CONTACTBABEL

The Inner Circle Guide to Fraud Reduction & PCI Compliance

Sponsored by

Exceptional Customer Contact

The Inner Circle Guide to Fraud Reduction & PCI Compliance (UK edition)

Published July 2025

Make PCI compliance simple.
Keep customer payments secure.

IPI CLOUD PCI

IPI Cloud PCI helps UK contact centres eliminate risk, reduce compliance overheads, and enable secure, seamless customer payments, across every channel.

- ✔ PCI DSS Level 1 compliant
- ✔ Agent-assisted and self-service support
- ✔ DTMF masking, tokenisation, Pay by Link
- ✔ Designed for hybrid teams and remote agents

Discover more here!

CONTENTS

TABLE OF FIGURES

IPI – Secure customer interactions without compromise

IPI delivers innovative, customer-focused solutions that help UK organisations improve contact centre performance, secure sensitive data, and transform customer experience.

Our flagship solution, **IPI Cloud PCI**, is a fully cloud-native secure payments suite that removes contact centre agents, systems, and networks from PCI DSS scope. It enables organisations to accept secure payments by phone, IVR, or digital channels, with no sensitive data touching your infrastructure.

IPI Cloud PCI supports:

- Agent-assisted and self-service payment journeys
- DTMF masking and real-time tokenisation
- Secure Pay by Link transactions
- Pause/resume automation
- Omnichannel integration with leading platforms

With PCI DSS v4.0 driving increased scrutiny and continuous compliance requirements, IPI Cloud PCI offers a futureproof solution that reduces audit complexity, enhances customer experience, and supports remote and hybrid working environments.

We work with clients across regulated sectors including financial services, insurance, utilities, retail and travel helping them reduce fraud, protect customers, and deliver seamless CX.

Contact:

w: www.ipintegration.com

e: enquiries@ipintegration.com

t: 0778 978 4600

Head Office: Integration House, Turnhams Green Business Park, Pincents Lane, Reading, Berkshire, RG37 4UH

Other offices: UK- Manchester, London, Edinburgh. International - Manila (Philippines). Burgas (Bulgaria). Nicosia (Cyprus)

THE INNER CIRCLE GUIDE TO FRAUD REDUCTION & PCI COMPLIANCE

Every year, UK contact centres lose hundreds of millions to fraud, despite spending millions trying to prevent it.

With fraudsters growing more sophisticated, the pressure is on contact centres to tighten security while maintaining seamless, efficient customer experiences. But achieving PCI DSS compliance isn't just about ticking a box, it's about embedding real, robust security into everyday operations.

This report dives deep into the evolving landscape of payment card compliance and fraud prevention.

From pause-and-resume to DTMF suppression, biometrics to call signalling analysis, we explore what's working, what's not, and what's coming next.

This guide offers data-driven insights, cost breakdowns, and practical takeaways you can use now.

PCI COMPLIANCE & CARD SECURITY

Fraud continues to be a widespread concern both for retailers (merchants) and the finance industry. According to UK Finance[1], fraud losses on UK-issued cards, remote banking and cheques totalled around £1.2bn in 2023 with payment cards accounting for £551m of financial fraud loss.

One of the key ways that contact centres currently prevent fraud is by training agents to understand the risks and to use security best practices. Manual processes and agent training are consistently stated to be one of the most widely-used methods for reducing fraud, with around half of UK contact centres doing so. However, with fraudsters becoming increasingly clever at picking up personal data and passwords, relying on training is no longer enough.

Additional security questions during a call are typically required to verify identity. However, this approach takes longer and can annoy the customer as their legitimacy as the card holder is being questioned. Declined transactions by issuing banks also present a challenge as they can lead to additional costs, as both the acquirer and gateway require payment.

A card payment may be declined for multiple reasons in addition to attempted fraud, for example insufficient funds, unusual purchase patterns, a new bank card or incorrect CVV code. All of these reasons can prove costly to contact centres and customers.

How agents manage card payments during a call is important in terms of customer experience. While it is necessary to carry out the right identity and affordability checks this should not be detrimental to customer service.

New technology solutions are available that can facilitate and protect mail order, telephone order (MOTO) payments and allow smoother customer journeys. They enable an agent to advise the customer that an additional level of validation is required, rather than simply saying the transaction has been declined. Card holder identity can be established using a variety of validation methods, including 3D Secure (3DS) which is an additional two-factor authentication security layer used in online credit and debit card transactions.

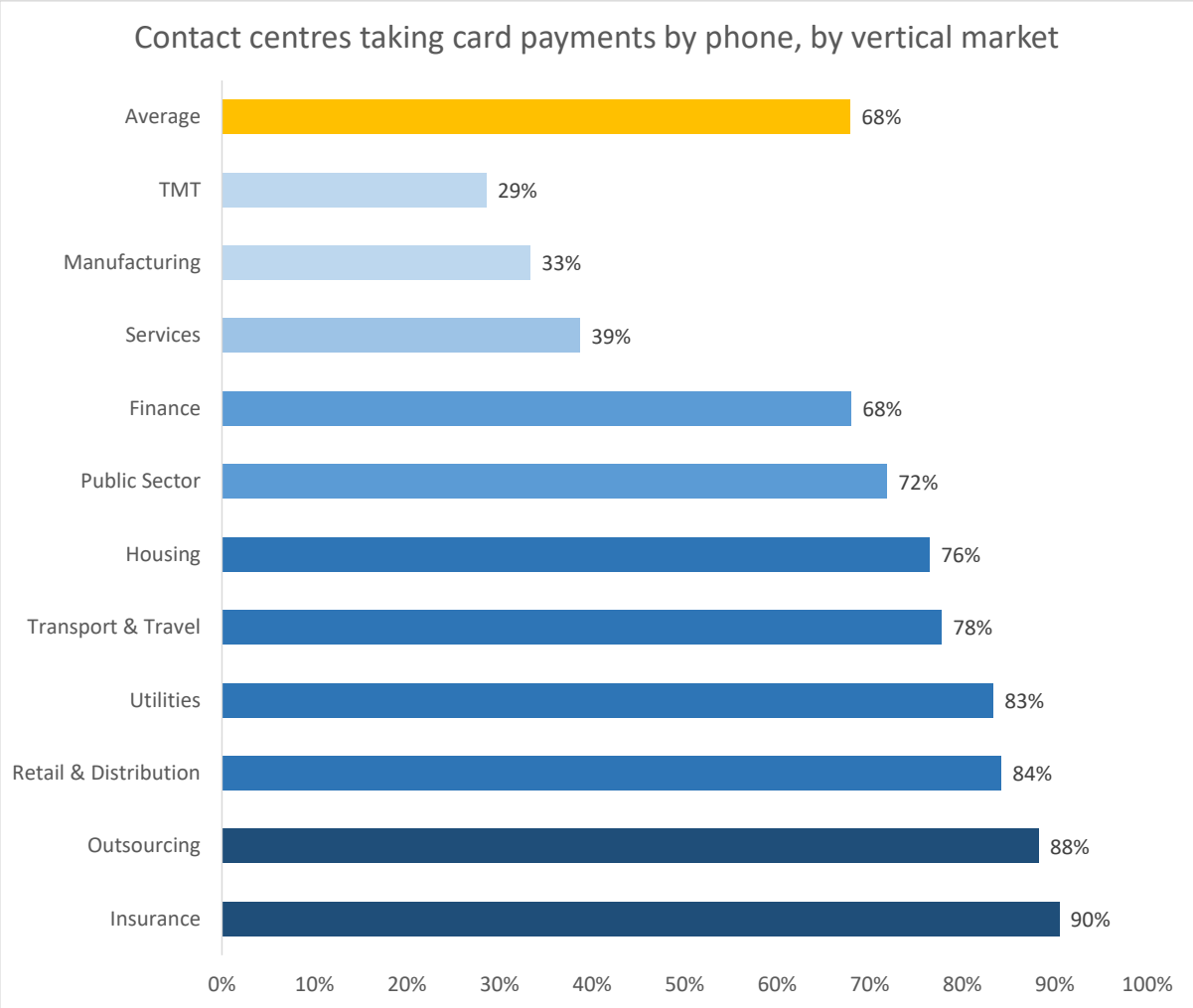
As well as helping to combat fraud, the result is increased transactions, reduce costs and a positive customer experience – a high priority for any contact centre.

[1] https://www.ukfinance.org.uk/system/files/2024-05/Annual%20Fraud%20Report%202024_0.pdf

THE USE OF PAYMENT CARDS IN THE CONTACT CENTRE

The majority of respondents in all vertical markets take card payments by phone in their contact centres, except for the manufacturing, TMT and services sectors.

Figure 1: Contact centres taking card payments, by vertical market



The usual positive size correlation is present to some extent once again this year. 65% of small and 64% of mid-sized operations take card payments, with 73% of large operations doing so.

Those businesses which wish to take card payments need to be PCI compliant, or take their operations out of scope entirely by contracting a third-party payment solution provider to handle payment for them.

PCI DSS BACKGROUND

The Payment Card Industry Data Security Standard (PCI DSS) is the creation of five of the largest payment card providers: VISA, MasterCard, American Express, Discover and JCB International, which together have named themselves the PCI Security Standards Council (PCI SSC).

Compliance to the PCI DSS is a contractual obligation by the Merchant to either the scheme or the acquirer (in the UK, to the acquirer; in the US to individual schemes and/or acquirer). Penalties are levied by the schemes in the event of a data breach, and may even deny the merchant the ability to take card payments at all. At the time of writing (December 2024), the current standard is PCI DSS 4.0.1, which will come into force on 31st March 2025.

To be PCI DSS compliant, merchants have to complete the correct Self Assessment Questionnaire (SAQ) that applies to the payment channel that they are assessing. They complete the SAQ documenting evidence of compliance and then get their most senior responsible executive to 'attest' (warrant) that the organisation that they represent meets the requirements of the standard. Third Party Service Providers (included hosted contact centre providers) have to complete SAQ D SP (Service Provider).

PCI DSS is not a prescriptive methodology to be followed to the letter, but should be viewed as a set of contractual requirements that organisations, their Internal Security Assessors and or, external Qualified Security Assessors (QSAs) can interpret in conjunction with the business's existing processes, technology and policies to reach the required level of information security.

PCI DSS 4.0 has moved towards being more flexible and outcome-based: rather than specifying exactly what and how a business needs to implement a technology or security measure, it states what must be achieved, leaving businesses to work out how best to do so while taking into account their own unique environment.

Compliance with PCI DSS should also be seen in the wider context of a far-reaching information security framework, which may also take into account industry-specific regulations.

There is likely to be a balance to be found between compliance with the various regulations in the context of the business's unique processes and internal guidelines. It's important to remember that – as especially noted in PCI DSS 4.0 – PCI compliance is not a once-a-year box-ticking exercise, but should be entwined in the security DNA of an organisation: QSAs are now told to select samples from throughout the year to prove compliance, rather than just using a snapshot at the time of assessment.

A list and explanation of each SAQ is available from the PCI Security Standards Council here.

PCI DSS REQUIREMENTS

There are 12 requirements to fulfil in order to achieve PCI DSS compliance (full details are available here[2]), with many specific sub-requirements within them, although for many businesses a large proportion of them may simply not apply.

- Build and Maintain a Secure Network and Systems
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need to know
  - Requirement 8: Identify and authenticate access to system components
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security for all personnel.

Whether contact centres decide to go down the self-assessment route or work with a QSA, all of the requirements of PCI DSS have some impact upon the way in which they work. Requirements 3, 4, 7, 9 and 12 may have the greatest relevance to the contact centre and its agents.

It should also be noted that requirements 5 and 6 can often be the most expensive, as the amount of work required gets exponentially bigger with the more staff a business has.

[2] https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

VALIDATING COMPLIANCE

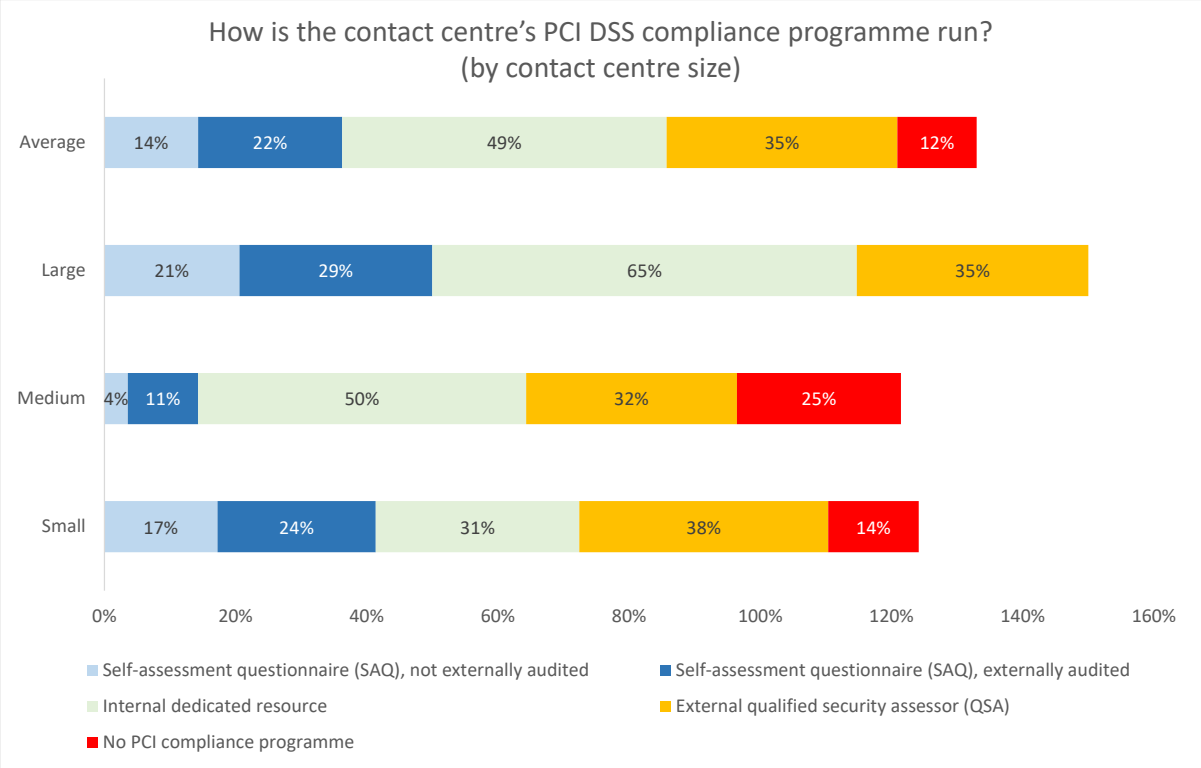
The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The Self-Assessment Questionnaire is a set of questionnaire documents that merchants must complete annually and submit to their transaction bank. Each SAQ question must be replied with “yes” or “no”. In the event that a question has the appropriate response of "no", the organisation must highlight its future implementation plans.

While small operations in the past were more likely to use internal self-assessment questionnaires, they have moved towards getting external help.

Roughly the same proportions across size bands use an external Qualified Security Assessor (QSA).

Larger operations are more likely to use a number of compliance methods, especially dedicated internal resource.

Figure 2: How is the contact centre’s PCI DSS compliance programme run? (by contact centre size)



NB: totals in the chart above add up to more than 100%, as multiple selections are allowed. Only those respondents that reported taking card payments **and** who were able to answer this question were included (35% of respondents did not know how their PCI compliance was run).

THE VIEW FROM THE CONTACT CENTRE

Potential danger points within the contact centre fall into three main areas: storage, agents and infrastructure. Storage includes customer databases and the recording environment – both voice and screen – and the potential opportunity for dishonest employees to access records or write down card details should also be considered.

In terms of infrastructure, this is not simply a matter of considering the CRM system or call recording archives, but also includes any element that touches the cardholder data environment. This could include, but is not limited to the telephony infrastructure, desktop computers, internal networks, IVR, databases, call recording archives, removable media and CRM / agent desktop software.

The PCI SSC information supplement "Protecting Telephone-Based Payment Card Data" had a change of emphasis away from "recorded" account data, towards "spoken" account data. The paper emphasised that "accepting spoken account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected into scope of PCI DSS", which also includes VoIP: "where VoIP is used for transmissions of payment card account data between a cardholder and an entity, the entity's systems and networks used for those transmissions are in scope.[3]"

The PCI SSC information supplement provides a useful classification of technology types. Technology is classified firstly by customer experience where the agent attends (in constant voice contact with the customer for the entire duration of the transaction) or unattended when they are not. The guidance then considers technology in terms of delivery media, either telephony or digital. Examples include:

- Telephony/attended: includes pause and resume, DTMF suppression
- Digital/attended: includes agent-initiated payment links sent via email, chat, SMS, social etc., where the agent remains on the call and can assist the caller
- Telephony/non-attended: IVR-based solutions, fully automated or initiated by agent
- Digital/non-attended: automated payment links sent without agent's action, or where the agent closes the call after the link has been sent but before payment is made.

The information supplement also differentiates between simple telephone environments (limited number of lines; dial-up or virtual payment terminal), and complex environments (agents linked to systems and servers, i.e. a contact centre). The supplement also explains the processes whereby an organisation can understand which part of their telephony environment is in scope for PCI DSS, and which the responsibility of third-party providers. Bear in mind that responsibility for the security of customer card data ultimately lies with the merchant organisation, so any third-party used must themselves be confirmed to be PCI compliant.

[3] See FAQ 1153 How does PCI DSS apply to VoIP? for more detail.

For those organisations which handle customer card data themselves, the various elements of card data are permitted to be processed and stored in different ways.

Figure 3: Data elements and storage in PCI DSS

	Data Element	Storage Permitted	Must Render Data Unreadable
Cardholder Data	Primary Account Number (PAN)	Yes	Yes (e.g. strong one-way hash functions, truncation, indexed tokens with securely stored pads, or strong cryptography
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiry Date	Yes	No
Sensitive Authentication Data	Full magnetic stripe data	No	Cannot store
	CAV2/CVC2/CVV2/CID (Card Security Codes)	No	Cannot store
	PIN / PIN Block	No	Cannot store

Compliance with PCI DSS should also be seen in the wider context of a far-reaching information security framework, which may also take into account industry-specific regulations. There is likely to be a balance to be found between compliance with the various regulations in the context of the business's unique processes and internal guidelines.

It's important to remember that – as especially noted in PCI DSS 4.0 – PCI compliance is not a once-a-year box-ticking exercise, but should be entwined in the security DNA of an organisation: QSAs are now told to select samples from throughout the year to prove compliance, rather than just using a snapshot at the time of assessment.

It's just as important to note that technology or payment solutions in themselves are not – and cannot be – "PCI compliant": compliance is judged and proven at a company level and is only complete when an organisation has not also considered their PCI compliance status but also the compliance status of Third Party Service Providers supporting their card payments process.

Policies and activities that are helpful include:

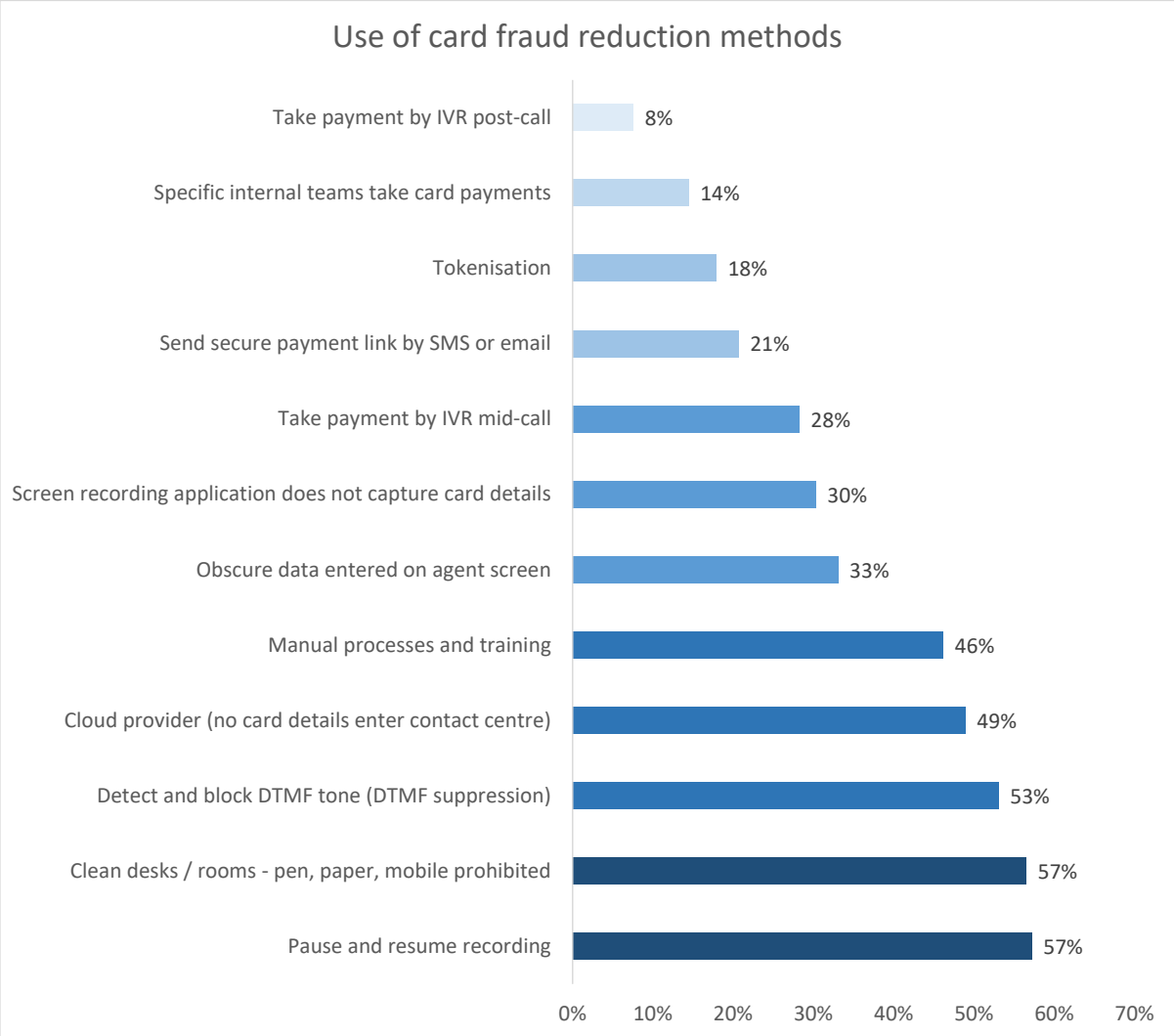
- make sure that contact centre employees do not share passwords or user IDs with each other, in order to maintain a segmented and auditable security and access environment
- limit the number of employees given access to full card information. For example, restrict access to call recordings based on logging and corporate role, only allowing screen recording playbacks that display payment card information to managers and compliance officers, having it masked for all other users
- manage the physical and logical access to stored recordings and regularly report upon those accessing this information
- do not allow payment card data to be transferred through non-encrypted means, including email, web chat, SMS or other means, and have the means to identify and delete it immediately if present
- initial focus should be on improving business processes, rather than implementing technology. For example, analysing and restricting access to cardholder information to only those employees who actually need it will significantly reduce the risk of fraud even before implementing any technology
- quarterly vulnerability scans should be carried out via an external approved scanning vendor approved by the Payment Card Industry Security Standards Council (PCI SSC), which holds a list of these. ASVs perform penetration tests on the company's network in order to verify that it cannot easily be hacked
- use secure data centres and limit physical access to servers storing payment card data
- do not record sensitive authentication data such as the card validation code in any circumstances
- use strong encryption for the storage and transit of voice traffic, call recordings, screen recordings and personal identification data, making sure that the most current guidelines on encryption and transmission protocols are adhered to
- up-to-date, fully patched and automated malware, anti-virus and personal firewall software (of particular importance to homeworkers) - requirements 5 and 6
- regularly review stored data, and keep only that which is necessary for business or regulatory purposes. For example, hotels may need to keep customers' credit card details from the reservation point until checkout: there is no hard and fast rule.

THE USE OF CARD FRAUD REDUCTION METHODS

The PCI DSS guidelines state: "As a starting point, consider whether the organisation should aim at excluding telephone-based card payment data entirely…for organisations committed to taking payments over the telephone, consideration should be given to techniques that minimise exposure of PAN and SAD to the telephone environment and balance that with user/customer experience requirements, with the object of significantly reducing the CDE (card data environment) or eliminating the CDE altogether".

Respondents were presented with a list of solutions, approaches and business processes that aim to reduce the risk of card fraud within the contact centre, and indicated which they used. It should be noted that many of these methods used do not in themselves render the operation fully PCI-compliant, although methods that do not allow the card data into the contact centre at any point (even encrypted) will take the operation out of the scope of PCI. Respondents use an average of 3.9 card fraud reduction methods.

Figure 4: Use of card fraud reduction methods



Beyond compliance:

Elevating payment security with IPI Cloud PCI

The introduction of PCI DSS version 4.0 marks a significant shift in how UK contact centres approach compliance, risk, and customer experience. Compliance can no longer be viewed as a one-time audit. Organisations must now demonstrate continuous adherence, outcome-based security practices, and full visibility into how payment data is handled and protected.

For contact centres managing hybrid and remote teams, this presents a growing challenge. Sensitive cardholder data must be safeguarded at every touchpoint, but legacy infrastructure, decentralised systems, and distributed workforces have widened the threat landscape.

This is where **IPI Cloud PCI** delivers its value.

IPI Cloud PCI is a cloud-native, secure payments suite that removes your contact centre, agents, and internal systems from PCI DSS scope. This reduces compliance overhead, simplifies audits, and dramatically lowers your risk profile. Payment data is tokenised at the point of capture, using DTMF masking, secure Pay by Link workflows, and voice-safe, agent-assisted methods - so no sensitive data ever enters your environment.

But compliance alone is not enough. IPI Cloud PCI also enhances customer and agent experience. Agents can remain present during the payment process without ever seeing or hearing card details. This creates a seamless journey for customers, reduces call abandonment, and supports those who may struggle with IVR or keypad-based systems.

In highly regulated sectors such as finance, insurance, utilities, retail and travel where reputational risk is high and compliance is non-negotiable, IPI Cloud PCI offers a future-proof approach. It supports secure payments across all channels, whether agents are on-site, remote, or hybrid, while aligning with broader governance frameworks like Cyber Essentials and GDPR.

Beyond security, the platform also integrates easily with existing systems and provides full audit visibility, making it as operationally practical as it is secure.

In a world of increasingly sophisticated fraud, compliance is no longer a checkbox - it's a strategic imperative. With IPI Cloud PCI, UK contact centres can protect their customers, empower their agents, and future-proof their business.

Discover IPI Cloud PCI: Seamless, secure, and scalable.

Find out more.

Contact Us

T +44 (0) 1189 184 600 **E** enquiries@ipintegration.com **W** ipintegration.com

Pause and resume recording, clean desk/room policies, DTMF suppression and cloud-based third-party solutions were the main methods used to reduce card fraud. Manual processes and training, and the use of a third-party cloud-based provider were also widely used.

Pause and Resume (57% at end of 2024 - down from 59% at end of 2023)

Pause and resume is consistently one of the most popular fraud reduction solutions.

'Pause and resume' or 'stop-start' recording aims to prevent sensitive authentication data and other confidential information from entering the call recording environment. Pause and resume may be agent-initiated, act for a fixed time period (e.g. stopping recording for a minute), or be fully automated. The PCI DSS standard is interpreted as preferring automation over manual intervention to avoid human error.

Automated pause and resume may use an API or desktop analytics to link the recording solution to the agent desktop or CRM application, being triggered when agent navigates to a payment screen, for example. The recording may then be paused, to be resumed at the time when the agent leaves the payment screen, which in theory should remove the period of time whereby the customer is reading out the card details.

This method, consistently the most popular, has several obvious benefits, not least of which include a very low set-up cost and the speed of implementation. However, breaking a recording into two parts makes it difficult to analyse the entire interaction, and goes against some industry-specific regulations, e.g. any financial services regulations which require a record of the full conversation, so some contact centres prefer to mute the recording or play a continuous audio tone to the recording system while payment details are being collected, meaning that there is still a single call recording which can be used for QA and compliance purposes.

This principle is similar to that applied to **screen recording** applications, where 30% of respondents (2023- 28%) stated that their application does not record card details from the agent's screen.

33% of respondents (2023 – 30%) **obscure card details** on the agent's screen, to prevent copies being made.

It should be noted that the November 2018 PCI SSC information supplement "Protecting Telephone-Based Payment Card Data" put more emphasis on "spoken" account data, rather than just focusing on recorded data, which is what pause and resume is obviously aimed at managing. The paper states that "accepting spoken account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected into scope of PCI DSS" including VoIP, so businesses should be aware that pause and resume solutions should be used as part of wider PCI compliance.

Improving Manual Processes and Agent Training (46% - up from 42% in 2023)

One of the most widely used fraud reduction methods is that of improving manual processes and agent training: the biggest risk in any organisation relating to data theft is its staff – not necessarily from fraudsters, but laxity in taking proper care of data – and the relatively low cost of training and education of the risks can go a long way in making staff vigilant to perils such as phishing emails and such like. Phishing emails can mean that staff innocently allow hackers to enter the system, and is a far bigger risk than a rogue staff member writing the odd card number down.

Clean Desks / Rooms (57% - up from 54% in 2023) and Dedicated Payment Teams (14% - down from 15% in 2023)

Some organisations set up dedicated payment teams, working away from other agents, often in a clean room environment with no pens, paper or mobile phones, so that customers can be passed through this team to make payment.

As these agents have a single responsibility – handling card payments – sometimes they are underutilised, and at other times there can be a queue of people waiting to make payments. In terms of the customer experience, this latter scenario is suboptimal.

A clean room is generally not seen as being a particularly pleasant working environment for agents, being spartan of necessity. Not being able to be in touch with the outside world, for example with children or schools, can be a significant problem for some agents. It has been estimated that it takes around £2,000 per agent per year to create and maintain a clean room environment.

A clean desk environment is somewhat easier to establish and maintain, and can reduce the threat of card fraud to some extent.

Third-Party Cloud-Based Payment Solution (49% - no change on 2023)

The increasing requirements and costs associated with more stringent payment technology, processes and training mean that many contact centres are choosing to use a third-party to handle card payments, rather than remove the payment option entirely.

49% of this year's respondents use third-party cloud-based payment solutions. Using a cloud-based solution to intercept card data at the network level means that no cardholder data is passed into the contact centre environment, whether infrastructure, agents or storage. As such, this de-scopes the entire contact centre from PCI compliance.

Like any cloud-based solution, it relies heavily upon the security processes and operational effectiveness of the service provider, although the PCI DSS attestation of compliance and external audits, along with regular penetration testing may well show superior levels of security over what is present in-house.

Some cloud-based solutions may require greater levels of integration or configuration than their on-site equivalents, but are engineered so as to minimise changes to the contact centre systems, processes or agent activities.

This option has become significantly more popular with businesses which wish to take card payments but not have to invest in technology or manage the processes that ensure PCI compliance.

IVR Payments – post-call (8% - down from 9% in 2023) and mid-call (28% - up from 20% in 2023)

A minority of respondents, especially those with large contact centres, use an automated IVR process to take card details from the customer, cutting the agent risk out of the loop entirely.

Mid-call IVR (or agent-assisted IVR) is seen as a more customer-friendly approach than post-call IVR and has grown in usage over the past few years: the caller may have additional questions or the requirement for reassurance and confirmation after the payment process, perhaps around delivery times or other queries not related to the payment process.

However, the card data is still within the organisation's network, so although this approach takes the agent out of scope, it does not in itself ensure PCI compliance.

Detect and Block the Phone's DTMF Tones (53% - down from 54% in 2023)

53% of this year's respondents use DTMF suppression in order to assist with card fraud reduction, which is a continuation of a strong general upward trend.

DTMF suppression describes the practice of capturing DTMF tones and altering them in such a way that cardholder details cannot be identified either by the agent, the recording environment or any unauthorised person listening in.

DTMF suppression aims to take the agent out of scope as well as the storage environment, as card details on the agent's screen may be masked as well as the DTMF tones being neutralised (thus removing any – albeit theoretically small – danger of a handheld recorder being used).

At the point in the conversation where payment is to be taken, the agent directs the customer to type in their card details using the telephone keypad. The DTMF tones are altered so that they no longer represent the card number or sensitive authentication details. The caller inputs their card data via a touchtone keypad in a similar way to an IVR session, keeping them in touch with the agent at any point in the transaction in case of difficulty, clarification or confirmation.

Although this method has grown in popularity in recent years, it can be one of the more expensive card fraud reduction methods to implement.

Tokenisation (18% - up from 11% in 2023)

The practice of **tokenisation** is used in 18% of this year's respondents' operations.

Tokenisation takes place in order to protect sensitive card information such as the PAN (primary account number or 'long card number') by replacing it with non-sensitive data which merely represents the initial data. The purpose of this is to devalue the data so that even if it is hacked or stolen, it is of no use to a criminal.

One of the main benefits to tokenisation is that it requires little change to the existing environment or business processes, as apart from the addition of a decoding mechanism, the flow of data, its capture and processing works in the same way as if it were true card information coming into the contact centre environment.

A customer entering a 16-digit card number might have six digits within the middle of the card taken out and replaced by entirely different digits, before this information is passed as DTMF tones into the contact centre environment. This allows the contact centre to be outside PCI scope, as there is actually no **real cardholder data** entering the environment, as well as making it a less attractive target for data hacking and stealing. Tokenisation does not require special integration with existing payment processes, storage systems, telephony or IVR systems, nor does the agent desktop have to change as the same data format is coming into the desktop environment.

The first stage of tokenisation is to collect the actual cardholder data via DTMF tones. The solution replaces the associated tone with a neutral or silent tone, and sends the actual number relating to the DTMF tone elsewhere within the solution in order to be tokenised. Card numbers and sensitive authentication data such as card validation codes are replaced, and the new tokenised DTMF tones are played down the line to the contact centre. The actual cardholder data is held temporarily within the hosted environment.

Within the contact centre environment, the tokenised DTMF goes to the same places that the existing payment process defines, being recorded as usual and going to the agent desktop as if the card information was actually true, passing through a decoder (which may be hardware or software) which converts the tones to keystrokes that are entered in the payment screen. As the card data is only a tokenised representation, it cannot be said to be actual cardholder data and thus does not fall into the scope of PCI DSS compliance.

Once the agent submits the tokenised payment card details, the transaction is sent back to the hosted environment, where the tokenised data is matched and converted back into the actual cardholder information, which is passed on to the payment service provider, which returns the usual payment success/failure confirmation.

Customers should check that any hosted tokenisation solution will not alter the performance of any required card number validation checks, including card length, range validation and 'Luhn' checks (to make sure a card number 'looks right' before presenting it to the payment services provider). The PCI SSC has published tokenisation product security guidelines[4].

[4] https://listings.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

Send Secure Payment Link by SMS or Email (21% - up from 20% in 2023)

This is the fifth year of tracking this self-service card fraud reduction method, which involves sending an SMS, email or WhatsApp link to a customer which then opens a secure form in which card details can be entered. It has grown from only 5% in 2020 to 21% in 2024.

Card data is kept outside the organisation, keeping it outside of scope and can also be linked with tokenisation to collect new information if existing data has expired.

This method is secure and reduces agent time, allowing customers to pay at their own convenience, although will possibly be more suitable for some demographics.

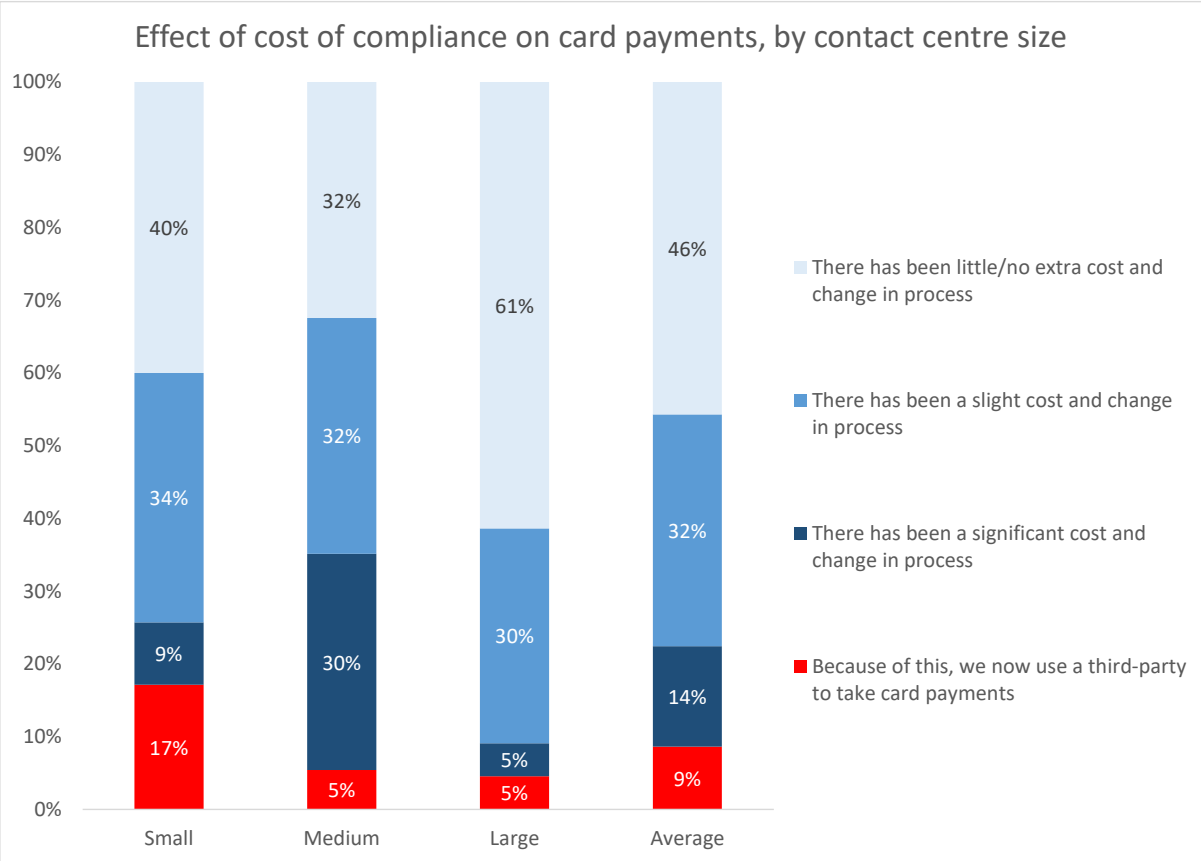
THE COST OF PCI DSS COMPLIANCE

The following chart shows that a significant proportion of contact centres have found that the cost of PCI DSS compliance is very considerable, with 14% of respondents – particularly in mid-sized operations – stating that they have seen a significant cost associated with compliance, as well as a change in their processes. A further 32% report a slight increase in cost.

46% of survey respondents state that they have not had to increase their costs or change they way in which they operate in order to be compliant.

9% of respondents state that the cost and effort of compliance was so high that they decided to use a third-party to take card payments, in order to take the contact centre out of scope.

Figure 5: Effect of cost of compliance on card payments, by contact centre size

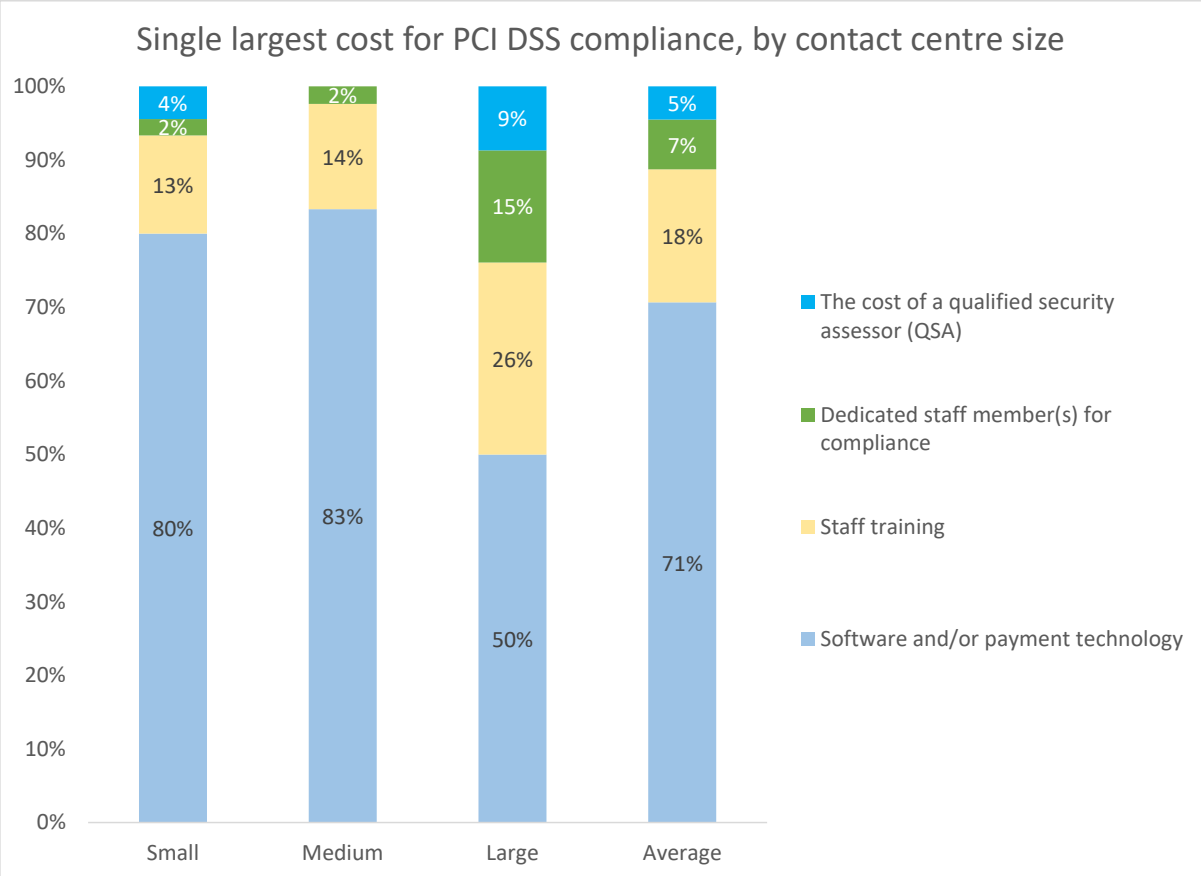


71% of survey respondents state that software and/or payment technology is the single largest cost associated with PCI DSS compliance. This is particularly the case in small and medium-sized operations.

In the largest contact centres, the cost of training staff in card fraud prevention techniques and processes is said to be the largest cost in 26% of cases, with 15% stating that having dedicated compliance staff was the largest cost.

9% of those in large operations stated that the high cost of bringing in external qualified security assessors (QSAs) was the greatest cost borne.

Figure 6: Single largest cost for PCI DSS compliance, by contact centre size



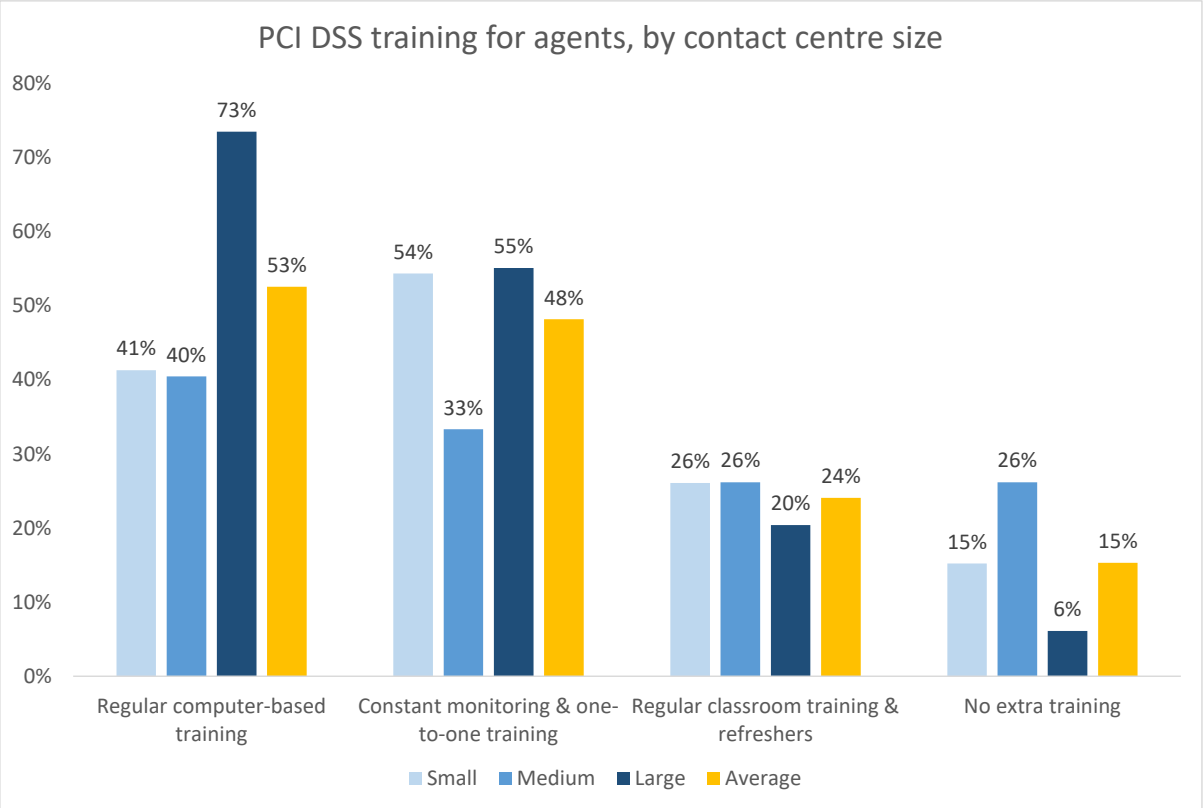
The cost of staff training is reported to be a major drain on resources for larger contact centres in particular. Regular computer-based training, used to educate agents about card fraud reduction practices, is likely to be scalable and require less personal support from managers and security specialists, which should make it popular with cost-sensitive small and medium operations as well as larger contact centres.

Agents in small operations are as likely as those in larger contact centres to be receiving monitoring and one-to-one training.

15% of survey respondents do not provide any additional PCI DSS or card fraud reduction training for agents whatsoever, and this is considerably more likely to be the case in smaller operations.

However, it should be noted that PCI DSS v4.0 places greater emphasis on the need for annual training courses and making staff aware of social engineering and phishing attacks.

Figure 7: PCI DSS training for agents, by contact centre size



CUSTOMER IDENTITY VERIFICATION & FRAUD REDUCTION

Customer security processes are about two factors: are you who you say you are, and are you allowed to do what you are trying to do? Until a few years ago many businesses relied on trust that the caller was who they claimed to be, asking only for a name and address.

Today, identity verification processes are now seen as critically important and most calls that are not initial enquiries will need to verify a caller's claimed identity by asking for additional information that only the real customer should know (knowledge-based authentication, or KBA).

However, fraudsters have often gained access to personal information such as mother's maiden name and date of birth, along with payment card details that have been stolen from websites, and research has shown that knowledge-based questions are answered correctly by fraudsters the large majority of the time.

The increasing focus upon fraud detection, strengthened by the need to comply with regulations, has meant that identity verification continues to become more important year-on-year, yet businesses have been slow to take up alternatives to the traditional challenge/response method.

Identity theft is high-profile, and businesses have tightened security and been seen to do so by their customers: fraud prevention is a brand issue, as well as a regulatory one. While fraud certainly causes losses to a business, along with the threat of regulatory fines, risk of losing customers' confidence by being seen as lackadaisical about security is at least as great a risk. Criminals' methods and the technology used have become more sophisticated, and businesses responded by introducing ever more complex identity verification processes.

In many cases, customer identity verification has become intrusive and inconvenient for the customer, who is expected to remember an increasing array of IDs, passwords, PINs, memorable information, or details of their last transactions.

It takes an average of 50 seconds to verify a customer's identity manually, and this mounts up: the UK contact centre industry spends billions of pounds each year, just to verify the caller is who they claim to be, and are permitted to do what they are asking.

Identity verification processes are typically based on one or more authentication factors that fall into the following generally accepted categories:

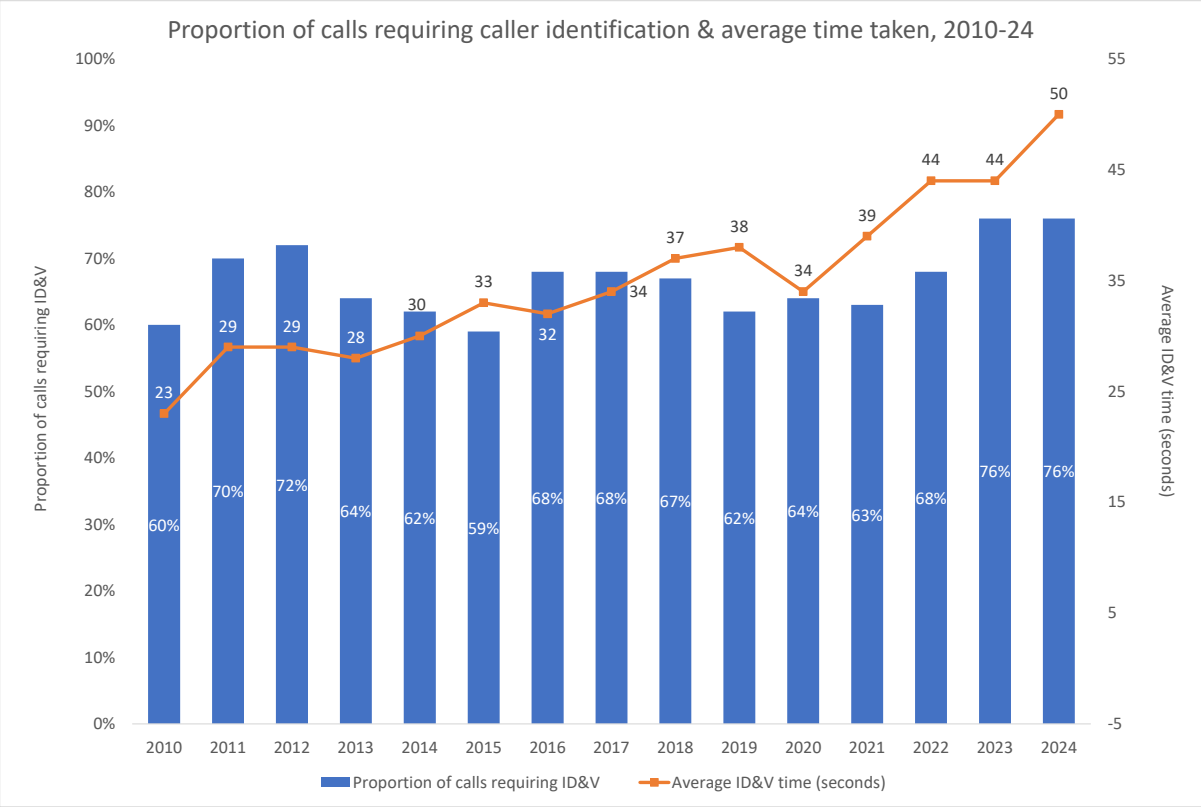
- something you know - e.g. password, PIN or memorable information
- something you are - a biometric such as a fingerprint, retina pattern or voiceprint
- something you have - a tangible object, e.g. a PIN-generating key fob, the 3- or 4-digit security code on payment cards or a registered phone to which an SMS or other authentication code can be sent.

Combining these factors creates a more complex, and potentially more secure two-factor or three-factor authentication process (2FA / 3FA), although this is often quite inconvenient and time-consuming for customers. Being able to rely upon previously enrolled voice features or having the calling device, location and other factors assessed pre-call (rather than have to remember various pieces of information or carry round a code-generating device) can make identity verification far quicker and easier for the customer.

This is also likely to impact positively on agent engagement: an agent taking 80 calls per day will spend around 45 minutes of an eight-hour shift doing the mundane and repetitive task of taking customers through security.

Although in-call efficiency has improved, identity verification is slower than it has ever been: over the past decade, our surveys have found consistently that around 60%-70% of calls require identity checks, which take considerably longer due to more stringent testing (a rise in the length of authentication of over 100% since 2010).

Figure 8: Proportion of calls requiring caller identification & average time taken, 2010-24



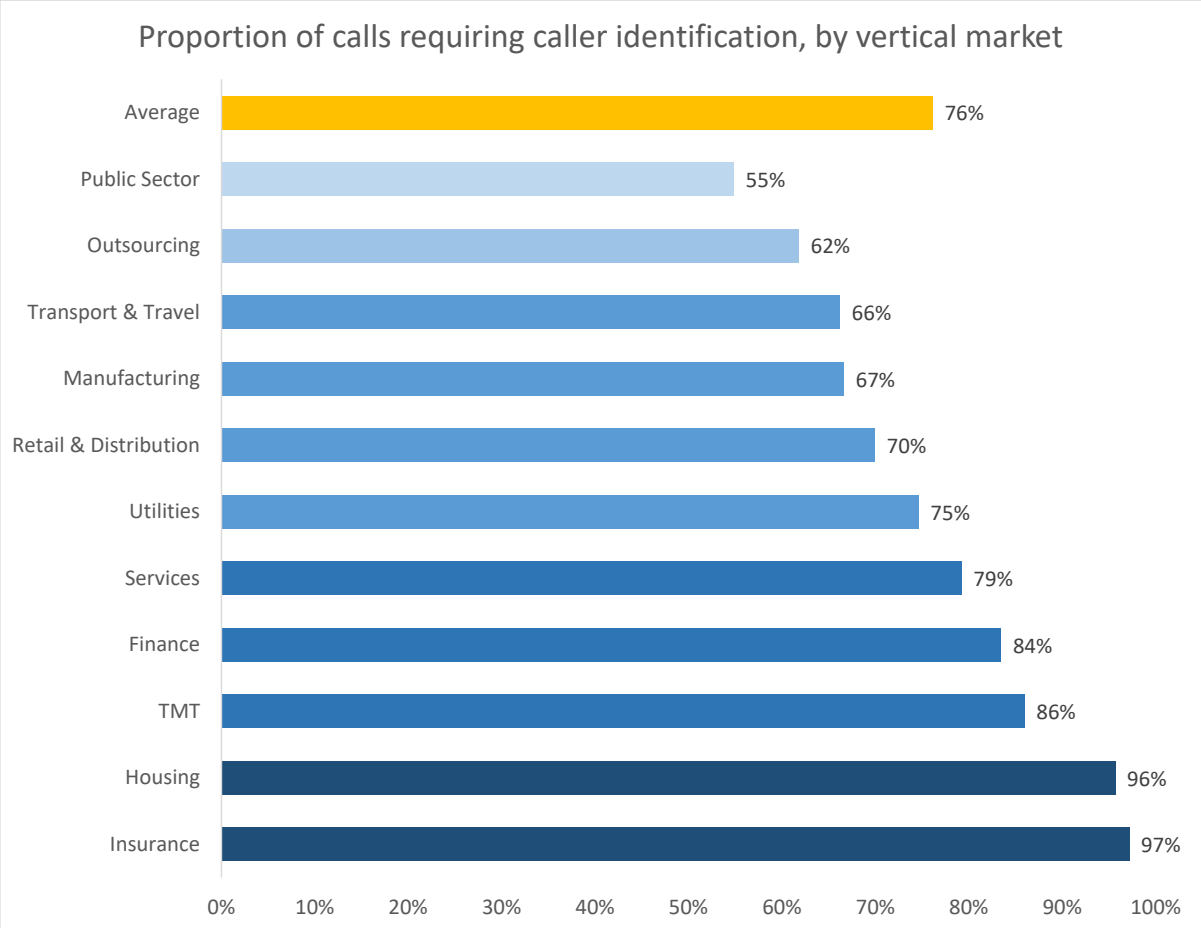
Industry-wide, a mean average of 76% of UK inbound calls are stated to require caller identity verification, the highest on record.

44% of respondents state that all callers go through identity verification, with only 7% stating that they never do so.

Insurance, finance, housing and TMT operations are the sectors most likely to require identity verification. Helplines, such as often found in the public sector and manufacturing vertical markets tend to require less authentication.

As we would expect, service-oriented operations are far more likely than sales-focused contact centres to require authentication, as access to user accounts is required.

Figure 9: Proportion of calls requiring caller identification, by vertical market



92% of calls requiring customer authentication need agents, with 10% handled through touchtone IVR.

Respondents that use IVR or speech recognition may also use the agent to double-check in some instances once the call is passed through, wasting the caller's time and increasing the contact centre's costs.

Figure 10: Caller identity authentication methods (only those contact centres which authenticate some or all calls)

Identification method	Proportion of callers identified using this method
Agent	92%
DTMF IVR (touchtone)	10%
Speech recognition	1%
Voice biometrics	<1%
NB: total is greater than 100% as some calls may require multiple identification methods	

The mean average time taken to authenticate using **only** an agent is 48 seconds. The figure for authentication using an IVR is 39 seconds. As the agent's time is not used, the call duration (from the operation's perspective) and cost per call is reduced.

The overall authentication figure of 50 seconds can be accounted for instances where the initial automated attempt to authenticate the customer fails or requires further checks by the agent.

Figure 11: Time taken to authenticate caller identity using only an agent (seconds)

	Seconds to authenticate caller identity using only an agent
1st quartile	20
Median	40
3rd quartile	60
Mean	48

The unnecessary cost of caller authentication

Using figures from this report and other ContactBabel research, it is possible to estimate the industry-wide cost of customer identification authentication using an agent. Please note that as respondents change each year, this figure is an indicative estimate based on this year's survey and should be read as such.

76% of all calls require a security and identification process to be completed first. This year, 92% of calls were reported to be authenticated by agents. On average, it takes 48 seconds to go through security using agents. Using these statistics, it is possible to estimate how much UK contact centres spend each year on screening customers by using agents.

Inbound calls per year (handled by agents): 5.85bn[5]

Proportion of inbound calls that require security and identification checks: 76%

Average length of agent-handled security and identification check: 48 seconds

Average call duration: 6m 56s (416 seconds), therefore 11.5% of the call is ID&V

Mean average call: £6.25

Cost of time spent on agent-handled security and identification check: 72.1p per call

Proportion of calls requiring ID&V: 76%, of which 92% require an agent

Therefore, overall cost of agent-handled security and identification checking: £2.95bn per year

[5] ContactBabel, "UK Contact Centres 2024-2028: The State of the Industry"

To recap, there are several factors to consider when trying to predict changes in the ways in which customers are identified:

- businesses want to reduce the cost of fraud
- customers want convenience, but also their personal information and assets protected
- businesses need to comply with existing and new laws and regulations
- the contact centre industry spends excessive amounts of money on identifying and verifying customer identities
- relying on a single method of customer identification relies heavily on it being fool proof
- existing methods of identity verification (e.g. PIN, password, device, etc.) are not secure and/or are user-unfriendly
- it is not just criminal fraud that identity verification aims to stop. The issue of privacy, especially in the healthcare vertical market, is a powerful driver for using right-party authentication to facilitate personal information sharing. This is also the case when using speech-enabled automated outbound calls, it being necessary to make sure that the person answering the call is the one to which the business actually needs to talk.

SECURITY CONCERNS

Respondents were asked to rate the level of concern they had about the possibility of fraud coming from various sources.

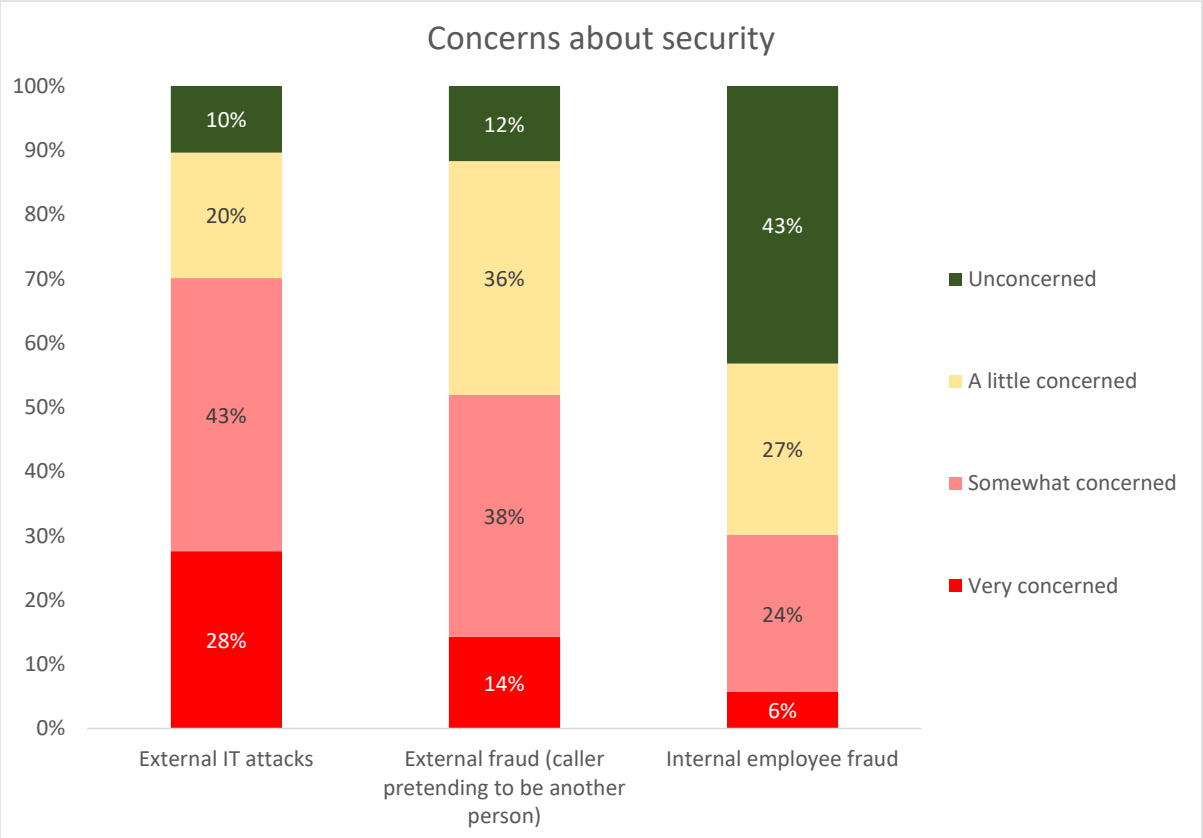
Concerns about external IT attacks have usually been consistently significant across all size bands, but this year, the largest operations show the greatest concern about this, with 79% of large operations reporting significant levels.

52% of survey respondents stated that they were concerned to some extent about external fraud, defined within the survey as the caller pretending to be another person. This is particularly the case with large operations, and supports the need for customer identity verification to be taken very seriously.

Levels of concern about internal employee fraud is fairly low again this year, despite the risks associated with remote working.

41% of respondents from large contact centres were at least somewhat concerned about this.

Figure 12: Concerns about security



THE EMERGENCE OF BIOMETRIC TECHNOLOGIES

Biometric technology uses physiological or behavioural characteristics to verify a person's claimed identity. Physiological biometrics includes fingerprints, iris, or retina recognition, and voice verification. Behavioural biometrics includes signature verification, gait and keystroke dynamics.

Of these, voice is the only biometric that can currently be used over the phone, making it a viable identity verification solution for contact centres. It should be noted that many businesses now allow smartphones with thumbprint- or face-recognition to be used as trusted devices to log into mobile apps.

Voice verification systems use spoken words to generate a 'voiceprint', and each call can be compared with a previously enrolled voiceprint to verify a caller's identity. Systems generate a voiceprint by using spoken words to calculate vocal measurements of a caller's vocal tract, thereby creating a unique digital representation of an individual's voice, as well as other physical and behavioural factors, including pronunciation, emphasis, accent, speech rate and other audio artifacts. These systems are not affected by factors such as the caller having a cold, using different types of phones, or aging.

A significant advantage of voice biometric verification is that both enrolment and verification can be done unobtrusively – in the background during the natural course of customers' conversations with an agent – using text-independent and language-independent technology. Real-time authentication significantly reduces average handle time and improves the customer experience by utilizing voice biometrics to authenticate customers within the course of the conversation.

Voice biometrics, while an excellent authentication tool, is not in itself enough to deter fraud attacks. Researchers found that a fraudster armed with just a few minutes of recordings of a person's voice could build a model of the victim's speech patterns and successfully pass voice biometric security. As voice is a characteristic unique to each person, such attacks essentially give the attacker the keys to that person's privacy, and as AI tools develop rapidly, the sophistication of fraudulent voice attacks is sure in increase.

Obviously, voice biometric solutions are improving all of the time – AI can be used for defence as well as attack – but so are the weapons that fraudsters are using, and it would be risky to place all of the responsibility for fraud detection onto a single technology such as biometrics.

Security solution providers have added considerably to their portfolio, and while voice biometrics is still a key part of this, they may also offer CLI validation, device validation, one-time passwords, risk-based authentication and real-time fraud detection.

It is also possible to use contextual analysis, such as the caller's geolocation (as detailed from their mobile phone's GPS coordinates, or their CLI) to add another layer of confidence in the security process, automatically notifying the agent whether the caller has been identified successfully, and guiding the agent to ask alternative questions if further verification is required.

Contact centres wishing to deter fraud should consider combining voice biometrics with phoneprinting technology for a multi-layered solution. Phoneprinting relies on background audio, source, and channel features that are more difficult for an adversary to manipulate than voice. Phoneprinting can detect CLI spoofing, voice distortion, and social engineering-based fraud attempts, which voice biometrics by itself would have missed.

Voice verification can also be used to protect the enterprise against repudiation (where the customer says at a later date that they did not do it) as it can verify the physical presence of an individual at the other end of a phone line. Interestingly, this capability is already used by various US law enforcement agencies to check that released offenders are where they should be.

For procedures such as internet password resetting, the higher level of security achieved with voice verification can enable businesses to offer real-time password resets or reminders. This benefits both customer and business and can reduce up to 70% of helpdesk calls.

It is interesting to note that some US states have privacy laws that require express consent and special handling capabilities to protect consumer privacy, which impact upon the cost and effectiveness of collecting, using and storing voiceprints, meaning that some businesses may not be able to use voice biometrics.

Potential cost savings are significant, especially for larger operations, and the customer also gains through a better experience, longer opening hours and greater identity protection.

While only 1% of survey respondents currently use voice biometrics, 13% are trialling it or have a trial planned in the future. Only 21% say that they will definitely not use voice biometrics.

INHIBITORS TO VOICE BIOMETRICS

One of the main inhibitors to voice biometrics is the perceived expense of the solution, with around half of respondents stating that this was a very important reason not to implement it. This was particularly the case for both small and medium operations.

Another issue with voice biometrics is the question of low customer adoption. Only around 60% of customers will call into a contact centre in a given year and of those, a significant group will be resistant to having a voiceprint created due to privacy concerns or will experience poor call quality. This means that voice biometrics may be applicable to 50% or less of customers and that a majority of customers will never be enrolled, leaving them vulnerable to fraud attacks.

It is still possible to give some protection to these non-calling customers' accounts, as criminals often try to mine the IVR in order to gather and using the stolen information to socially engineer agents and take over accounts across the enterprise.

Fraudsters identify and take over legitimate accounts by using automated bots in the IVR to test large numbers of stolen credentials and credit card numbers. Some solutions monitor inbound calls for IVR bot activity, suspicious phone numbers and accounts that have had multiple attempts to be accessed, flagging these accounts as requiring particular attention when a caller then tries to access that account on a call. As every caller exhibits unique behaviour patterns when engaging with a call centre, by classifying the cadence of each keypress, a pattern can be established for every genuine caller.

In terms of usability, some issues have been reported with callers using speakerphone or cordless phones, leading to false negative responses, which means the caller then has to go through a very long and stringent manual ID&V process, taking far more time than is usually the case for agent-led identification.

Although the reliability of the technology was a concern, almost half of respondents admitted that they did not know enough about this to even form on opinion. Worries about managing the solution were also present in smaller operations and there are concerns over customer sentiment for contact centres in all size bands.

As might be expected, respondents in small contact centres are far more concerned that call volumes are too low to make the solution worthwhile: for large operations, it is not the case that the commercial benefit isn't there, but concerns over the use of the solution and its cost are far more important.

CALL SIGNALLING ANALYSIS

Solutions that focus on identifying potential fraudulent callers don't rely solely on matching the voiceprint, which is not an infallible method of authentication especially with the capabilities that AI now has, and businesses may wish to consider using biometrics in association with other security measures such as call signalling analysis, which is focused more on identifying and preventing fraud than on simply authenticating genuine customers.

Call signalling analysis is the process by which the metadata surrounding a call can be looked at, for the purpose of identifying potentially fraudulent and suspicious calls that can then be handled differently by the business.

The process collects information about the call being made, such as location, the type of phone being used (VoIP is far more likely to be used in fraudulent calls), caller ID, the phone number's history and the chances it has been 'spoofed', levels of voice distortion, etc. These factors can be scored, and after assessing the likelihood of the call being fraudulent will then impact upon the security processes and questions that the agent is required to ask the caller, speeding up the process for genuine callers, and focusing the tightest levels of security on potentially fraudulent calls.

For solution providers who have access to their country's PSTN, data such as network level caller ID may be collected from the call at carrier-level compared to the presentation caller ID: a mismatch may indicate that the call is suspicious.

Call metadata may include many dozens of individual pieces of data, which are put together to form a phone print:

- presentation caller ID
- network caller ID
- geographic ID
- the type of device being used
- codec artefacts
- packet loss
- clarity.

The solution checks to see if this pattern of metadata has been seen before, and if so which account it is linked to. If it is anything other than the account of the customer that the caller claims to be, it is flagged as a potentially fraudulent interaction. If the phone print is not recognized, it will be stored and used in future interactions.

The caller's voiceprint and phoneprint can be matched against a database of fraudsters: while this "bad voice" method of matching recorded voice against the database of known fraudsters can be effective, this is usually done as a retrospective batch process so does not work in real-time, although it can be useful to check that requests for new credit cards are authentic before the card itself is sent out.

Some fraudsters call in multiple times to find an agent that they can socially engineer. Identifying and logging multiple calls from the same caller/device can identify this and allow agents to be aware and/or block calls.

Call signalling analysis can work in conjunction with voice biometrics to alleviate some of the weaknesses of the latter. By identifying suspicious phone prints, the caller can be identified as being suspicious and handled accordingly:

- IVR spear-phishing: fraudsters use the IVR to validate customer information such as recent transactions, which is then used to conduct fraud through other channels
- Fraudulent voice biometric registration: if the customer has not already registered their voiceprint, a fraudster can do so if they have sufficient static identification information about the customer (e.g. password, date of birth, address, etc.)
- 'Catch and release' fraud: fraudsters contact the bank to clear blocked fraudulent payments that they themselves have made, if they are able to successfully authenticate themselves as the customer
- SIM swap and fraudulent ports: fraudsters gain control of genuine customers' phone numbers in order to bypass two factor authentication (e.g. caller ID and another factor)
- Call signalling analysis can also reduce unnecessary customer callbacks caused by a lack of confidence about the caller ID: in cases where voice biometrics has been uncertain, metadata around the call can be used to provide a more definite answer either way.

Some solutions allow fraudulent phone numbers to be gathered and shared with other businesses, red-flagging likely fraudsters. Data from various sources can be added, such as consumer complaint sites, spam calls databases, detecting attack patterns and improving suspicious call identification. Such information can also feed into fraud detection platforms which gather data from many sources often do not include flags from the telephony channel causing a limited detection of cross-channel attacks.

Some solution providers offer a fraud investigation service for SMEs who may not have the resources to implement the full biometrics or call signalling analysis solution, taking audio recordings to identify fraudulent activity on an as-needed basis.

Sophisticated fraud detection solutions use AI and machine learning to identify fraudulent transactions and also to analyse cases where legitimate users fail the authentication attempt (e.g. due to noise variations, the ageing process, a change in devices, etc.) to amend and optimize the voiceprint so that they are more likely to be identified correctly in future.

To summarise, the strongest security will be present where there is multi-factor authentication around voice biometrics, device authentication, shared information about known fraudsters and customer behaviour such as keypress analysis and call patterns.

SUMMARY

As the contact centre environment evolves, so too must its approach to payment security and PCI DSS compliance.

This report has shown that fraud prevention is no longer just about technology or ticking a compliance box: it requires a coordinated strategy across people, processes, and platforms.

Contact centres face a growing threat landscape, with criminals becoming more sophisticated and regulations more demanding. PCI DSS 4.0 reflects this shift, emphasising continuous, outcome-based compliance rather than rigid checklists.

Businesses must now think beyond one-off assessments and embed security throughout their operations.

The findings highlight that:

- Reducing PCI scope through techniques like pause & resume, tokenisation, DTMF suppression and third-party cloud solutions can significantly cut costs and risk.
- Manual identity verification is both time-consuming and vulnerable: voice biometrics and call signalling offer scalable, intelligent alternatives.
- Compliance is ultimately a shared responsibility: your internal team, external providers and technology stack must all align.
- The cost of inaction is high: reputational damage, regulatory penalties and customer churn are very real risks.

Contact centres must act now to modernise their compliance strategies, balance fraud prevention with user experience and adopt technologies that protect both their customers and their brand.

Security is not an annual task. It's a daily discipline.

ABOUT CONTACTBABEL

ContactBabel is the contact centre industry expert. If you have a question about how the industry works, or where it's heading, the chances are we have the answer.

We help contact centres compare themselves to their closest competitors so they can understand what they are doing well, what needs to improve and how they can do this.

The coverage provided by our massive and ongoing primary research projects is matched by our experience analysing the contact centre industry. We understand how technology, people and process best fit together and how they will work collectively in the future.

e: info@contactbabel.com | w: www.contactbabel.com | t: +44 (0)1434 682244

Free research reports available from www.contactbabel.com (UK and US versions):

- **The Inner Circle Guide to:**
  - Agent Engagement & Empowerment
  - Agentic AI
  - AI-Enabled Agent Assistance
  - Chatbots & Voicebots
  - Cloud-based Contact Centre Solutions
  - Customer Engagement & Personalisation
  - Customer Interaction Analytics
  - First-Contact Resolution
  - Fraud Reduction & PCI Compliance
  - Omnichannel Workforce Optimisation
  - Remote & Hybrid Working Contact Centre Solutions
  - Self-Service
  - Voice of the Customer

- **The UK Contact Centre Decision-Makers' Guide**
- **The UK Customer Experience Decision-Makers' Guide**
- **Exceeding UK Customer Expectations**
- **UK Contact Centre Verticals**: Communications; Finance; Insurance; Outsourcing; Retail & Distribution; Travel; Utilities
- **AI in UK Contact Centre Verticals**: Finance; Insurance; Retail & Distribution; Utilities

- **The US Contact Center Decision-Makers' Guide**
- **The US Customer Experience Decision-Makers' Guide**
- **Exceeding US Customer Expectations**
- **US Contact Center Verticals**: Finance; Insurance; Outsourcing; Public Sector; Retail & Distribution
- **AI in US Contact Center Verticals**: Finance; Insurance; Retail & Distribution

- **The AI Series**: how can AI can help contact centres' operational and commercial issues? Research reports: First-Contact Resolution; Sales Growth; Workforce Engagement; Business Insights: Customer Insights; Agent Productivity; Digital Customer Contact; Contact Centre Cost Reduction; Customer Satisfaction.