CONTACTBABEL

The UK Contact Centre Decision-Makers' Guide 2023

(20th edition)

The PCI Compliance & Card Fraud Reduction chapter

Sponsored by

ENCODED

secure automated payments

From “The 2023 UK Contact Centre Decision-Makers’ Guide (20th edition)”

Unravel payment *Complexity* with Encoded

Encoded is an independent payment services and gateway provider of secure solutions for all payment channels, including contact centres.

Our portfolio of solutions includes:

- Payment Gateway Services
- E-Commerce Solutions
- IVR Payments
- Agent Assist Payments with Fraud Prevention
- PayByLink
- Alternative Payment Methods
- Payment Orchestration

To find out more visit **encoded.co.uk**

Many of the world's leading brands trust Encoded to secure their payments

Shell ENERGY · LUSH FRESH HANDMADE COSMETICS · THE WINE SOCIETY 1874 · Mercedes-Benz · SAMSUNG · BMW · SEVERN TRENT WATER · TOYOTA

ENCODED
secure automated payments

ENCODED
secure automated payments

Encoded is a well-established UK Payment Service Provider that understands that customers like to pay in different ways, whether online, via self-service options or speaking to a real person. Encoded's payment solutions are designed to work with each other and enable customers to pay by their preferred payment process, in an easy and secure way.

Encoded's payment solutions help organisations to remain PCI DSS compliant and protect customer data while offering an excellent customer experience (CX). Customers include – Samsung, Mercedes-Benz, BMW, Toyota, The Wine Society, LUSH and Shell Energy

Take a closer look at Encoded's secure automated payment solutions

Encoded's card payment solutions are designed to meet your specific requirements while reducing operational costs and improving CX. Whether you choose a fully automated Interactive Voice Response (IVR) solution, an agent assisted process, mobile or online platform Encoded's solutions have been designed to give your customers choice and the confidence that their payments are secure.

Solutions include:

- Payment Gateway Services
- E-Commerce Payments
- IVR Payments
- Agent Assisted Payments with
- Fraud Prevention Platform
- PayByLink

Contact:

Robert Crutchington

t: + 44 (0)1293 229 700

e: sales@encoded.co.uk

w: https://encoded.co.uk

a: Encoded Ltd, Spectrum House, Beehive Ring Road, London Gatwick Airport, West Sussex, RH6 0LG, UK

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 £730.4m million in 2021 with payment cards accounting for 40% of total 2021 financial fraud loss during the year.

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.

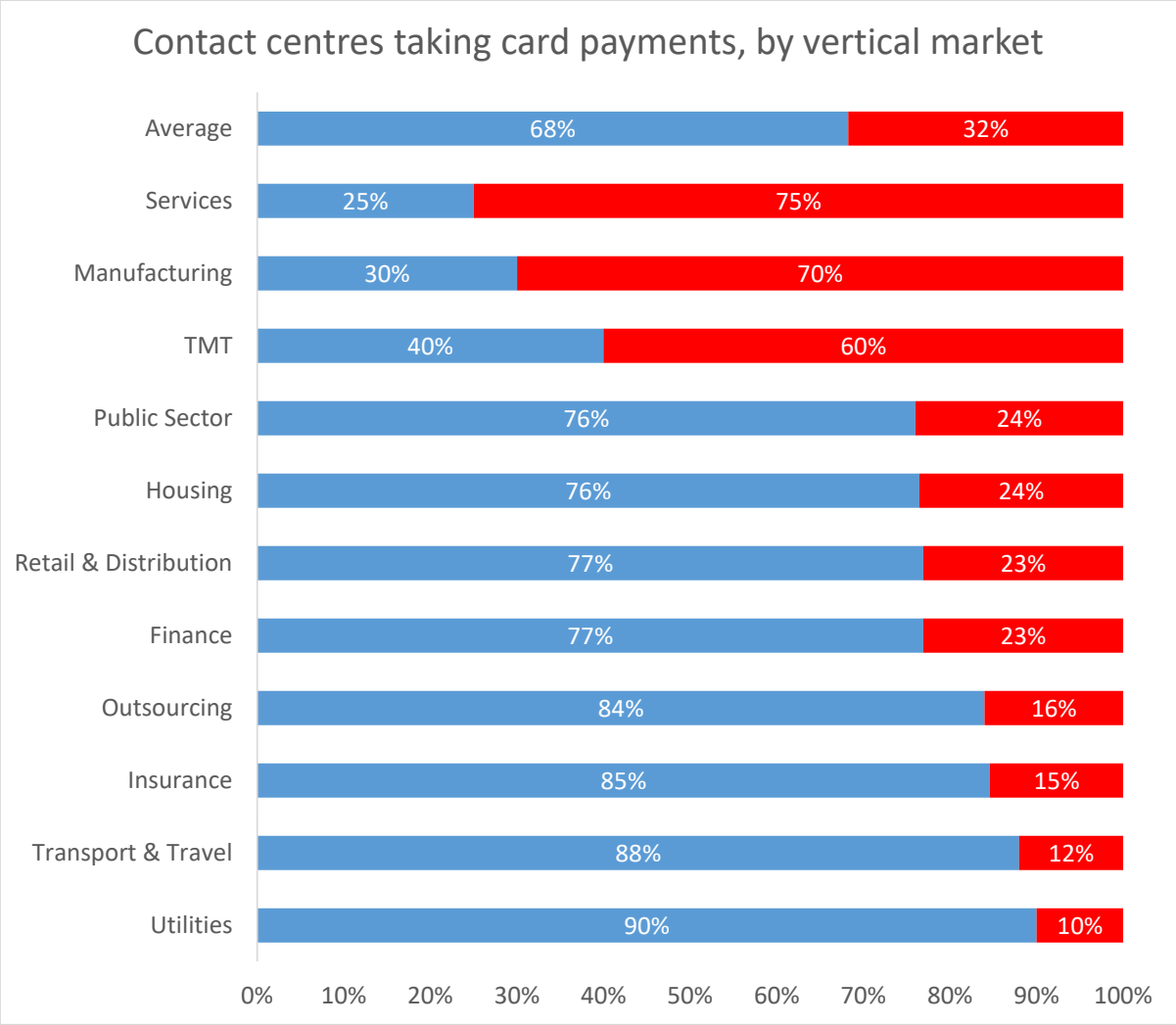
New technology solutions are available that can facilitate and protect mail order, telephone order (MOTO) payments and allow smoother customer journeys. They enable an agent to advise the customer that an additional level of validation is required, rather than simply saying the transaction has been declined. 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/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf

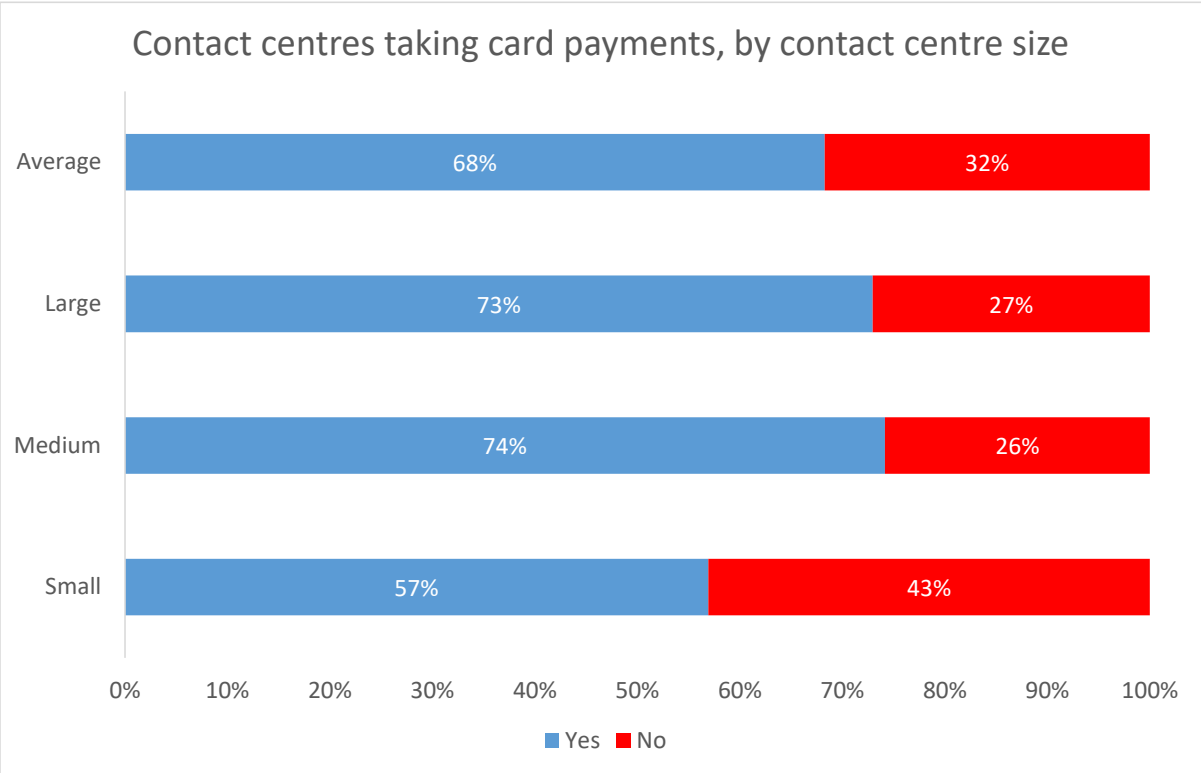
The majority of respondents in all vertical markets take card payments in their contact centres, except for the manufacturing, TMT and services sectors.

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



The usual positive size correlation is present to some extent once again this year. As is shown later in this chapter, the cost of compliance means that some contact centres have stopped taking card payments.

Figure 2: Contact centres taking card payments, by contact centre size



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).

The Council wished to clarify and align their terms, conditions and regulations into a single agreed global framework. The Council maintains, evolves, and promotes the Payment Card Industry Security Standards. It also provides critical tools needed for implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

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, the current standard is PCI DSS 4.0, which supersedes version 3.2.1 which was retired in March 2022. The new standard states that PCI contact centre training must be reviewed and updated annually, including how to manage threats such as social engineering and phishing. It also must include training on end-user technologies that are used in the remote working environment such as video calls.

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. Having said that, in the event of a data breach the card schemes will take a very dim view of any documentation that is not readily available as evidence of meeting the contractual requirements of official PCI SSC, card scheme or acquirer documentation that has been signed fraudulently or without due care.

Compliance with PCI DSS should also be seen in the wider context of a far-reaching zero-trust 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 PCI compliance isn't a once-a-year box-ticking exercise, but should be entwined in the security DNA of an organisation. 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.

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

QSAS AND SELF-ASSESSMENT QUESTIONNAIRES (SAQS)

SAQ A is relevant to card-not-present merchants (including contact centres) who have outsourced all cardholder data functions to a compliant third-party, and who do not process, transmit or store any card data, even if encrypted, in any circumstances. Completion of SAQ A is therefore relatively easy and quick and on the face of it, this seems to be the obvious method for contact centres to consider, with many QSAs recommending this.

For Level 1, 2 and some 3 merchants, SAQs have become channel-related (e.g. a organisation may complete an SAQ for chip-and-pin payments, and another for phone or website payments), and PCI strategies are becoming increasingly built up by channel, reflecting the specific risks and controls that need to be put in place.

If using IVR, businesses should make sure that they do not discriminate against those customers who are unable to complete card payments via touchtone, and who need to read out card payment details. Examples include blind people, a proportion of elderly people uncertain with DTMF touchtone, and those customers who are perhaps driving at the time of the call or cannot use their hands for other reasons. Forcing customers to type card details into a keypad may also provide a sub-optimal experience in the case of smartphones, where the phone is taken away from the ear, the touchpad activated, and the required data typed in on multiple occasions (i.e. going through each stage for the long card number, expiry and CVC), or else use the speakerphone, which is not always appropriate. If a frustrated or confused customer decides just to read out the card details and let the contact centre deal with it, the call recording system will pick these up and immediately put the operation back in scope and become non-compliant.

Even in non-cardholder data environments (e.g. those completing SAQ A), there are likely to be some exceptions where card data is introduced into the environment unintentionally. Businesses should agree with the acquirer controls to be put into place to cover exceptions, and implement people controls, make sure any exceptional card data is handled on a terminal that is not connected to the main network or stored electronically, and provide a demonstration and documentation if required.

If businesses store any electronic cardholder data, including any legacy data, SAQ D will apply, and businesses should review whether there is the need to maintain electronic cardholder data storage. SAQ D is the most complex questionnaire, and if cardholder data storage can be avoided, compliance efforts will be eased significantly by completing a different SAQ.

Each organisation should carefully assess the level of risk, the time and effort taken to complete the relevant SAQ(s), the cost of technology and the effect on customer experience. It should be noted that SAQ D for merchants may involve 12 requirements and well over 300 controls, rather than the 5 requirements and 31 controls involved in SAQ A, which is used in cases where there is no cardholder data environment within the business.

Merchants looking for a service provider should investigate the limit of the scope that any self-assessment takes, for example a cloud-based solution provider only applying it to the segments of their platform that handle sensitive data. Merchants may prefer a holistic perspective of security, and should also ask how the service provider tracks its assets (for example software versions, servers, operating and transport systems), in order to identify risk and react more quickly.

Proving compliance is also about understanding which parts of the business fall into the scope of the PCI compliance audit. It is important that whoever runs the PCI compliance programme, whether internal or external, is experienced in interpreting it fully. QSAs should look at intent and risk: what was the PCI requirement trying to achieve, and what risk was it trying to minimise?

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

Requirement 3: Protect stored cardholder data

This requirement is about reducing the impact of any data breach or fraud, by minimizing the holding of any unnecessary data as well as reducing the value of any stored payment card information. Data must only be stored if necessary, and if stored must be strongly encrypted, and only kept for the period where it is actually needed, with a formal disposal procedure. Businesses should revisit the necessity of data storage on an ongoing basis, and it should be remembered that the storage of sensitive authentication data (SAD) such as card verification codes is prohibited even if encrypted, and must be permanently deleted immediately after authorisation. The requirements of other regulations (which may mandate keeping recordings for a long period of time) may need to be balanced against PCI DSS guidelines, with possible compromises occurring such as archiving encrypted call recordings offsite in a secure facility, with access to them only in the case of fraud investigation or when proving industry-specific regulatory compliance.

PCI DSS requirements also indicate that the full card number (PAN) should only be available on a need-to-know basis, and should otherwise be hidden, with 1234-56XX-XXXX-7890 considered the minimum masking format. For businesses which choose for agents to type in card details, post-call masking and role-based access to the full PAN should be considered, along with strong cryptography when stored.

For contact centres taking payments in their own environment, the most obvious place where data is stored is in recordings, and the use of RAM scrapers should be guarded against (a form of malware that takes data from volatile memory as it as being processed and before it is encrypted).

Organisations have to determine all of the locations which credit card data could potentially be stored, even if it is not part of the formal card handling process. For example, there is nothing to stop the customer sending their credit card details, including the card verification code, by email or web chat. However, if it were to happen, then a formal and documented policy would be required to evidence that the card data had been either removed or securely deleted: if the email or chat interaction is found to be stored, then a risk exists, and the operation is not PCI DSS compliant. There is an increasing use of data loss prevention solutions as a way to track data that has somehow moved out of the original environment, and businesses need to have a good inventory not just of the equipment and infrastructure, but also of their logical environment as well.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

In the event of a security breach, it is important to make sure that credit card data (such as the PAN, or 'long card number') is not readable, through the use of strong cryptography not only at its stored location but also as it is being passed across the network. The network is only as strong as its weakest link, and badly configured wireless networks, with out-of-date security and weak passwords are a particular concern. 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. 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.

Requirement 7: Restrict access to cardholder data by business need to know

Identify roles which require access to specific card data, limit access privileges and restrict access to information such as the full PAN only where needed in specific instances. 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. Regularly review stored data, and keep only that which is necessary for business or regulatory purposes. For example, hotels need to keep customers' credit card details from the reservation point until checkout: there is no hard and fast rule.

Requirement 9: Restrict physical access to cardholder data

Restrict physical access to environments where card data is present only to legitimate employees through access control. Discourage risk by encouraging a clean desk policy, and restricting the use of smartphones and cameras. Use secure data centres and limit physical access to servers storing payment card information.

Requirement 12: Maintain a policy that addresses information security for all personnel

This requirement is mainly about managing the security of payment card data through having an incident response plan that deals with card data at risk, and also deals with third-party solution providers – TPSPs – as requirement 12.8 states: Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

Requirement 12.8 requires the merchant to have policies & procedures in place to manage their service providers, in addition to

- Maintaining a list of service providers
- Having a written agreement where the service provider acknowledges responsibility for card data security
- Having a documented engagement process in place "including proper due diligence"
- Having a program to monitor compliance status at least once every 12 months
- Maintaining information on which Requirements each provider is responsible for and which the merchant is responsible for (Responsibilities Matrix)

NB: In the context of contact centres, Requirement 12.8 will not apply to 'carriers' delivering voice traffic 'point to point'.

Requirement 12.6 also states that all employees should be made aware, in writing and through daily exposure to information security guidelines, of what their responsibilities are in terms of handling data. The regular and ongoing minimisation of potential security risks is perhaps even more important for homeworking agents, who are less likely to be in a rigidly maintained environment, and whose vigilance and adherence to security guidelines may therefore be less rigorous.

Compensating controls

Businesses that are unable to fully comply with PCI DSS objectives, for technical or business process reasons perhaps, may consider implementing 'compensating controls', which act as workarounds to achieve roughly the same aim as the PCI control in situations whereby the end result could not otherwise be achieved. These are not meant as an alternative to the control objectives, i.e. to be used in cases where the business simply does not want to meet the requirement and associated controls in full, but are supposed to act as a last resort allowing the business to achieve the spirit of the control, if not actually the very letter. Guidelines for valid compensating controls indicate that it must meet the intent of the original requirement, and provide a similar level of defence, go at least as far as the original requirement and not negatively impact upon other PCI DSS requirements.

VALIDATING COMPLIANCE

Merchant compliance validation involves the evaluation and confirmation that the security controls and procedures have been properly implemented as per the policies recommended by PCI DSS.

For merchants (organisations accepting card payments), there are four levels:

- Level 1 – Over 6 million transactions annually
- Level 2 – Between 1 and 6 million transactions annually
- Level 3 – Less than 1 million transactions annually and more than 20,000 ecommerce transactions
- Level 4 – Less than 1 million transactions annually and less than 20,000 ecommerce transactions

However, each of the card issuers has their own specific criteria:

- Visa
- Mastercard
- Discover
- American Express
- JCB

Depending on the merchant level (i.e. how many card payments are taken), businesses may either self-certify PCI compliance or use a **Qualified Security Assessor** (QSA) who is accredited by the PCI SSC. Only Level 1 merchants with over 6 million VISA transactions per year or any other merchant at the request of their acquirer or scheme, who are a 'Compromised Entity' (having experienced attacks before) must have an annual on-site QSA audit rather than one of the **Self-Assessment Questionnaires** (SAQs). They are required to have an Annual Report on Compliance ("ROC") delivered by the QSA - commonly known as a Level 1 onsite assessment – or by an internal auditor if signed by a senior officer of the company. They must also have a quarterly network scan by an Approved Scan Vendor (ASV), and complete an Attestation of Compliance Form. NB: Level 1 TPSPs with more than 300,000 Visa transactions annually also have to be externally audited and have an RoC. Level 2, 3 and 4 Merchants may choose to use a QSA, but do not have to, as a Self-Assessment Questionnaire, quarterly network scan and Attestation of Compliance form are the requirements.

An **Internal Security Assessor** (ISA) is an individual who has earned a certificate from the PCI Security Standards Company for their sponsoring organisation, giving them the competence to perform PCI self-assessments for their organisation. ISA certification empowers inward appraisal of their organisation and allows them to propose security solutions and controls.

Dependent on the SAQ that the merchant completes based on PCI SSC SAQ Guidelines, an **Approved Scanning Vendor** (ASV) may be required. ASVs perform penetration tests on the company's network in order to verify that it cannot easily be hacked, through using a set of security services and tools to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor's ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC's List of Approved Scanning Vendors.

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.

A formal **Attestation of Compliance** (AOC) which is usually signed by the Financial Director or Information Security Officer states that all PCI requirements have been met and that any compensation controls have been put in place in case of system or process failure or exception.

Visa provides a partial list of compliant TPSPs on its website: while it is a requirement by Visa that TPSP's complete the listing documentation, a TPSP can be compliant without being on the published Visa list. In 2018, Visa listing became free of charge – prior, it was around £5,000 to register, so a more complete listing should be expected in future. It is worth noting that many corporate procurement teams make a Visa listing a requirement for their TPSPs.

QSA-audited PCI certification offers independently confirmed security, which removes the issue of how an organisation might interpret a PCI requirement in an internal self-assessment. Businesses should see QSAs as expert consultants, rather than as auditors who are just there to tick boxes, agree compliance and then disappear for a year, but should question them as to which SAQs are most appropriate for their business. It should be remembered that any business with a no card data environment (no CDE) approach will not require an external audit.

The vast majority of contact centres do not require a full audit, and self-assessment questionnaires (SAQs) are the norm for many organisations, and many Level 3 and 4 merchants complete an online questionnaire provided by their acquirer, as all main acquirers offer this service in the UK. The PCI DSS 3.0 standard introduced some new types of SAQ, with changes to others, recognising that one size did not fit all. It was acknowledged that it was inappropriate for smaller and less at-risk companies to have to complete the same list of requirements as a large multinational taking many millions of card payments each year. A list and explanation of each SAQ is available from the PCI Security Standards Council here. To make compliance easier, quicker and cheaper, businesses should consider a descoping process by limiting the number of places where card data is present in the logical or physical environment. This allows businesses to choose a less onerous SAQ to report their compliance.

For service providers, things are different: there are two levels, rather than four, and compliance requirements are different. A service provider is a business entity that isn't a payment brand, but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another business. This includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, hosting providers, payment service providers, etc.

A Level 1 Service Provider stores, processes, or transmits more than 300,000 Visa credit card transactions annually. The PCI Requirements need to be validated through:

- An annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA)
- Quarterly network scan by an Approved Scanning Vendor (ASV)
- Penetration Test
- Internal Scan
- Attestation of Compliance (AOC) Form.

Receiving a ROC and validating as a Level 1 Service Provider allows the service provider to be on Visa's Global Registry of Approved Service Providers.

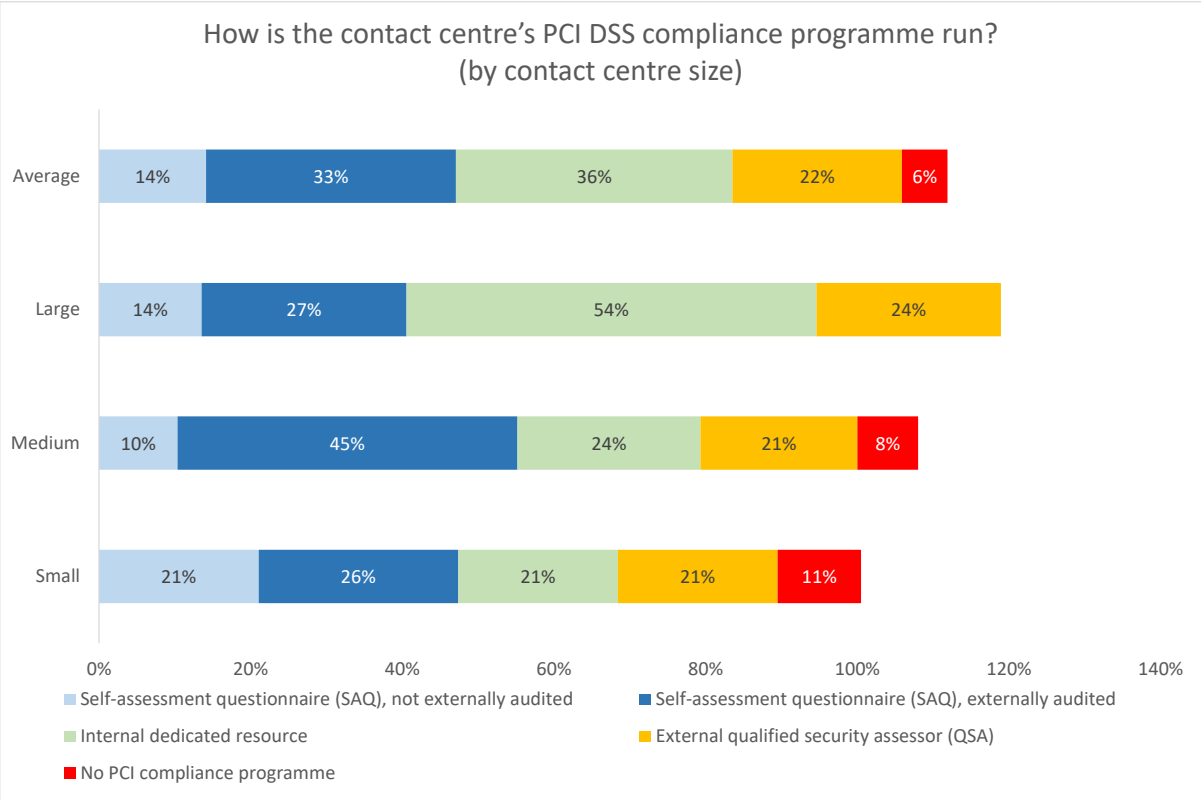
Level 2 Service Providers store, process, or transmit less than 300,000 Visa transactions annually. Their PCI Requirements are validated through:

- Annual Self-Assessment Questionnaire (SAQ) D
- Quarterly network scan by an ASV
- Penetration Test
- Internal Scan
- AOC Form.

Operations of all sizes are fairly equally likely to use self-assessment questionnaires and/or an external Qualified Security Assessor (QSA).

The majority of large operations use dedicated internal resource.

Figure 3: 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 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. The storage element will include 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 November 2018 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 attested 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 4: 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 be seen in the wider context of a far-reaching zero-trust 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.

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 information
- 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.

It is worth noting that with the takeover of Visa Europe by Visa, US security methods are more likely to be brought into Europe. The requirement to supply the CVV code (3 digits on the back of the card) is something which UK merchants and customers are now trained to do, but it is worth noting that many merchants will pay the same processing fees to Visa regardless of whether they supply the CVV code or not, and that small merchants may simply be on a blended tariff where CVV/non-CVV transactions are grouped together.

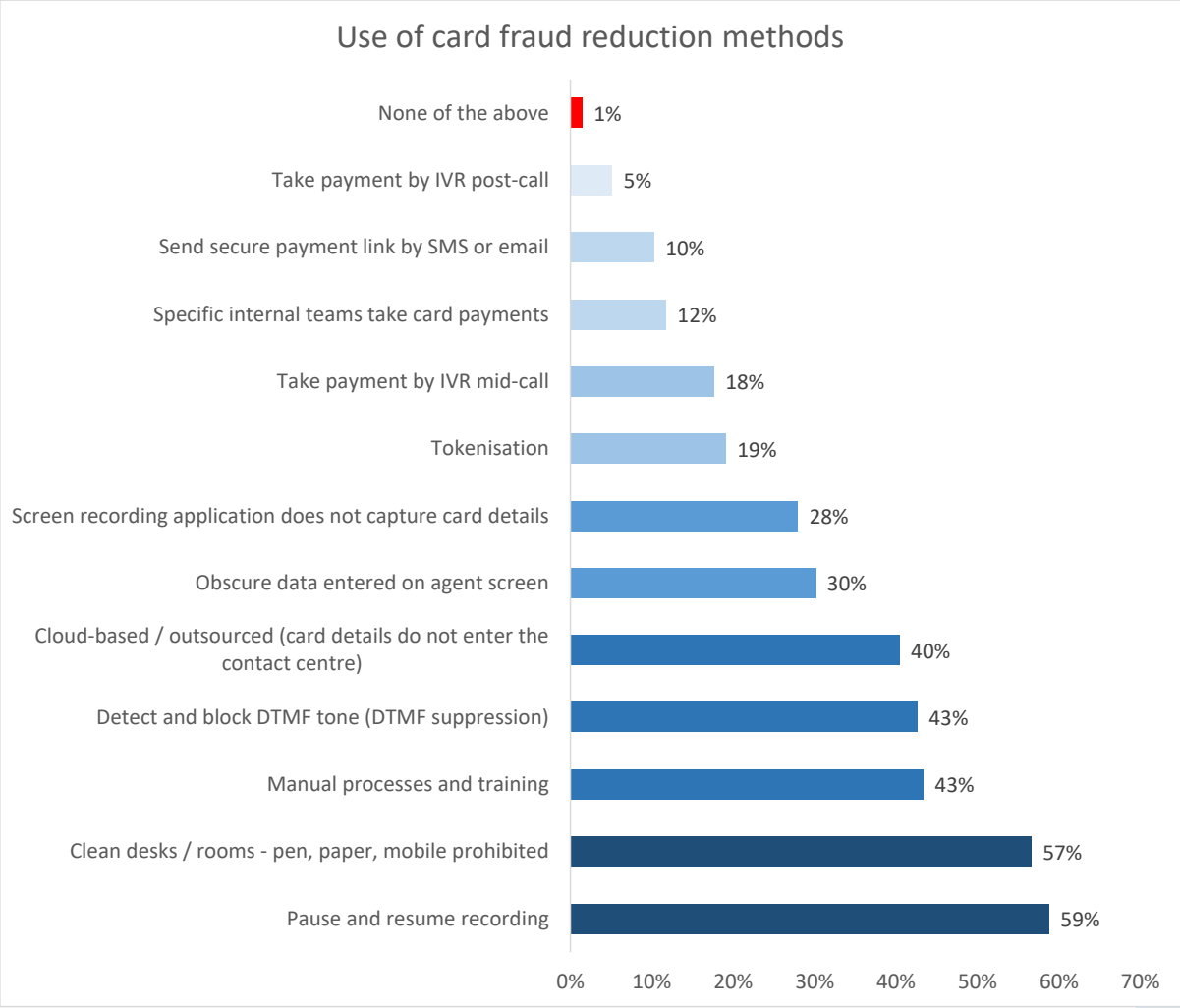
THE USE OF CARD FRAUD REDUCTION METHODS

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 long list of solutions, approaches and business processes that aimed to reduce the risk of card fraud within the contact centre, and were asked to indicate 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 used a mean average of 3.6 card fraud reduction methods.

Pause and resume recording and clean desk/room policies were the main methods used to reduce card fraud, with DTMF suppression, cloud and manual processes / training also being widely seen.

Figure 5: Use of card fraud reduction methods

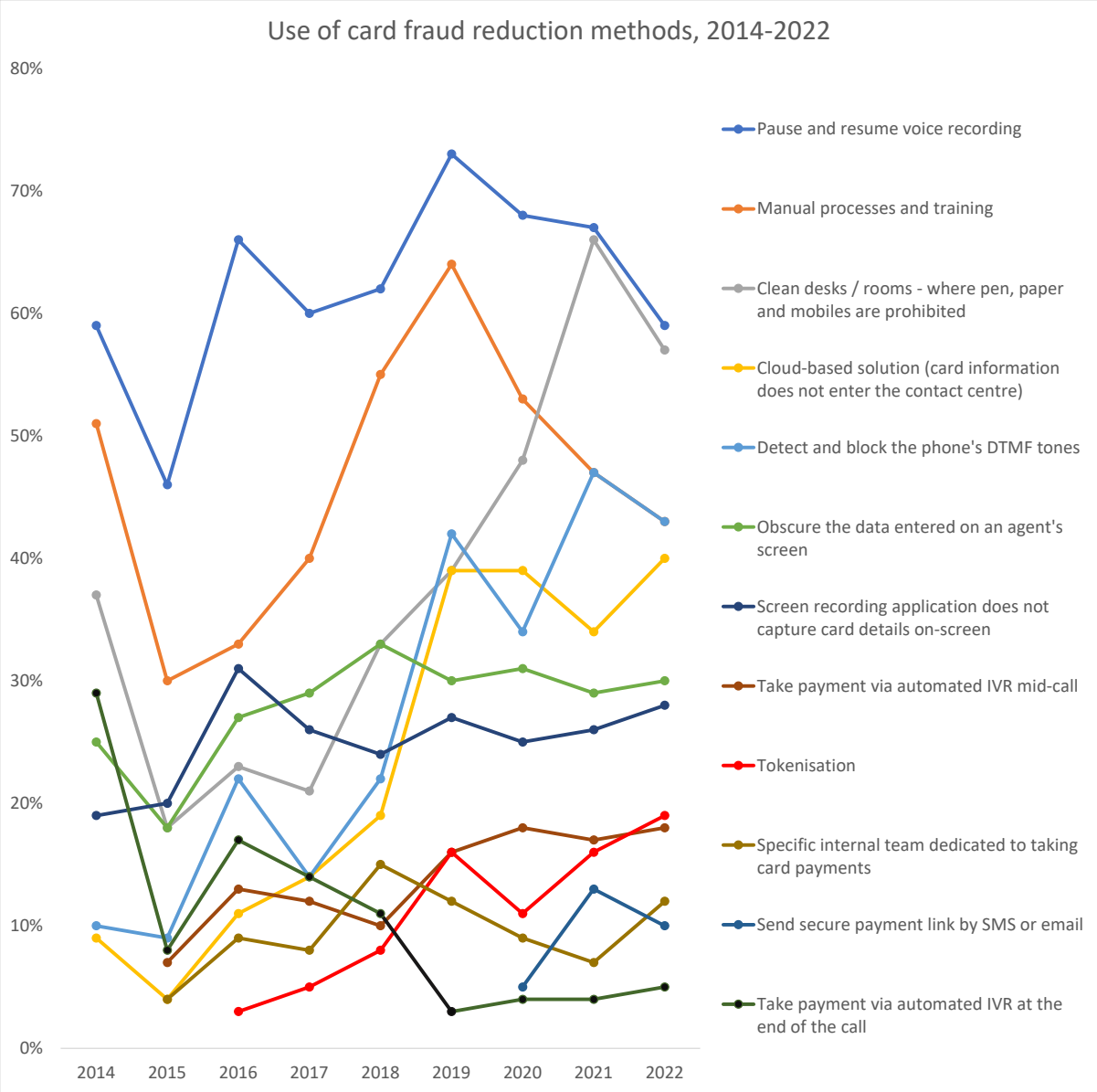


The chart below shows the use of card fraud reduction methods over the past nine years. Care should be taken when considering these data: a rise or fall from one year to the next may not necessarily be indicative of what is happening industry-wide, as many of the respondents taking part in the survey from one year to the next are different. The chart should be viewed as providing a view of card fraud reduction methods relative to each other, and as a longer-term trend.

Pause & resume voice recording and manual processes & training have been consistently the two methods most used, although the use of clean desks/rooms has grown considerably since 2019.

Cloud-based solutions have shown significant growth, as has DTMF suppression. Tokenisation has risen from a low base, and this is the third year that sending secure payment links by SMS or email has been tracked, and is used in 10% of survey respondents' operations.

Figure 6: Use of card fraud reduction methods, 2014-22



The following section discusses some of these more common card fraud reduction methods.

Pause and Resume (59%)

'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 28% of respondents stated that their application does not record card details from the agent's screen. 30% of respondents **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 could only be part of PCI compliance.

Improving Manual Processes and Agent Training (43%)

The third most-widely used method was 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%) and Dedicated Payment Teams (12%)

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 (40%)

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. 34% 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 (5%) and mid-call (18%)

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: 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 (43%)

43% of this year's respondents use DTMF suppression in order to assist with card fraud reduction, which is a large jump on 2020's figure of 34%.

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 is one of the more expensive card fraud reduction methods to implement.

Tokenisation (19%)

The practice of **tokenisation** is used in 19% of this year's respondents' operations (up from 16% last year).

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. For each key press, 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 as necessary, 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 just 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.

Of course, cardholder data is not the only DTMF-provided information coming into the contact centre environment, as other data such as IVR routing options and the entry of account numbers often requires capture of DTMF tones as well. Various configuration options exist within solutions, based upon the specifics of the business in order to circumvent confusion. 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].

Send Secure Payment Link by SMS or Email (10%)

This is the third 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.

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.

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

ENCODED
secure automated payments

Jersey Telecom Chooses Encoded for Payment Orchestration

For more information download the full **case study**

Channel Islands based global telecoms business simplifies processes, meets payment security compliance regulations and improves customer experience with Encoded payment solutions.

All in one integrated solution

JT (Jersey Telecom) chose Encoded as a 'one-stop supplier' for a suite of solutions to ensure compliance with the latest PCI DSS security standards and enable it to merge multiple websites and contact centre operations.

The company implemented Encoded IVR Payments, E-Commerce payments, Payment Gateway Services, Agent Assisted payments and PaybyLink. As a Level 1 PCI DSS compliant payment service provider, Encoded ensures compliance with GDPR, PCI DSS and the latest Payment Services Directive (PSD2). The new solutions work together making it easier for contact centre agents to use seamless 'behind the scenes' payment processes to improve the customer experience.

Customer service transformed

Tim Peach, Finance Operations Manager from JT said, "We found the easy integration between Encoded's solutions gave us more payment choices that benefit our customers. For example, PayByLink offers a great option for a secure and convenient way for customers to pay using their mobile devices, without compromising their data.

"Encoded's suite of solutions also provides us with unified reporting and management from a single portal and can be easily supported by our helpdesk, backed up by the Encoded team."

Gateway services for a seamless customer experience

Encoded Payment Gateway Services bridge the gap between JT's 'back office' systems and its chosen acquirer. This ensures that customer payments are protected and that the company meets with regulatory requirements. Encoded's Gateway integrates with the company's other payment solutions, including E-commerce and IVR, sharing transaction information seamlessly between channels for smooth payment orchestration.

A trusted partner

According to Tim Peach, "One of the key reasons for choosing Encoded was to improve the team's experience of managing large scale migrations from legacy payment systems. With Encoded's in-depth knowledge of data security, PCI DSS compliance and the latest payment regulations, JT had confidence that the integration would be carried out within the project timescales and to budget."

Fast Facts

Successful migration from JT's legacy systems to Encoded payment solutions ensures compliance with latest PCI DSS, GDPR and SCA regulations.

- Encoded payment solutions used to support 40-strong contact centre team
- Integrated Encoded automated payment solutions enable unified customer service across multiple channels
- Encoded Payment Gateway Services bridge the gap between JT's 'back office' systems and its payment acquirer, sharing transaction information seamlessly and securely
- Encoded Agent Assisted Payments allows agents to process payments securely without exposure to customer card details
- Tokenisation ensures protection for stored card data, making regular customer payments easy and secure
- Payment orchestration makes it easier for agents to provide the best customer experience.

About JT

JT is a government-owned full-service global connectivity and business enterprise provider offering the full range of communications services and solutions required to connect people together and deliver excellence in customer experience. For more information please visit: https://international.jtglobal.com/

About Encoded

Encoded's solutions are trusted by many of the world's leading brands including Samsung, Mercedes-Benz, BMW, LUSH and The Wine Society as well as a host of UK utility companies such as Green Star Energy (now Shell Energy) and Severn Trent Water.

Omni-channel solutions include:

- Agent Assisted Payments
- E-Commerce payments
- IVR Payments
- PayByLink - Mobile Payments
- Encoded Gateway Services

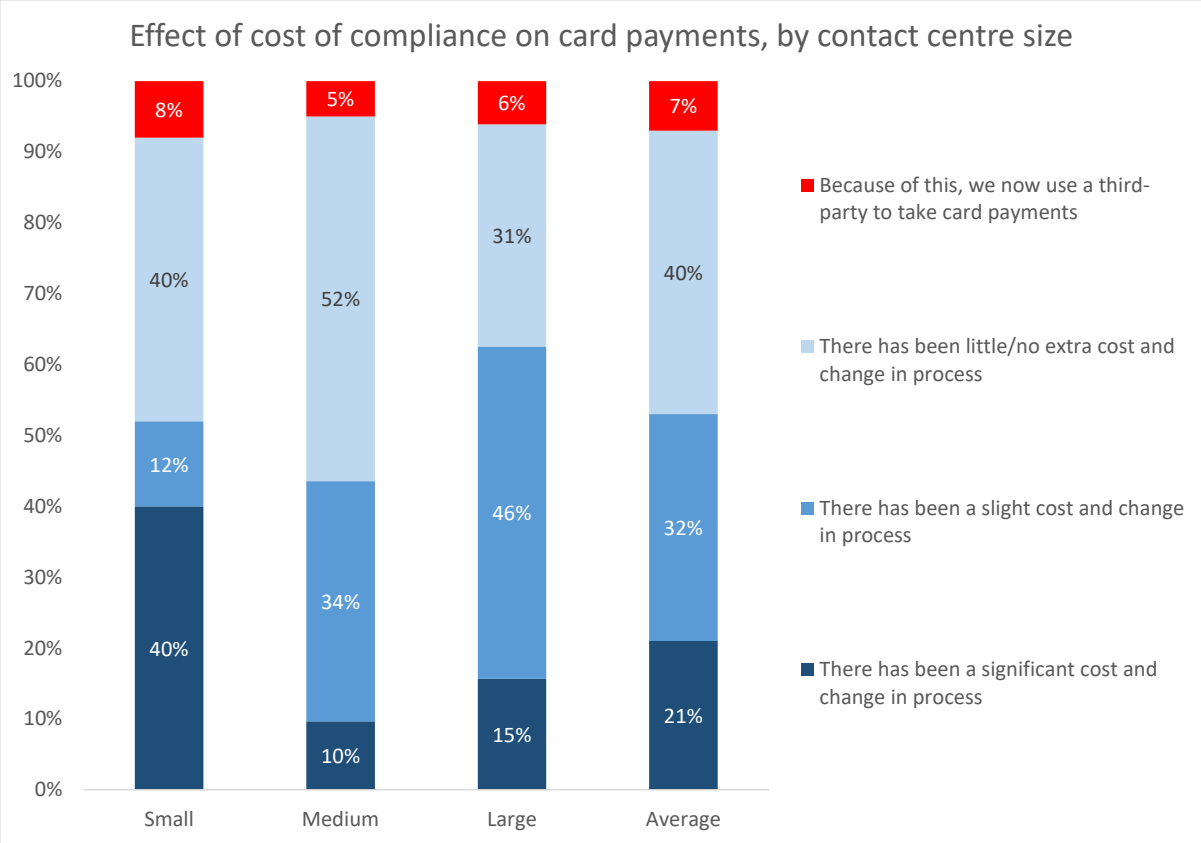
For more information visit **www.encoded.co.uk**

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 21% of respondents stating that they have seen a significant cost associated with compliance, as well as a change in their processes. 40% 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.

Furthermore, 7% of respondents state that they have decided use a third-party to take card payments in order to take the contact centre out of scope.

Figure 7: Effect of cost of compliance on card payments, by contact centre size

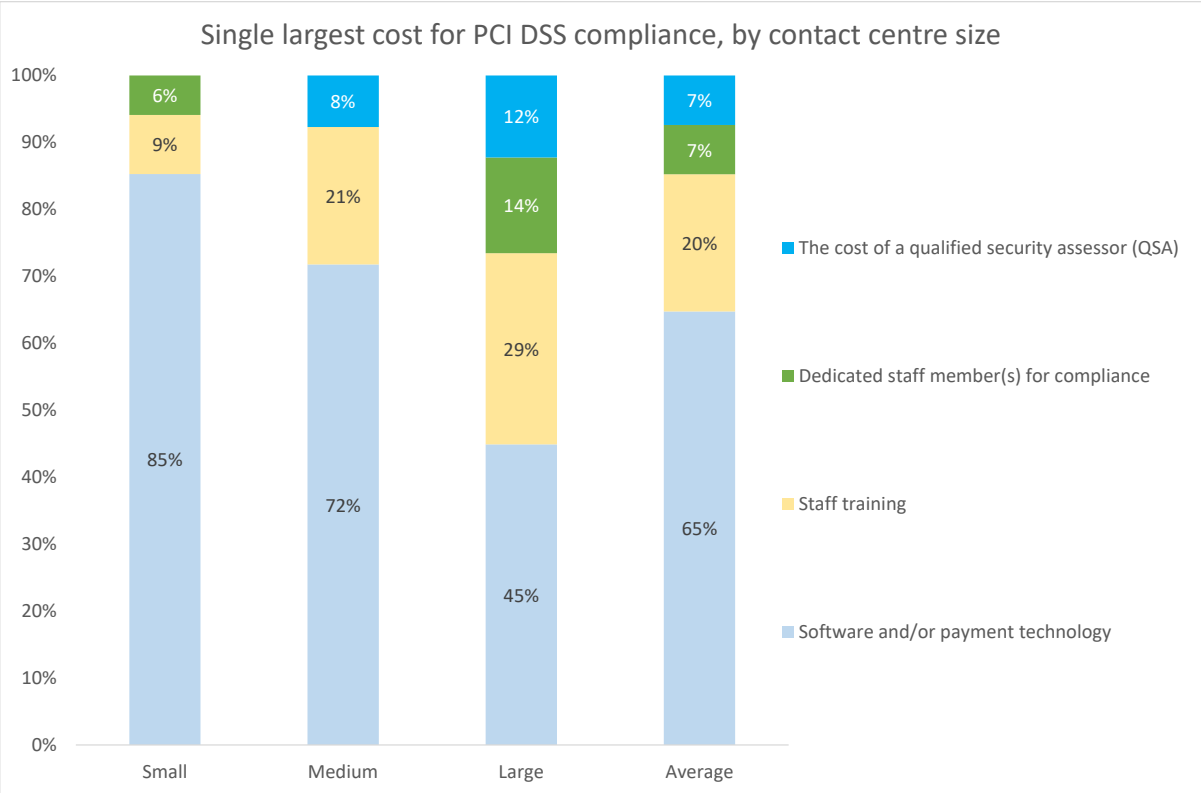


65% of survey respondents state that software and/or payment technology is the single largest cost associated with PCI DSS compliance. This is particularly the case in small and medium-sized operations.

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 29% of cases, with 14% stating that having dedicated compliance staff was the largest cost.

A small minority in large and mid-sized operations stated that the high cost of bringing in external qualified security assessors (QSAs) was the greatest cost borne.

Figure 8: Single largest cost for PCI DSS compliance, by contact centre size

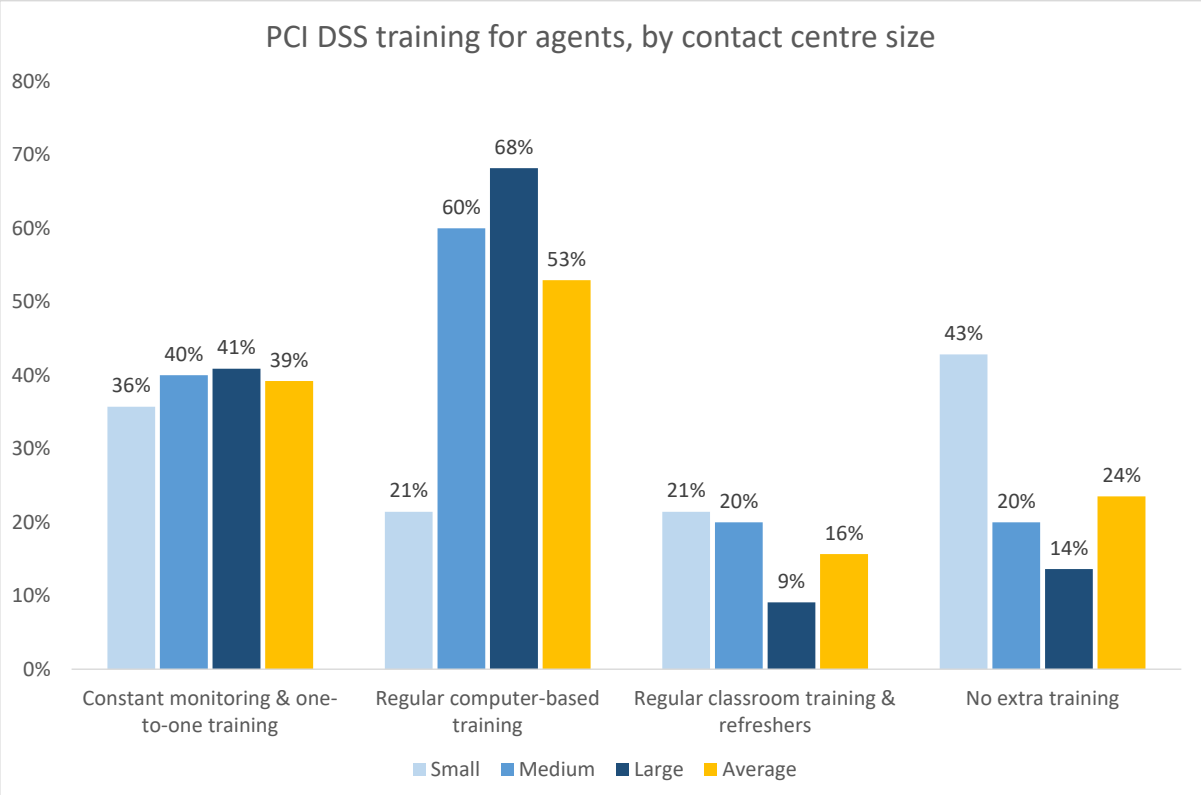


The cost of staff training is reported to be a major drain on resources for large contact centres in particular. Regular computer-based training, used to educate agents about card fraud reduction practices, is likely to be scalable and require less personal support from managers and security specialists,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

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

24% 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 small 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 9: PCI DSS training for agents, by contact centre size

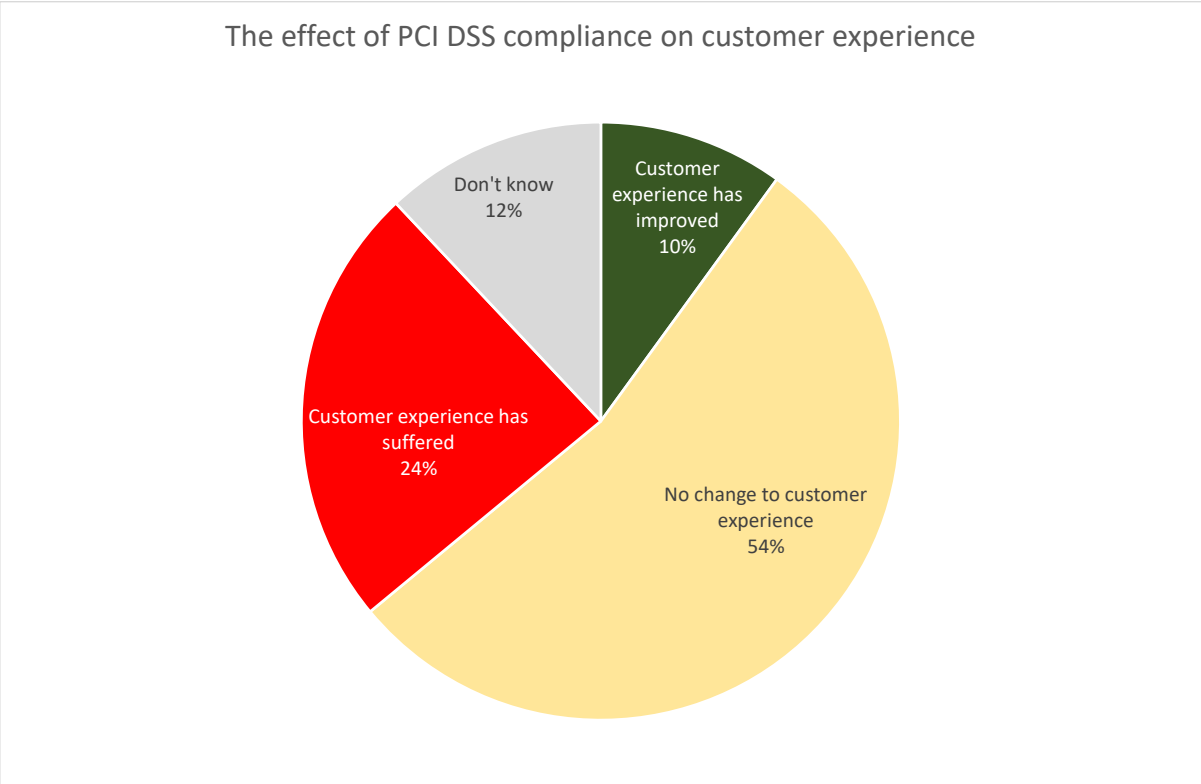


Many PCI DSS compliance and card fraud reduction methods are likely to have an impact upon the customer, in terms of increased effort or inconvenience (e.g. having to type in a card number can be awkward if using a smartphone, as navigation through screens will be required while holding the phone away from the ear; or waiting for a dedicated card-handling agent to become available).

Other methods are less intrusive: pause and resume recording or DTMF tone suppression are unlikely to be noticed from the customer's perspective.

24% of respondents stated that PCI DSS compliance had a negative effect on the customer experience, with only 10% believing that there had been an improvement.

Figure 10: The effect of PCI DSS compliance on customer experience



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 US and UK 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.

If you have a question about the contact centre and CX industry, please get in touch.

Email: info@contactbabel.com / Website: www.contactbabel.com / Telephone: +44 (0)1434 682244

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

- The Inner Circle Guide to Agent Engagement & Empowerment
- The Inner Circle Guide to AI, Chatbots & Machine Learning
- The Inner Circle Guide to AI-Enabled Self-Service
- The Inner Circle Guide to Cloud-based Contact Centre Solutions
- The Inner Circle Guide to Customer Engagement & Personalisation
- The Inner Circle Guide to Customer Interaction Analytics
- The Inner Circle Guide to First-Contact Resolution
- The Inner Circle Guide to Fraud Reduction & PCI Compliance
- The Inner Circle Guide to Omnichannel
- The Inner Circle Guide to Omnichannel Workforce Optimisation
- The Inner Circle Guide to Outbound & Call Blending
- The Inner Circle Guide to Remote & Hybrid Working Contact Centre Solutions
- The Inner Circle Guide to Video & Next-Generation Customer Contact
- The Inner Circle Guide to the Voice of the Customer

- The Australia & New Zealand Contact Centre Decision-Makers' Guide
- The European Contact Centre Decision-Makers' Guide
- The UK Contact Centre Decision-Makers' Guide
- The US Contact Center Decision-Makers' Guide
- The UK Customer Experience Decision-Makers' Guide
- The US Customer Experience Decision-Makers' Guide

- UK Contact Centre Verticals: Communications; Finance; Insurance; Outsourcing; Retail & Distribution; Utilities
- US Contact Center Verticals: Communications; Finance; Healthcare; Insurance; Outsourcing; Retail & Distribution.

To download the full "2023 UK Contact Centre Decision-Makers' Guide" for free, please click here.