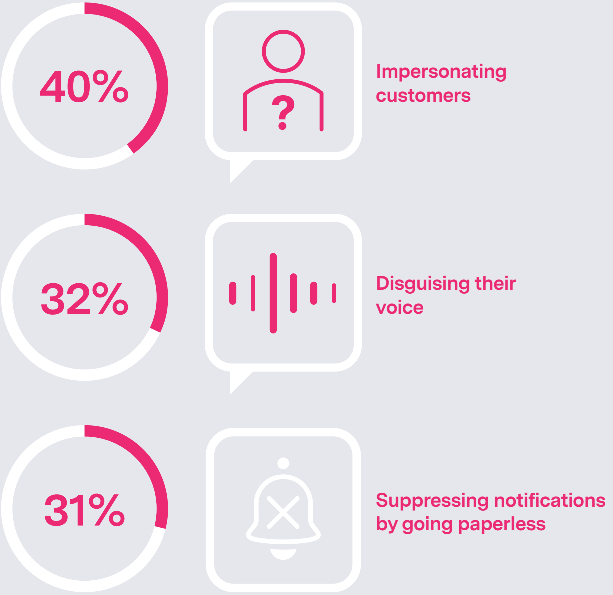


> **Fraudsters are constantly looking for softer targets in sectors like retail or airlines, where they can conduct last-minute attacks such as fraudulent ticket purchases**
>
> **Tim Burton**
> Smartnumbers
> Chief Product and
> Success Officer

Humans are an easy target

Fraudsters are becoming more skilled at manipulating agents into giving away information or carrying out small account changes. These are early signs of fraud that often happen long before the cash-out stage.

Tim Burton
Smartnumbers
Chief Product and
Success Officer



Human vulnerabilities are easy to exploit, and this was clear in the survey results. Among the most common fraudster tactics are tricking agents (social engineering), which was reported by 40% of respondents, and using devices to change the caller's voice, reported by 32%. Agents are trained to be helpful and they're under time pressure, which means they might unwittingly overlook security rules for a fraudster who they think is a genuine customer with a difficult problem.

Suppressing notifications, for example, by switching to paperless statement,s was a tactic reported by 31% of respondents.

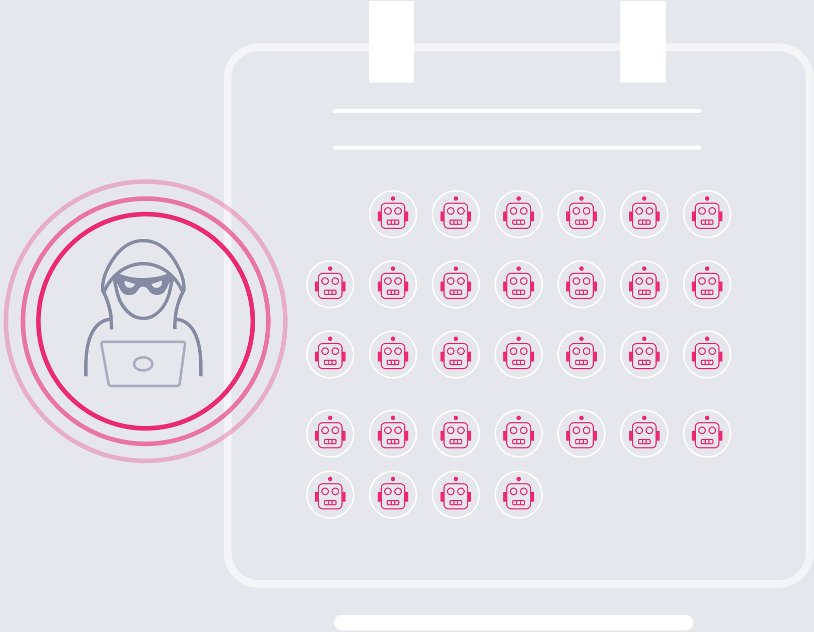
"Fraudsters are becoming more skilled at manipulating agents into giving away information or carrying out small account changes. These are early signs of fraud that often happen long before the cash-out stage," Burton explains.

Yet human-to-human fraud is the tip of the iceberg and – with call recording relatively easy to track and understand – it's not scalable. It's the bots we should be scared of. As with many legitimate organisations, fraudsters are turning to automation technology to increase the speed and volume of their activity.

Beware the bots

Mass attacks on multiple companies in multiple sectors use bots to target IVRs and identify high-value accounts to ensure maximum return on fraud. For example, if a fraudster knows the target's birth year and birth month, they can use a bot to call up to 31 times. This gives them the chance to also uncover the correct day of birth, which can be used in the next stage of the process.

"Fraudsters exploit the IVR by making numerous attempts to extract or validate information, a process that can take multiple calls before they get what they need," says Addison. "This activity is often invisible to businesses".

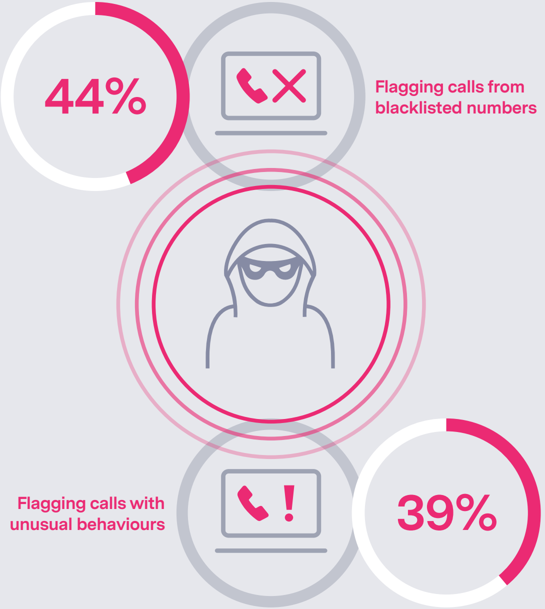


> **Fraudsters exploit the IVR by making numerous attempts to extract or validate information, a process that can take multiple calls before they get what they need. This activity is often invisible to businesses.**
>
> **Matthew Addison**
> Smartnumbers
> Chief Revenue Officer

Current fraud-prevention gaps

The lack of integration between fraud and contact-centre teams means they're not working towards the same goal.

Tim Burton
Smartnumbers
Chief Product and Success Officer



Yet many companies still take a reactive approach to fraud. Fewer than half of those surveyed have automated fraud-detection methods in the contact centre, such as flagging incoming calls from blacklisted numbers (44%) or flagging incoming calls because of unusual behaviour, such as making multiple calls in quick succession (39%).

Many are relying instead on outdated or manual processes. Even processes that can be automated easily today are sometimes still done manually. For example, some large organisations continue to use sticky notes on agents' desktops to flag blacklisted numbers.

Organisations are not always linking the vital data they do have or ensuring it's distributed to those who need it. Fraud signals – such as multiple calls within a short time or calls from withheld or blacklisted numbers – should be fed into overall fraud-prevention strategies because they're signs of reconnaissance or data acquisition.

But this data is not always linked to the downstream fraud that occurs later in other channels. "The lack of integration between fraud and contact-centre teams means they're not working towards the same goal," Burton says.

Missed opportunities for data sharing

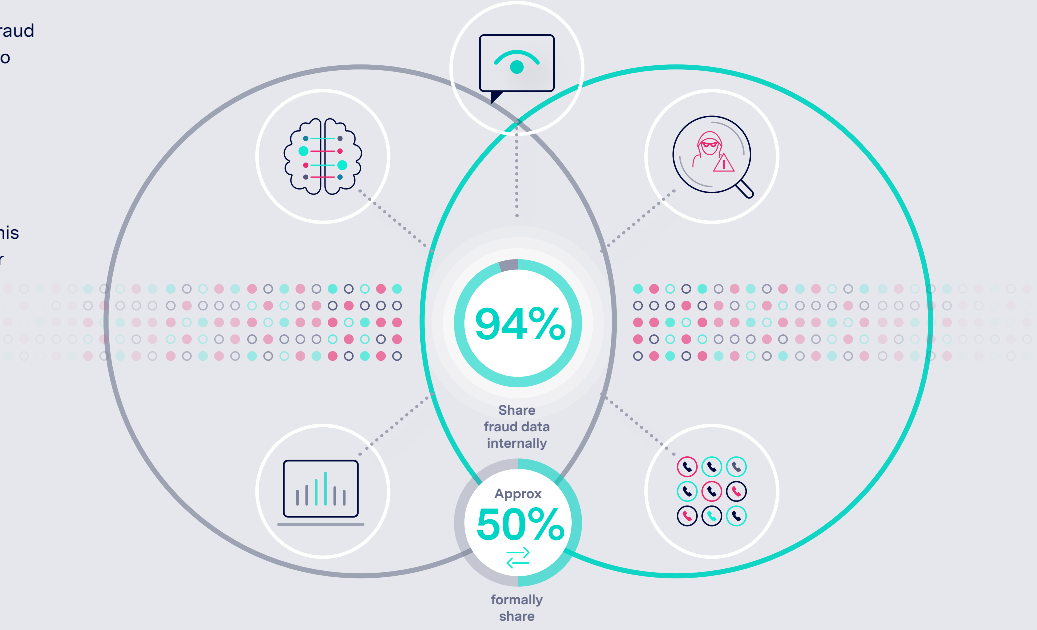
Data sharing is key because fraudsters commonly exploit weaknesses in one organisation or channel to gather the data needed to attack another target. While 95% of businesses share some form of contact centre fraud data internally and externally, approximately half have formal processes for this.

Externally, there is also a hesitancy to share fraud intelligence – because of fears about data quality, giving away a competitive advantage or concerns about perception. But fraud threatens entire sectors, not just a few companies.

Sharing should be easy and standard practice, because insights about fraudsters' activities and behaviour patterns could make everyone safer.

For example, if company A shares fraud intelligence that helps company B to strengthen its defences, then both companies might be more secure.

Ironically, fraudsters are proactive in sharing information. Some gangs will specialise in verifying account details, for example, and then sell this – now more valuable – data to other fraudsters with a greater capability to exploit it.



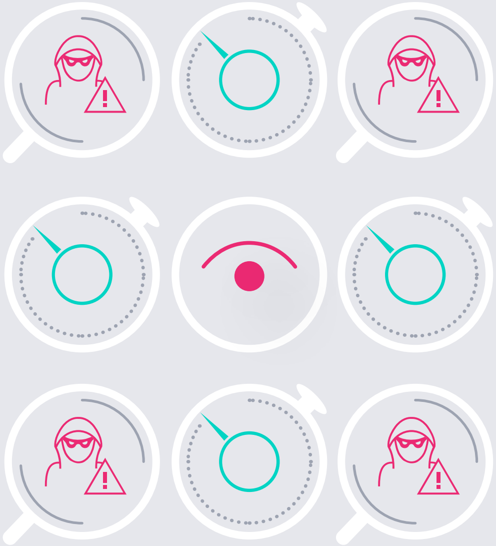
Moving beyond financial loss

When organisations prioritise and measure fraud prevention at the financial transaction stage, they overlook the critical role that protecting customer data plays in preventing fraud. But a focus on preventing data leakage is key to avoiding larger financial losses overall.

In fact, better awareness at this stage can make it easier to catch fraudsters. An organisation that has the tools to identify suspicious data-gathering activity can flag the accounts being targeted so its fraud-prevention team can watch those accounts. The fraudsters can then be caught in the act when they try to complete the transaction.

Allowing the cycle to safely play out like this means organisations learn more. It also makes it easier to attach a fiscal value to the fraud that's been prevented. Some top retail banks we work with are already doing this. "By using early-warning systems and sharing fraud intelligence, companies can spot suspicious activity sooner," Burton says. "This means less damage and fewer opportunities for fraudsters to exploit data across multiple channels."

Without proactive prevention measures, including solutions to automate detection and prevent reconnaissance activity, fraud will continue to cost the economy billions in stolen revenue. But focusing on the financial loss alone can only take us so far. Counter-fraud teams, across all sectors, must prioritise the protection of customer data to make it harder for criminals to exploit such a vital resource.



> **By using early-warning systems and sharing fraud intelligence, companies can spot suspicious activity sooner. This means less damage and fewer opportunities for fraudsters to exploit data across multiple channels.**
>
> **Tim Burton**
> Smartnumbers
> Chief Product and Success Officer

3

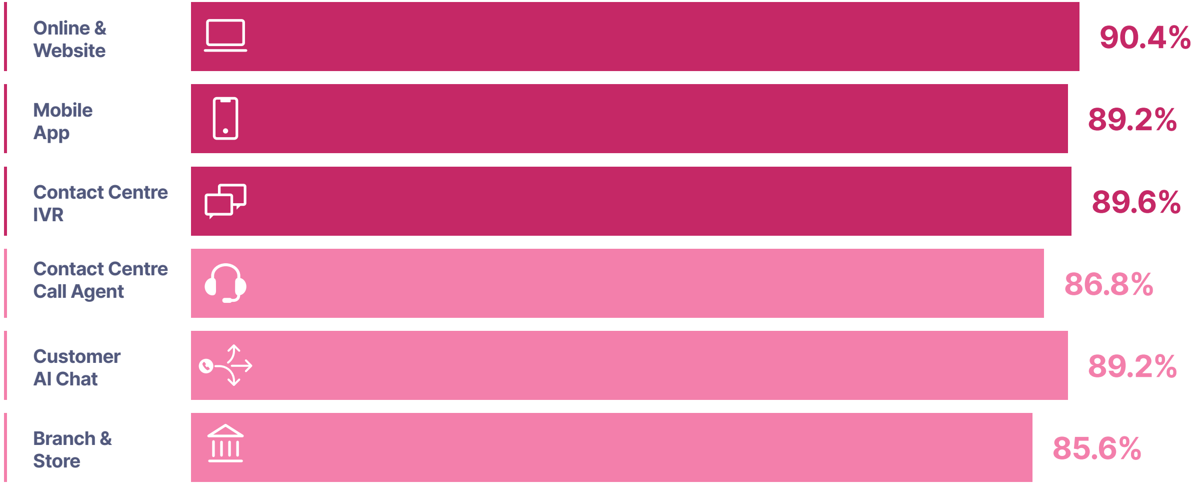
Survey in detail

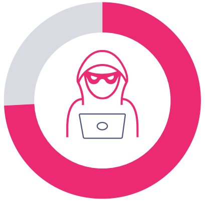
Q1: Channels

Thinking about the different ways fraudsters attempt to target/access customer accounts in your organisation, what levels of activity, if any, do you see in the following customer channel(s)?

- More than 85% of respondents report high fraud-related activity across all business sectors, with telephony channels being just as vulnerable as online or mobile channels.
- Clearly organisations understand that fraudsters exploit the contact centre but may lack the visibility provided by technology to detect the scale of fraud (based on later responses).

All responses:





High-level activity reported in contact centres

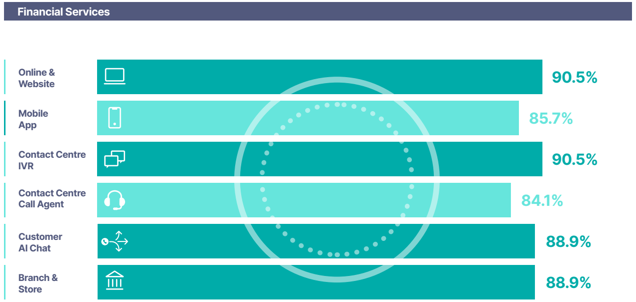
88%

By industry sector:

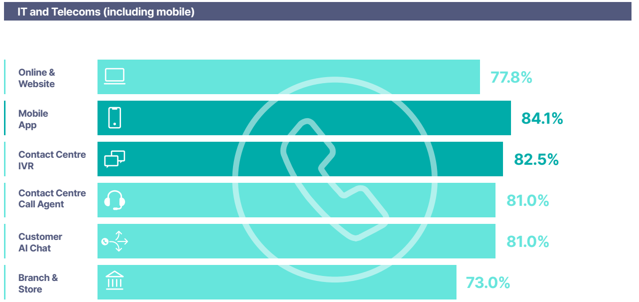
Q1: Channels

Thinking about the different ways fraudsters attempt to target/access customer accounts in your organisation, what levels of activity, if any, do you see in the following customer channel(s)?

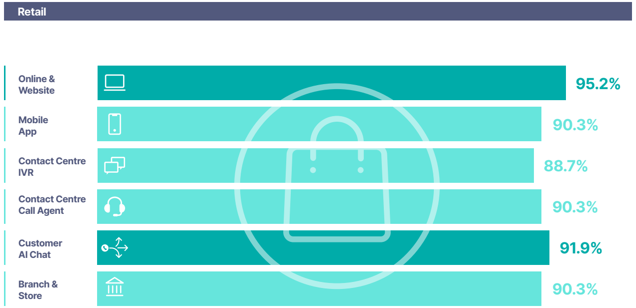
- In Financial Services, the majority of respondants reported equally high actiity in online and IVR channels.
- Travel and transport sector had the highest number respondents reporting high levels of fraud across all channels. Almost 97% of respondents reported high activity in the IVR.



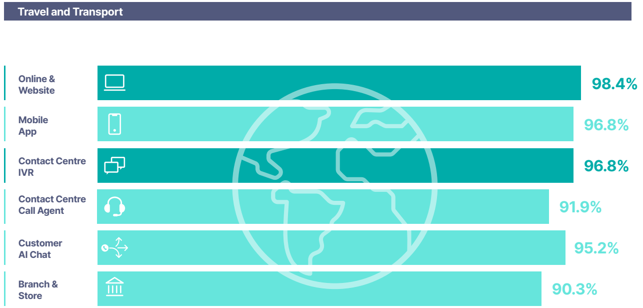
Financial Services



IT and Telecoms (including mobile)



Retail

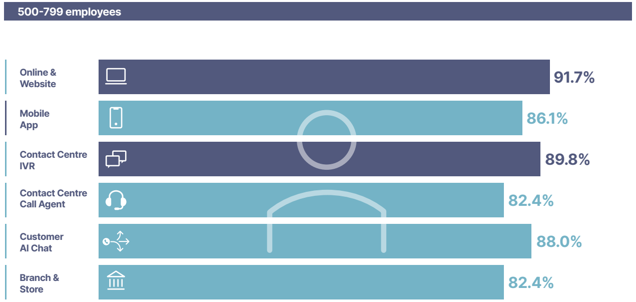


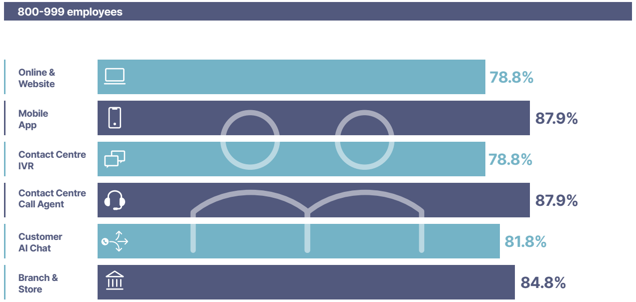
Travel and Transport

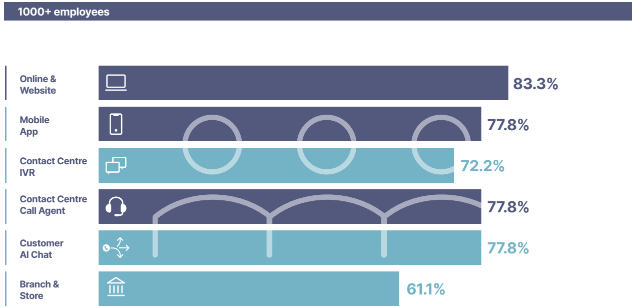
Q1: Channels

Thinking about the different ways fraudsters attempt to target/access customer accounts in your organisation, what levels of activity, if any, do you see in the following customer channel(s)?

By company size:





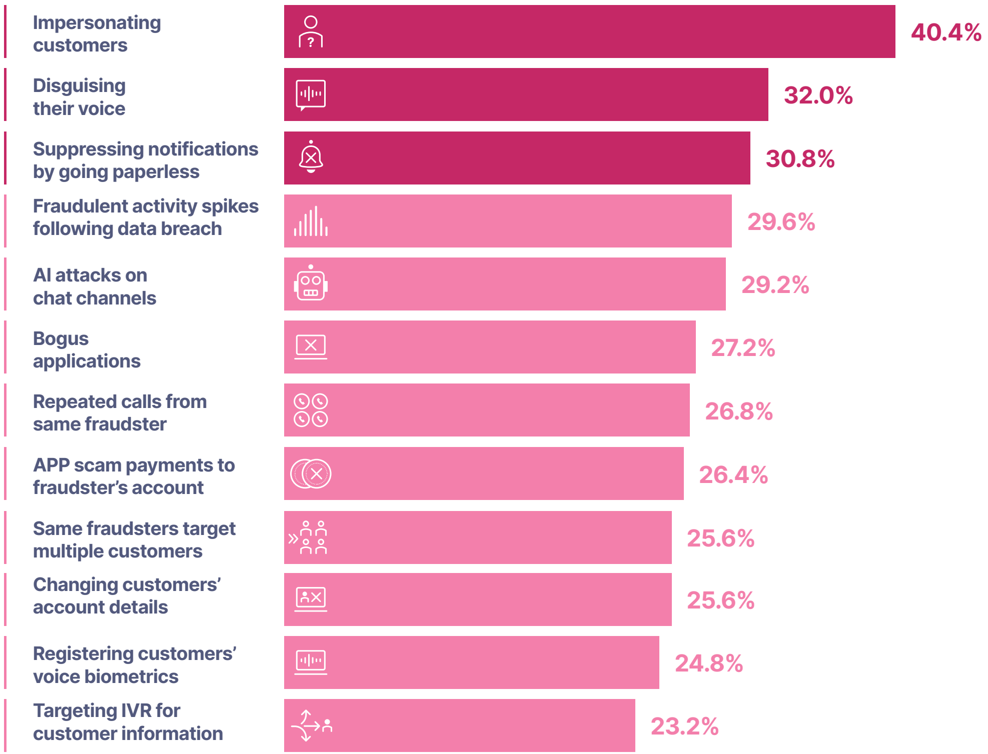


Q2: Fraudster tactics

Thinking about fraudulent activity in your organisation's contact centres in the last 12 months, which fraudster tactics, if any, are the most common?

- Social engineering of agents, the use of voice changers and the suppression of customer notifications, are the top three most commonly reported tactics used by fraudsters to target contact centre.
- These tactics are also the most easy to detect, which (in our experience) suggests contact centre fraud is being under-reported.

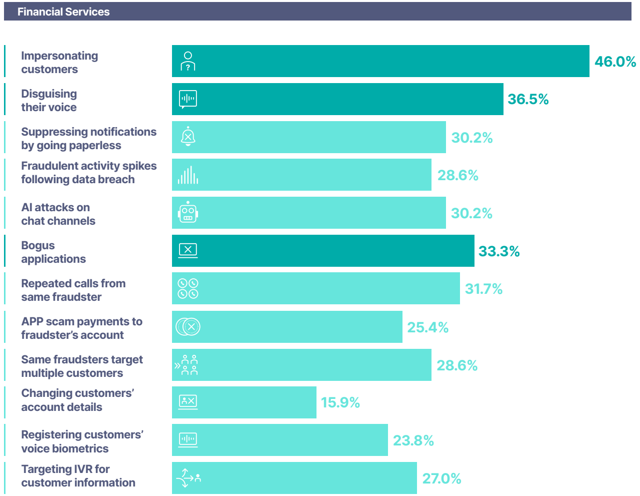
All responses:

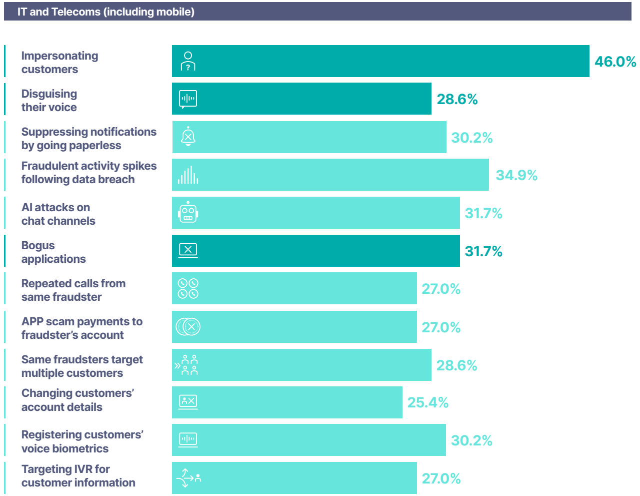


By industry sector:

Q2: Fraudster tactics

Thinking about fraudulent activity in your organisation’s contact centres in the last 12 months, which fraudster tactics, if any, are the most common?

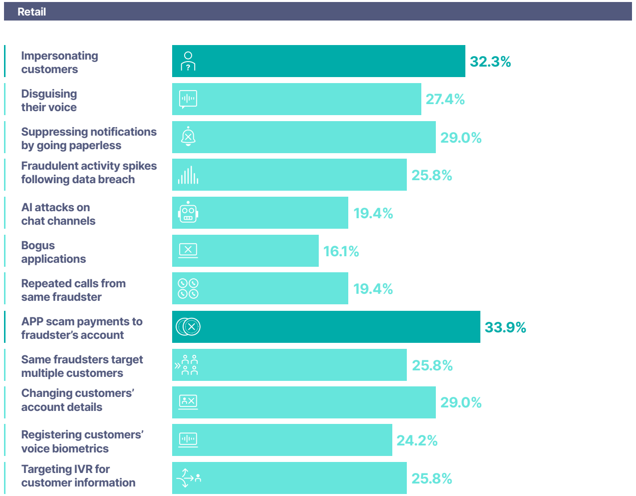


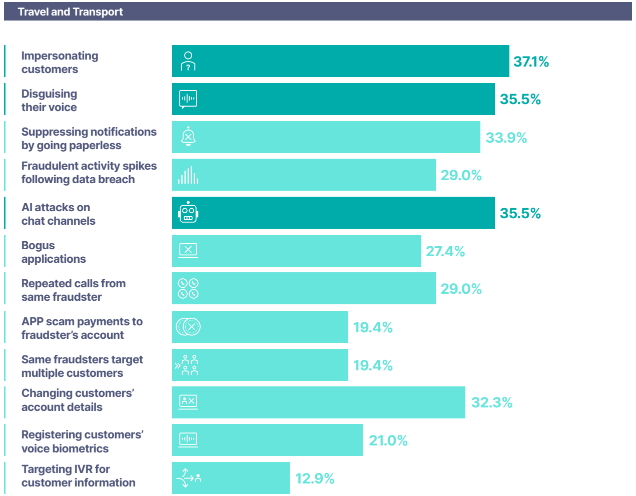


Q2: Fraudster tactics

Thinking about fraudulent activity in your organisation's contact centres in the last 12 months, which fraudster tactics, if any, are the most common?

By industry sector:

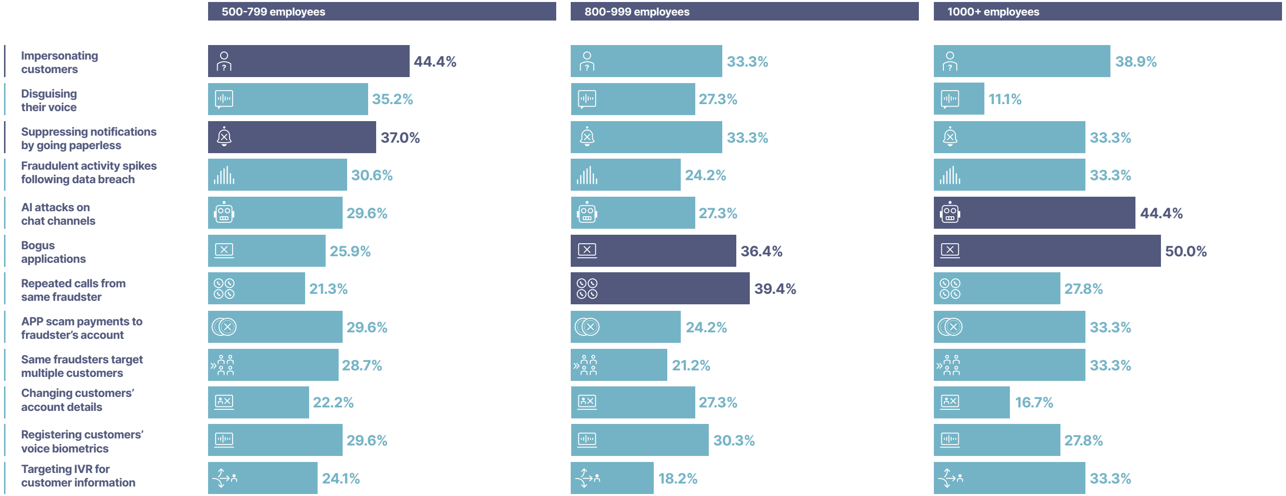


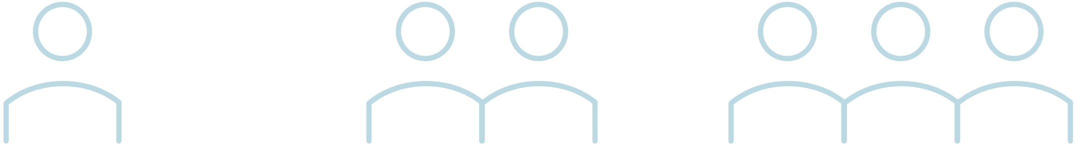


By company size:

Q2: Fraudster tactics

Thinking about fraudulent activity in your organisation's contact centres in the last 12 months, which fraudster tactics, if any, are the most common?



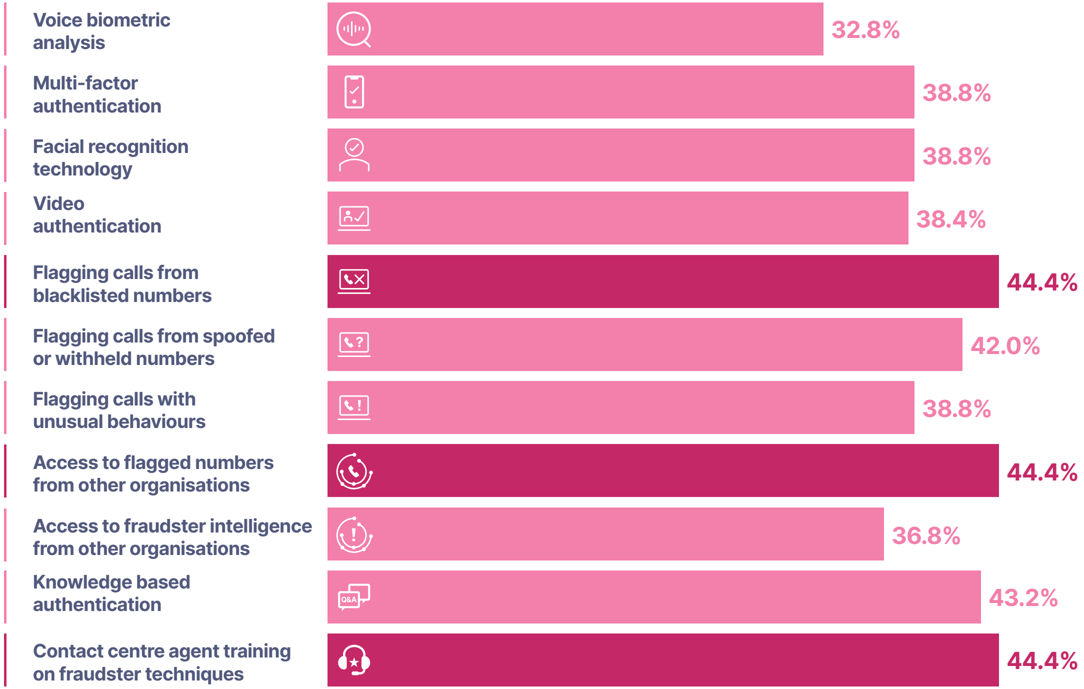


Q3: Detection

Considering some of the different counter-fraud focus areas and approaches available in the contact centre, please select the statement which best describes where you are at with your adoption/implementation of each of the following:

- The most commonly reported counter-fraud controls used to secure the contact centre:
  - training agents to avoid social engineering attacks
  - sharing intelligence
  - flagging calls from blacklisted numbers

All responses: Implemented already

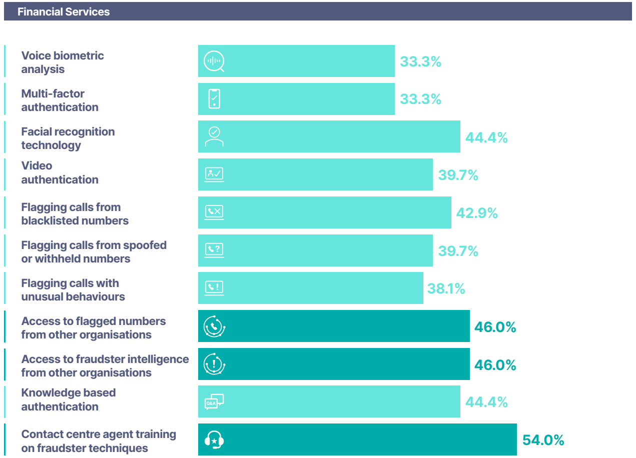


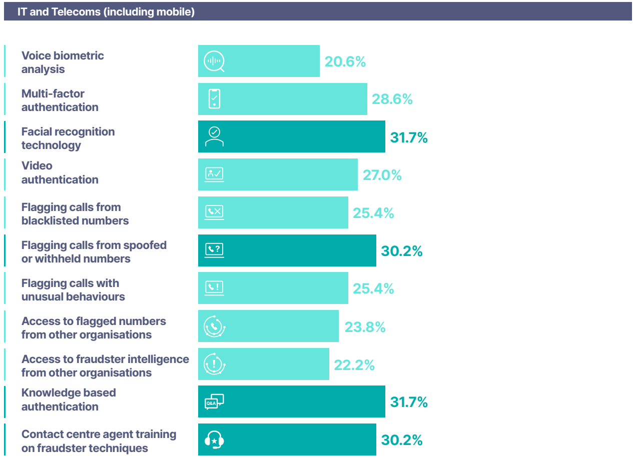
Q3: Detection

By industry sector: Implemented already

Considering some of the different counter-fraud focus areas and approaches available in the contact centre, please select the statement which best describes where you are at with your adoption/implementation of each of the following:

- A higher proportion of respondents from Financial Services report the adoption of agent training, KBAs and shared databases.
- IT and Telecoms have gone for adoption of multi-factor authentication, facial recognition, and flagging calls was reported by a higher percentage of IT and Telecoms respondents.



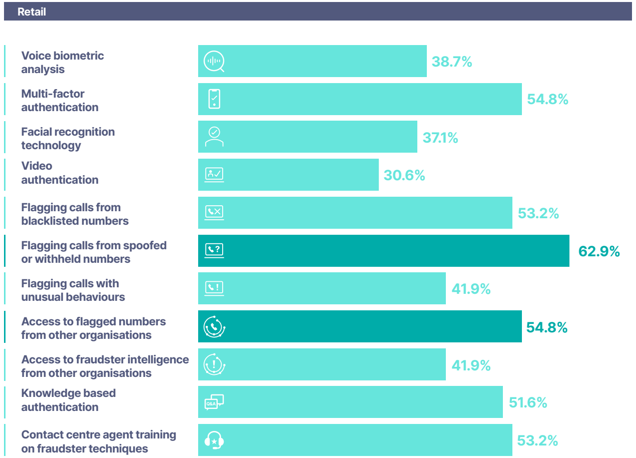


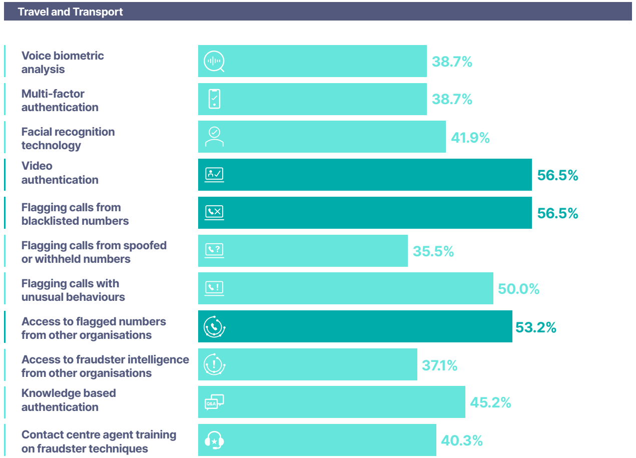
By industry sector: Implemented already

Q3: Detection

Considering some of the different counter-fraud focus areas and approaches available in the contact centre, please select the statement which best describes where you are at with your adoption/implementation of each of the following:

- Respondents from retail and travel sectors report especially high adoption of the range of controls.


Retail

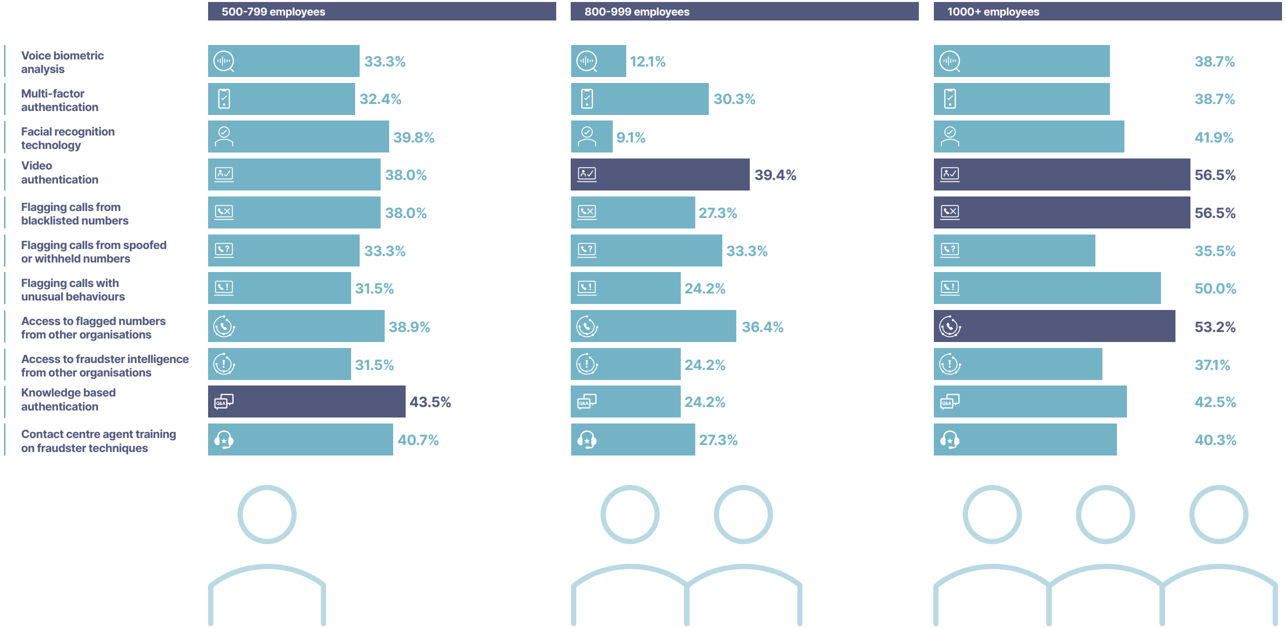

Travel and Transport

By company size: Implemented already

Q3: Detection

Considering some of the different counter-fraud focus areas and approaches available in the contact centre, please select the statement which best describes where you are at with your adoption/implementation of each of the following:

- Respondents from larger organisations are more likely to report the adoption of a particular control, such as flagging black-listed numbers and sharing intelligence.
- A higher proportion of respondents from smaller organisations report the adoption of video or facial recognition technology.

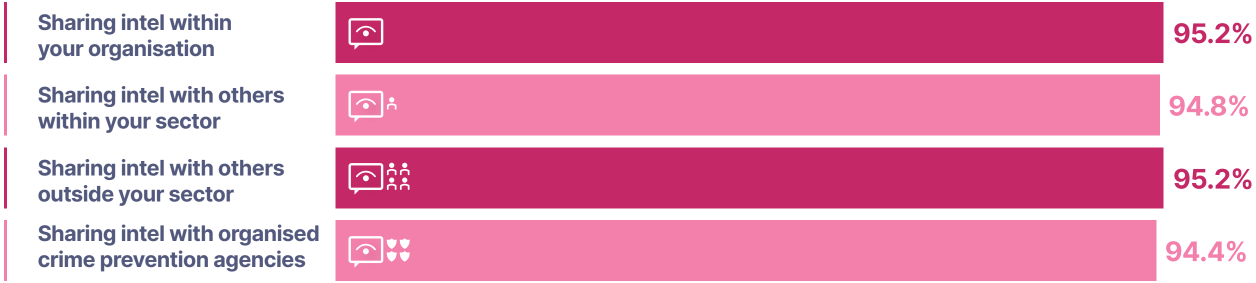


Q4: Sharing intel

When it comes to sharing of telephony fraud intelligence inside and outside your organisation, how often, if ever, do you carry out the following data-sharing practices in your organisation?

- Almost all respondents, across all sectors, report that they often share (always or sometimes) telephony fraud intelligence within their organisation, but they do not always have a formal process in place.

All responses: Sharing data often

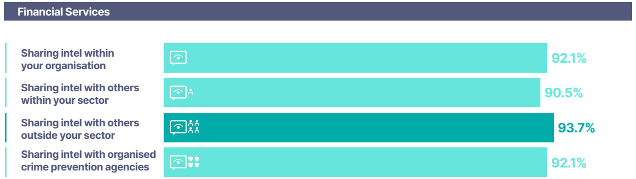


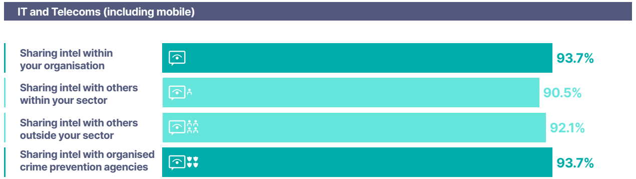
By industry sector: Sharing data often

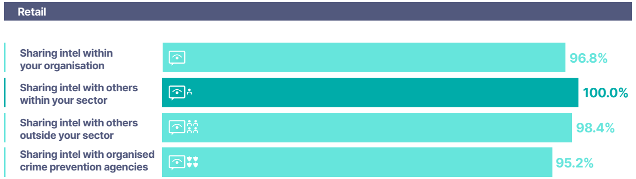
Q4: Sharing intel

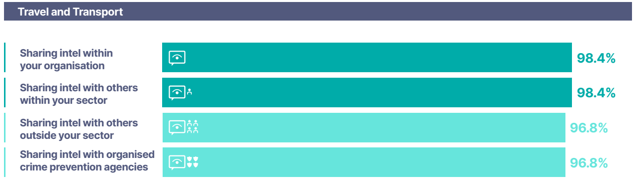
When it comes to sharing of telephony fraud intelligence inside and outside your organisation, how often, if ever, do you carry out the following data-sharing practices in your organisation?

- In Financial Services the most respondents report sharing with other sectors.
- In IT and Telecoms, the most respondents report sharing intel with both within the organisation and with organised crime prevention agencies.
- In retail, ALL respondents reported they often share intel within the sector.
- In Travel and Transport the most respondents share within the organisation and within sector.


Financial Services


IT and Telecoms (including mobile)

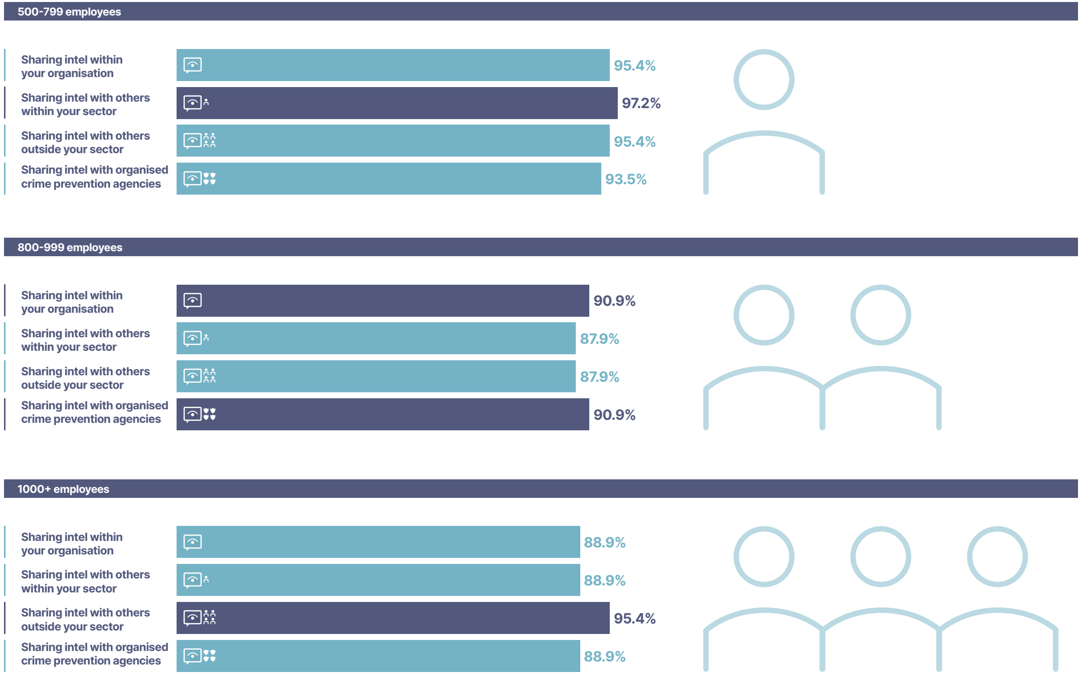

Retail


Travel and Transport

Q4: Sharing intel

When it comes to sharing of telephony fraud intelligence inside and outside your organisation, how often, if ever, do you carry out the following data-sharing practices in your organisation?

By company size: Sharing data often

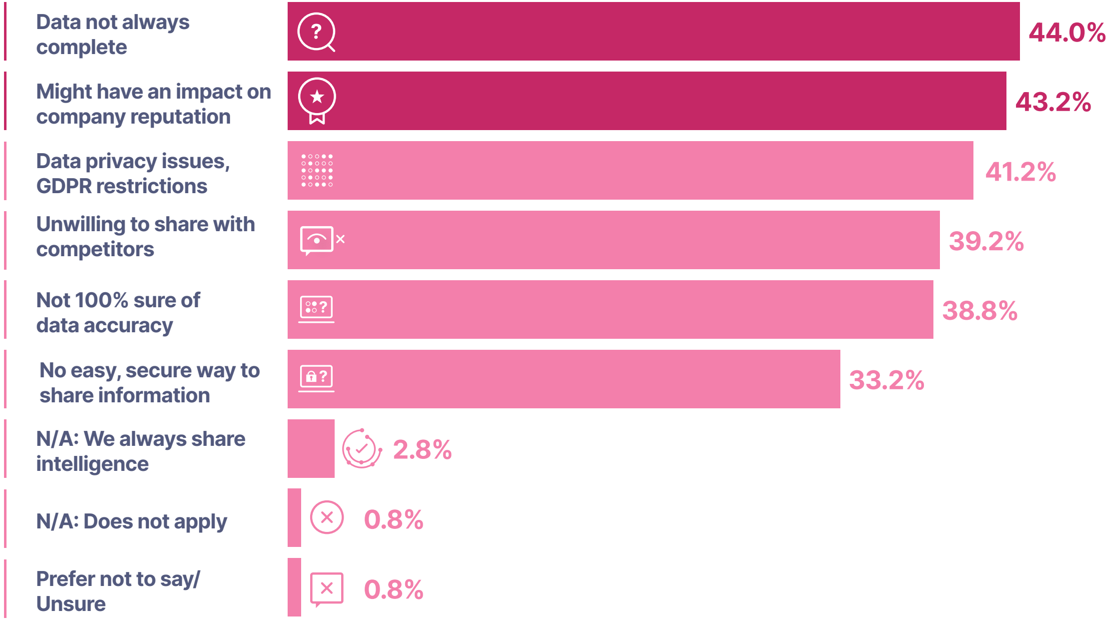


Q5: Sharing externally

When external intelligence sharing does NOT take place, if ever, what are the reasons, if any, for this?

- The most commonly reported concerns around data sharing are that data isn't complete (44%), or that there will be a negative impact on reputation or data privacy concerns.
- A high proportion of respondents appeared to be concerned about the negative impact on the company or that competitors may take advantage.

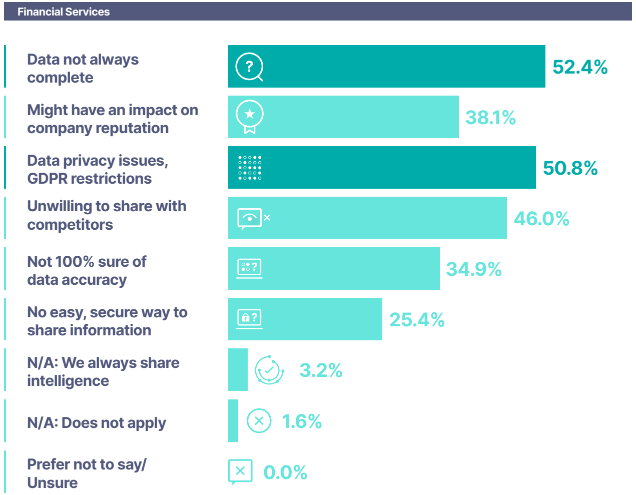
All responses:

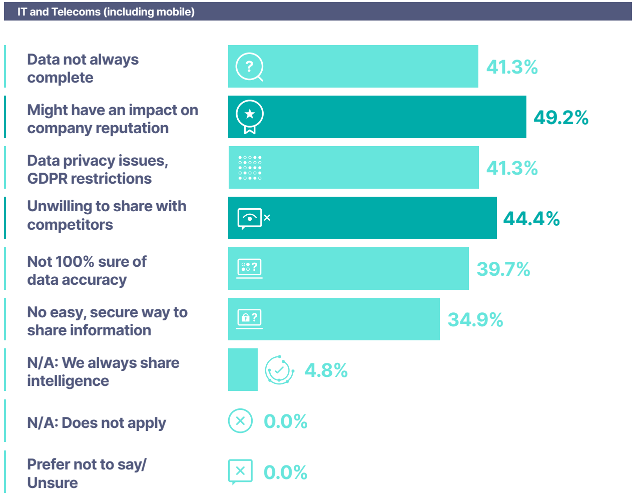


By industry sector:

Q5: Sharing externally

When external intelligence sharing does NOT take place, if ever, what are the reasons, if any, for this?

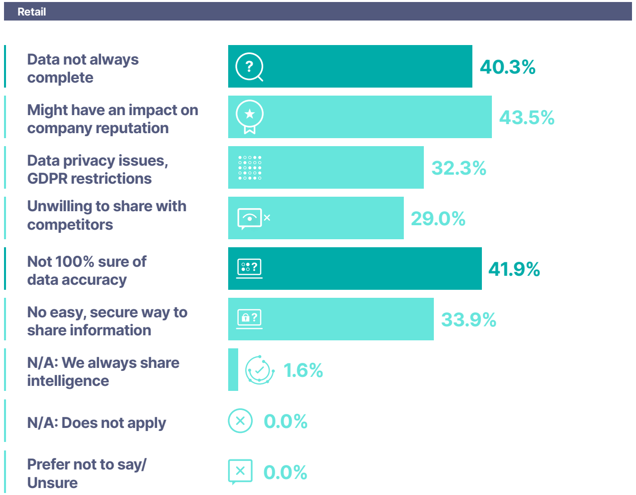


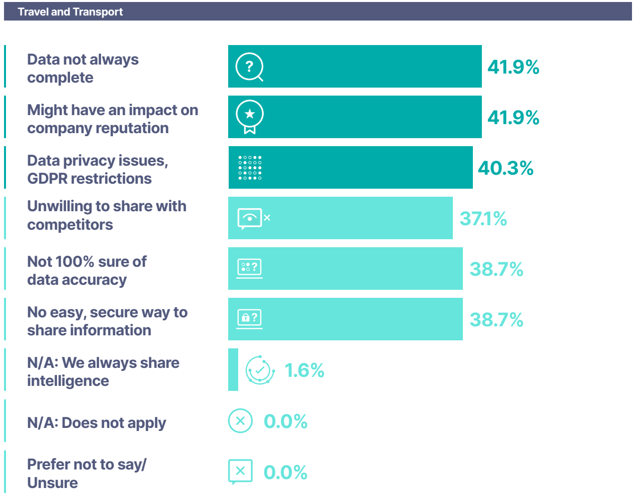


By industry sector:

Q5: Sharing externally

When external intelligence sharing does NOT take place, if ever, what are the reasons, if any, for this?

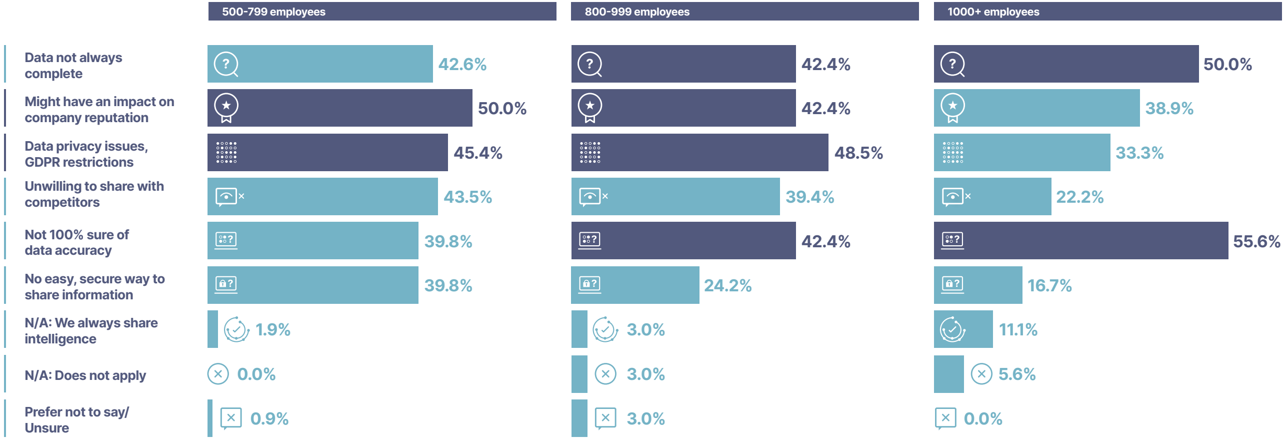

Retail

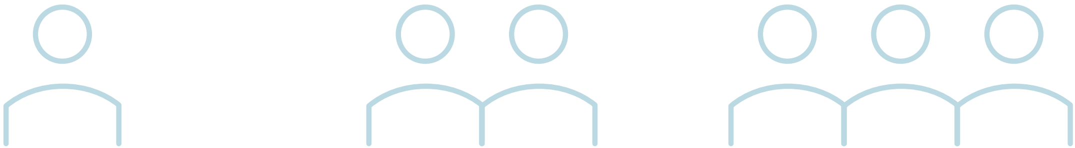

Travel and Transport

Q5: Sharing externally

When external intelligence sharing does NOT take place, if ever, what are the reasons, if any, for this?

By company size:





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.

Telephone: +44 20 3379 9000

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers

Smartnumbers Protect

Our cloud-based AI-powered platform - Smartnumbers Protect - analyses call data, caller behaviour and data on known fraudsters shared by our customers to assign a risk rating to incoming calls.

This helps contact centres prevent downstream fraud and improve customer experience for genuine callers.

Smartnumbers Consortium

Through the Smartnumbers Consortium, our community of customers and partners share intelligence in real time on the fraudsters they know.

Organisations are also able to connect and collaborate through Smartnumbers Consortium events.

Fight fraud. Protect the contact centre.

Contact us for more information.

Telephone: +44 20 3379 9000

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers