CONTACTBABEL

The Inner Circle Guide to Fraud Reduction & PCI Compliance

Sponsored by

ENCODED

secure automated payments

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

ENCODED
secure automated payments

CONTACTBABEL

CONTENTS

TABLE OF FIGURES

Encoded is a UK company founded in 2001 to offer affordable, pay-as-you-go IVR and payment solutions to small and large businesses. Many contact centres now rely on Encoded secure automated payments for their PCI DSS compliance requirements. Today the company's software supports many of the UK's leading brands including Virgin Holidays, Mercedes-Benz FS, BMW FS, Green Star Energy and Anglian Water Business.

All the company's services are designed to fulfil three key objectives:

- Reduce costs by automating card payments
- Increase security around payments and reduce PCI DSS compliance scope
- Improve customer service by maximising resource efficiency.

Solutions include:

- Agent Assisted Card Payments
- IVR Phone Payments
- Mobile App
- Instant Messaging, SMS Customer Engagement
- Pay-by-Link
- Virtual Terminal Payments
- Web Payments

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)

ENCODED
secure automated payments

Looking for a fast, hassle-free method for customers to pay from their mobile devices or email addresses?

Worried about discriminating against customers who will not or cannot use touchtone?

Want to remove card data from your agents and networks for security and PCI DSS compliance?

Agent Assisted

IVR payments

Mobile App

SMS Chat

Web payments

Then it's time to take a closer look at **Pay-by-link** from Encoded.

Designed for speed and security Pay-by-link is a new safe, hassle-free method of sending a one-time short code link to a customer's phone or email address which then triggers a simple pre-populated and pre-authorised payment form.

Available as a standalone service or to compliment other payment channels Pay-by-link is a convenient and secure way for customers to submit their card details and pay in an instant.

To find out more information on products and services please call 01293 229 700
email sales@encoded.co.uk or visit encoded.co.uk

All of Encoded's payment services work co-operatively. Sharing stored card details between solutions, enabling card holders to use the service of their choice without having to re-enter card data.

Encoded is a Level 1 PCI DSS Service Provider

PCI Compliant
Level 1 PCI-DSS Service Provider

ABOUT THE INNER CIRCLE GUIDES

"The Inner Circle Guide to Fraud Prevention & PCI Compliance" is one of the Inner Circle series of ContactBabel reports. Other subjects include AI, Chatbots & Machine Learning, Cloud-based Contact Centres, Omnichannel, Self-Service, Outbound & Call Blending, Workforce Optimisation and Customer Interaction Analytics, and can be downloaded free of charge from here.

The Inner Circle Guides are a series of analyst reports investigating key customer contact solutions. The Guides aim to give a detailed and definitive view of the reality of the implementing and using these technologies, and a view on what the future holds.

As well as explaining these solutions to the readers, we have also asked the potential users of these solutions whether they have any questions or comments, and we have selected six of the most popular to ask to the report's sponsor. The answers to these are distributed throughout the report and give interesting insight into real-life issues.

The report is in two parts, the first looking at PCI DSS compliance, and the second considering issues around customer identity verification and authentication.

Statistics within this report refer to the UK industry, unless stated otherwise. There is a version of this report available for download from www.contactbabel.com with equivalent US statistics.

"Small" contact centres are defined in the report as having 50 or fewer agent positions; "Medium" 51-200 agent positions; and "Large" 200+ agent positions.

BECOMING PCI COMPLIANT

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 (April 2019), the current standard is PCI DSS 3.2.1, which was released in May 2018 and supersedes version 3.2 which was retired at the end of 2018.

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 or 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 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.

THE CARD PAYMENT ECOSYSTEM

In order to understand the landscape of payment card processing, there first needs to be a clear understanding of the players within it. The PCI Security Standards Council has detailed definitions of many commonly used terms[1]. Here are some relating to entities within the card payment ecosystem:

- **Acquirers:** Acquirers provide Merchant Accounts and charge for providing that service. Compliance to the PCI DSS is part of the contractual obligations between the Acquirer and the Merchant.. The acquirer receives authorisation requests from merchants via a payment gateway and or payments processor, then passes the request to the card issuer for approval. Payment outcomes are then reported to the merchant via the payments processor and/or gateway, with funds from successful transactions then being deposited by the acquiring bank into the merchant account.

  PCI compliance has to be 'attested to' by the Merchant or Third Party Service Provider signing to say that they comply with the standard. In the event of a data compromise, acquiring banks will pass on the card scheme penalties onto the merchants, as well as being able to increase the cost per transaction or even pass on the card scheme's instructions to withdraw facilities until compliance is certified. It is important to remember however that merchants always bear full responsibility for their own PCI DSS compliance, and also to ensure that their Third Party Service Providers (TPSPs) maintain compliance too.

- **Card brands/schemes:** The schemes or Brands are responsible for the payments ecosystem that they set up. Card Issuers provide cards to people and corporations. Visa Inc., MasterCard, JCB International, American Express and Discover Financial Services banded together in 2006 to form the PCI Security Standards Council (PCI SSC), which is responsible for developing the PCI standard and for supporting organisations' attempts to become compliant. The card brands created the PCI SSC to reduce fraud risk, acting together so that they all have the same regulations and not one of them had a competitive advantage over the other. The card brands have contracts with the acquiring banks, who themselves have contracts with merchants

- **Merchants:** organisations which accept payments made by credit or debit cards

- **Qualified security assessors (QSA):** QSAs are qualified by the PCI SSC to help organisations interpret the PCI standard and become compliant, and the firms that they work for must have a license for each of the territories they work in. Individual QSAs need to be employed by an organisation and annually certified and examined by the PCI SSC against their knowledge against the DSS and against all current guidelines

- **Third-Party Service Providers (TPSPs):** a service provider is a business entity that is not a payment brand, which is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. There are many types of businesses that could fall into the category of "service provider," dependent on the services provided.

[1] https://www.pcisecuritystandards.org/security_standards/glossary.php

From May 2017, the Card schemes only levy penalties in the event of a data breach. Those penalties are based on a number of factors including who found the breach (Merchant or Card scheme), the Merchant's compliance status, and the Merchant's compliance status at the point of breach. Penalties differ per scheme, but are based on a fixed tariff and levied against the amount of card data 'at risk' during the breach.

The card schemes may also decide to remove the merchant's ability to take card payments or charge increased transaction fees. Higher fees are charged by some acquirers for non-compliance – as monthly charges and as transaction charges. Additionally, the damage to brand and trust that a high profile card payment data breach could cause is potentially even more damaging than financial sanctions. As payment card data is personal data, a data breach opens entities up to potential ICO fines as well.

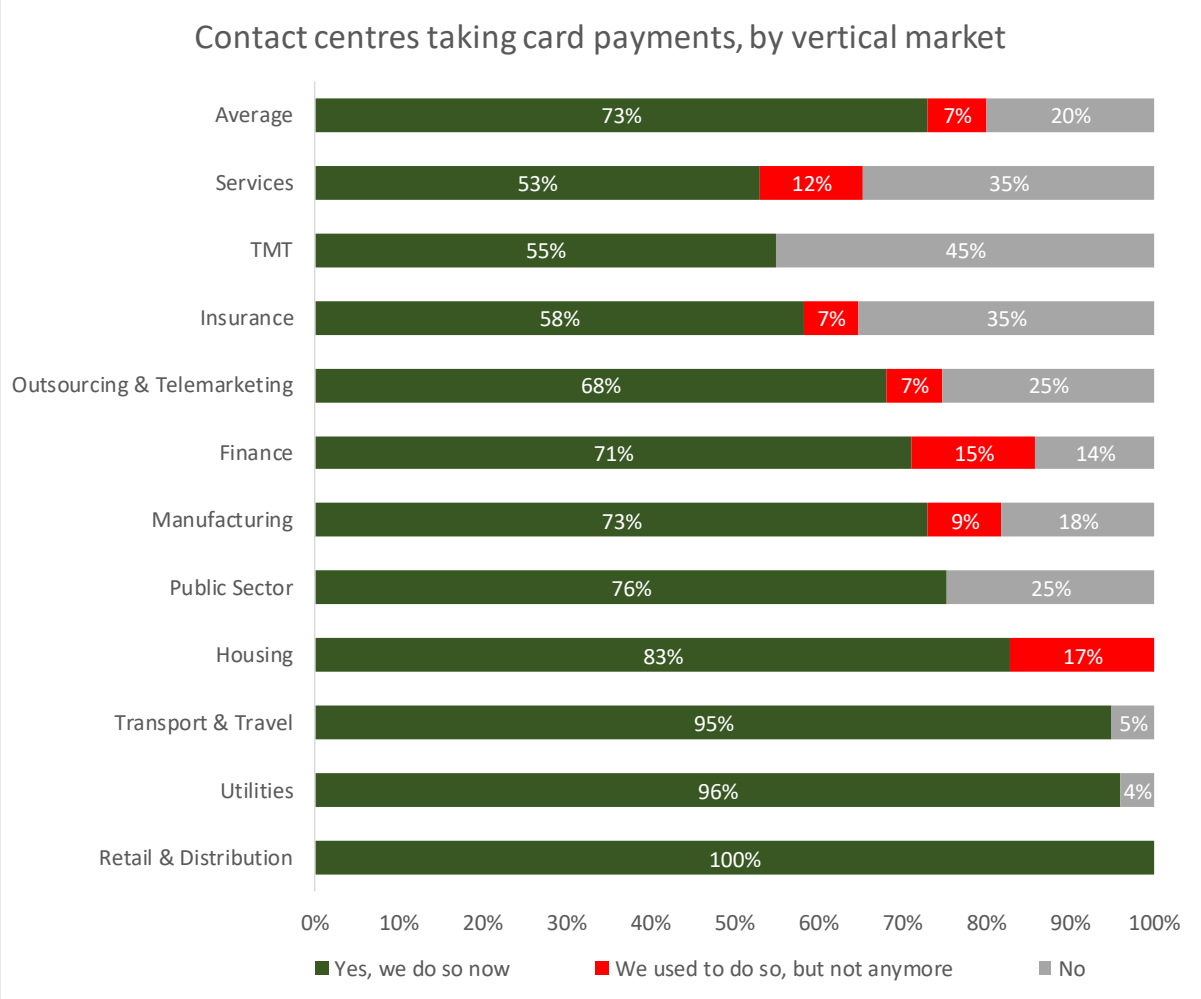
THE USE OF PAYMENT CARDS IN THE CONTACT CENTRE

The majority of respondents in all vertical markets take card payments in their contact centres.

The following charts show that the ability to take card payments is not an inexorably growing process, with 7% of respondents no longer doing so. This is especially the case for respondents from the housing, finance and services sectors.

Although the survey does not ask for the specific reasons why card payments are no longer taken, it is unlikely to be the case that customers now prefer to pay via other methods. More likely, the increasing requirements and costs associated with more stringent payment technology, processes and training outweigh the benefits of being able to take card payments over the phone. In such cases, many contact centres will choose to use a third-party to handle card payments, rather than remove the payment option entirely.

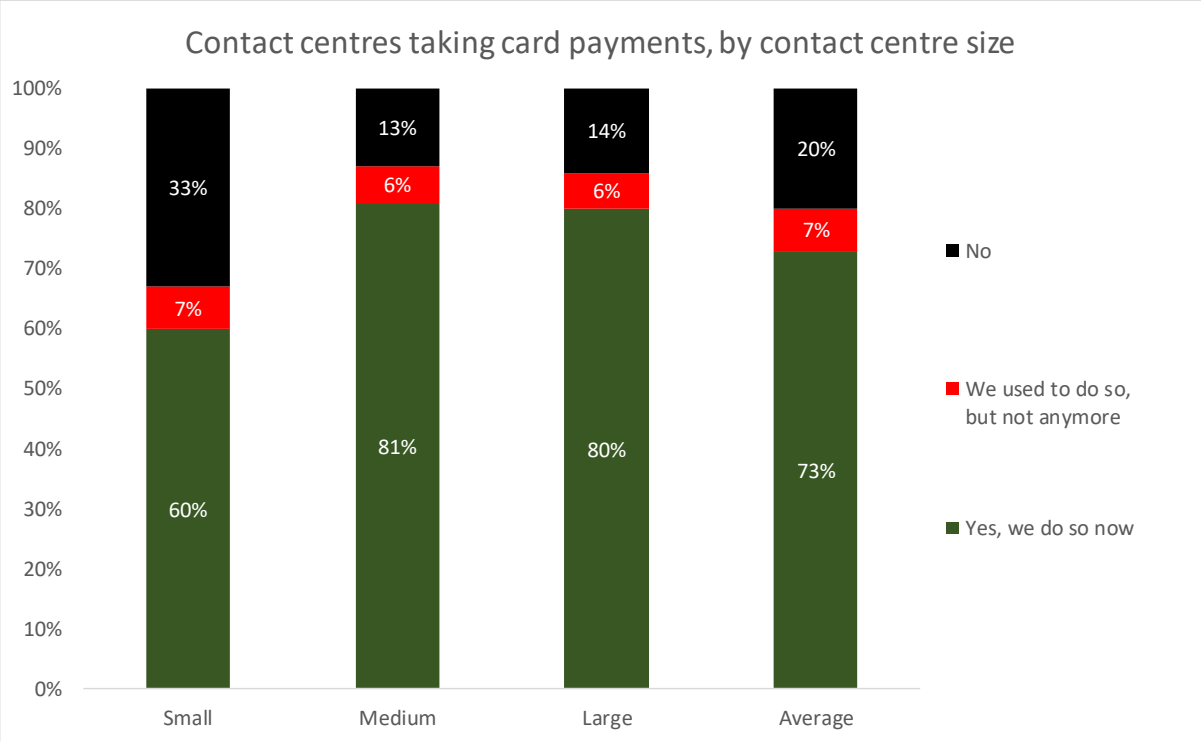
Figure 1: Contact centres taking card payments, by vertical market



NB: TMT = technology, media & telecoms

The usual positive correlation between size and card payment is again present this year. A similar proportion of respondents across all size bands have stopped offering card payment options themselves, showing that the expense and effort of achieving and maintaining PCI DSS compliance is applicable to all types of contact centre.

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



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.

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

Each merchant has a level assigned to it, based on the number of card payments taken annually across all payment channels and for a single payment card scheme (typically Visa, which has c. 70% market share).

Level 1 merchants have over 6m transactions per year (and/or has had a data breach that resulted in account data compromise, and/or is identified as Level 1 by Security Standards Council); Level 2: 1-6m; Level 3: 20k– 1m online transactions, Level 4: under 1m transactions, and less than 20k online transactions.

- Level 1 merchants have to be externally audited annually by QSA and have a Record of Compliance (RoC) or audited if any significant change in infrastructure that may impact on payment card security
- Level 2 – some banks ask to be externally audited by QSA and have a RoC, but not all do this
- Levels 3 and 4 self certify.

TPSPs have to externally certify by QSA and produce a RoC if they process more that 300K Visa transactions per annum

In version 3 of the standard, self-assessment questionnaires (SAQs) additional to those already existing were introduced to assist merchants and service providers to report the results of their PCI DSS self-assessment.

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.

Requirement 3: Protect stored cardholder data

This requirement is about reducing the impact of any data breach or fraud, by minimising 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 such as card verification codes is prohibited even if encrypted, and must be permanently deleted immediately after authorization. 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.

Sensitive authentication data (SAD) such as the card verification code (CVC) should normally never be stored, even in an encrypted format. 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, the most obvious place where data is stored as in the recorded environment, and the use of RAM scrapers should be considered, being 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 PCI DSS version 3.2.1 states more clearly than previously that 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 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 has a significant impact on contact centre industry, as providers move to the cloud, as it is mainly about managing the security of payment card data, having an incident response plan that deals with card data at risk, and also deals with TPSP's (through requirement 12.8: Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data).

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 programme to monitor compliance status
- 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, 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.

The annual Verizon Payment Security Report is a very useful and insightful document which tracks the level of PCI compliance, looking at each of the 12 key requirements and quantifying where the gaps in compliance are. 2018's report found that the level of full compliance – where all applicable security controls are in place – dropped from 55.4% in 2017 to 52.5% in 2018, bucking the upward trend since 2012. The greatest gaps were in Requirement 11 (Security Testing) and Requirement 12 (Security Management), whereas 88.5% of organisations had 100% of controls in place for Requirement 7 (Restrict Access).

The Verizon report noted that 42% of organisations used at least one compensating control in order to achieve PCI compliance.

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 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

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 CVC (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 the payment processor / payment gateway regardless of whether they supply the CVC or not, and that small merchants may simply be on a blended tariff where CVC/non-CVC transactions are grouped together.

In the case of chargebacks or disputes, the card brand will reduce their fees in cases where CVCs are present, but some merchants may consider that the cost of making sure that these codes are never stored in any format within their business (even encrypted) outweighs the potential benefit of reduced chargeback fees.

Even if were allowed, CVC storage is not necessary as recurring transactions do not require CVCs to be provided on each occasion: the payment service provider can supply a reference number from the original transaction that can then be used as a token which stands in for the card details and which does not require card details to be entered each time.

MEASURING AND PROVING 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 and/or the Visa Europe Merchant Agent Weblisting depending on their location.

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.

SELF-ASSESSMENT QUESTIONNAIRES (SAQS)

The PCI DSS guidelines state: "As a starting point, consider whether the organization should aim at excluding telephone-based card payment data entirely…for organizations committed to taking payments over the telephone, consideration should be given to techniques that minimize 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".

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 329 controls, rather than the 5 requirements and 24 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?

END-USER QUESTION 1:

WITH PCI COMPLIANCE SAQS BEING COMPLETED PER CHANNEL, WHOSE RESPONSIBILITY IS OVERALL COMPLIANCE? IS THERE A NEED FOR A SINGLE COMPLIANCE OFFICER, OR ARE EACH CHANNEL RESPONSIBLE FOR THEMSELVES?

While SAQs may be channel related as a result of the specific risks and controls required for different channels it should be remembered that **only companies and legal entities can be PCI DSS compliant**, not technology solutions or communication channels. Therefore, depending on the size of company there maybe multiple compliance officers, however, the responsibility for compliance and security should be at board level and the "buck stops" at the top.

One of the biggest myths regarding PCI DSS is that a technology solution can be compliant. This is a misconception perpetuated by procurement and marketing people when a tick-box is included in tenders asking whether a solution is PCI compliant? Compliance can only be achieved at a company level and therefore the type of questions you should be asking are, is your organisation PCI DSS compliant and to what level? And, how much of **my** PCI DSS responsibility does your solution remove from scope? It's a good idea to check the Visa Europe Merchant Agent Weblisting, before drawing up a shortlist of suppliers.

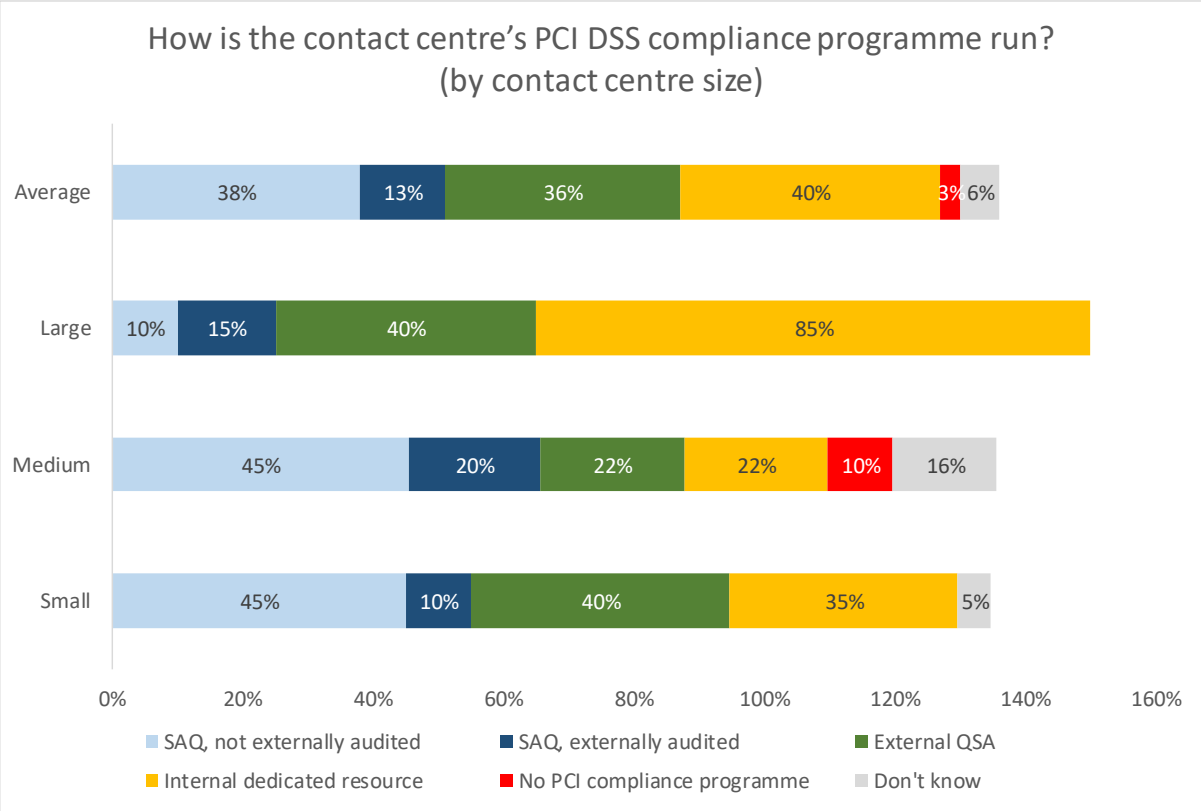
COST AND RESPONSIBILITY FOR COMPLIANCE

Small and medium operations are most likely to use self-assessment questionnaires, not usually externally audited.

Larger operations are very likely to use dedicated internal resources, with 85% of respondents stating that this was the case.

External QSAs were used by 40% of large operations, and the same proportion of smaller operations. Large operations are much less likely to use self-assessments of any kind.

Figure 4: 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.

Even if an organisation chooses to work with a outsourced service provider to handle all of their card payments, the final responsibility for card security lies with the merchant organisation. PCI DSS covers the entire trading environment, and all third-party partners and suppliers must also comply before full PCI compliance can be achieved.

Both Level 1 and 2 TPSPs have to complete SAQ D SP, with Level 1 organisations using a QSA and producing a Report on Compliance (ROC), and Level 2 using either self-assessment which may or may not have a QSA signing off on it.

The Attestation of Compliance (AOC) produced should be:

- Be provided on PCI SSC official documentation
- Identify the services the provider is supplying
- Identify the requirements tested
- Identify the completion date.

AOCs are designed to be public documents of proof of compliance, and any provider who is reluctant to provide theirs should be of concern.

In 2015, the PCI Council issued an FAQ[4] directly addressing the unacceptability of other types of compliance documentation or certificates, and clarified the requirement for official PCI SSC documentation:

"The only documentation recognized for PCI DSS validation are the official documents from the PCI SSC website. Any other form of certificate or documentation issued for the purposes of illustrating compliance to PCI DSS or any other PCI standard are not authorized or validated, and their use is not acceptable for evidencing compliance. The use of certificates or other non-authorized documentation to validate PCI DSS Requirement 12.8 and/or Requirement 12.9 is also not acceptable."

Alternatively, organisations can audit the service provider as part of their own PCI compliance validation: clearly, this is far less satisfactory and more expensive than using an AOC.

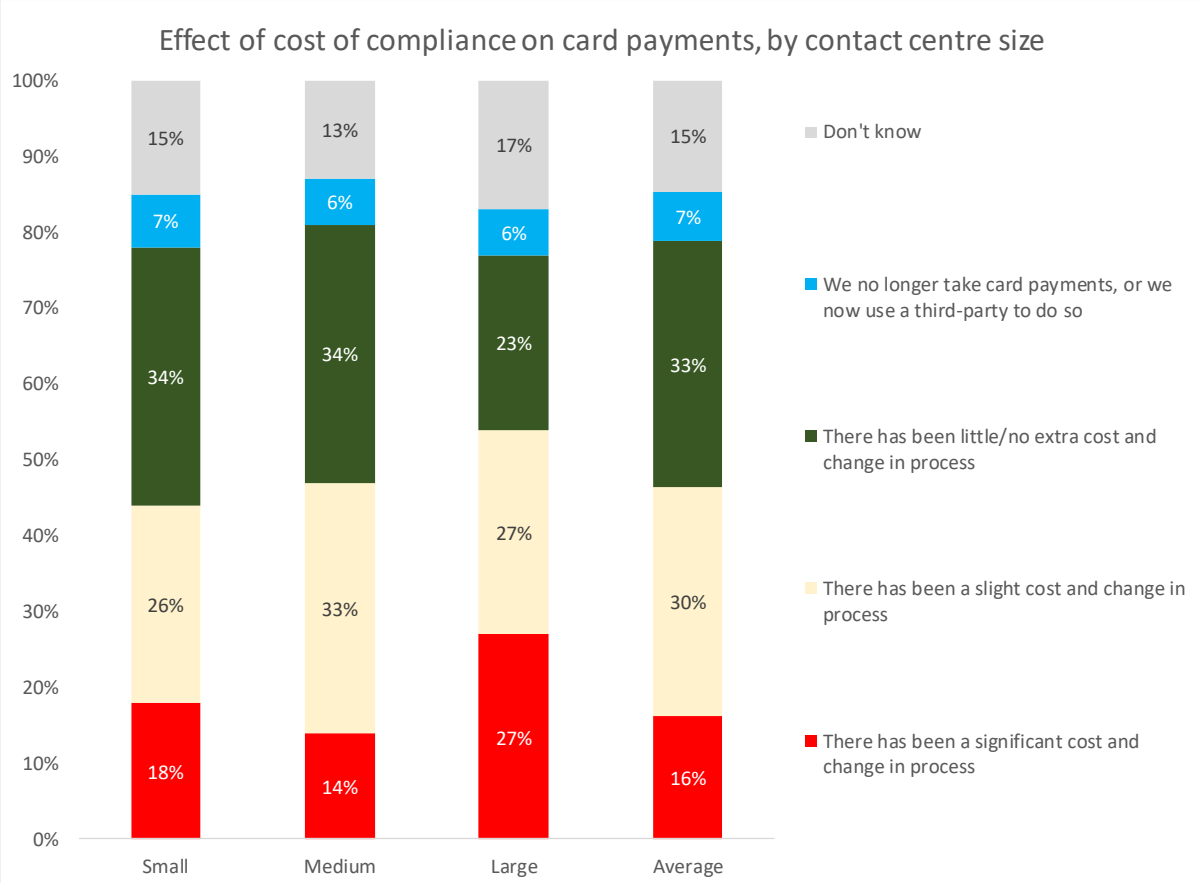
It is a requirement of PCI DSS for organisations to complete a PCI DSS Responsibility Matrix, which clarifies how responsibilities for maintaining PCI DSS requirements are shared between a merchant and their outsourced Third Party Service Provider (TPSP) / PCI provider. A Responsibility Matrix is made up of a list of PCI DSS requirements, indicating which are the responsibility of the PCI provider, which the merchant's, and which are shared, along with detailed notes on how this will be achieved.

[4] https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Are-compliance-certificates-recognized-for-PCI-DSS-validation

The following chart shows that a significant proportion of contact centres have found that the cost of PCI DSS compliance is very considerable, with 27% of respondents from large operations stating that they have seen a significant cost associated with compliance, as well as a change in their processes. These operations are the likeliest to be using external QSAs. Only one-third 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 either no longer take card payments or use a third-party to do so, in order to take the contact centre out of scope.

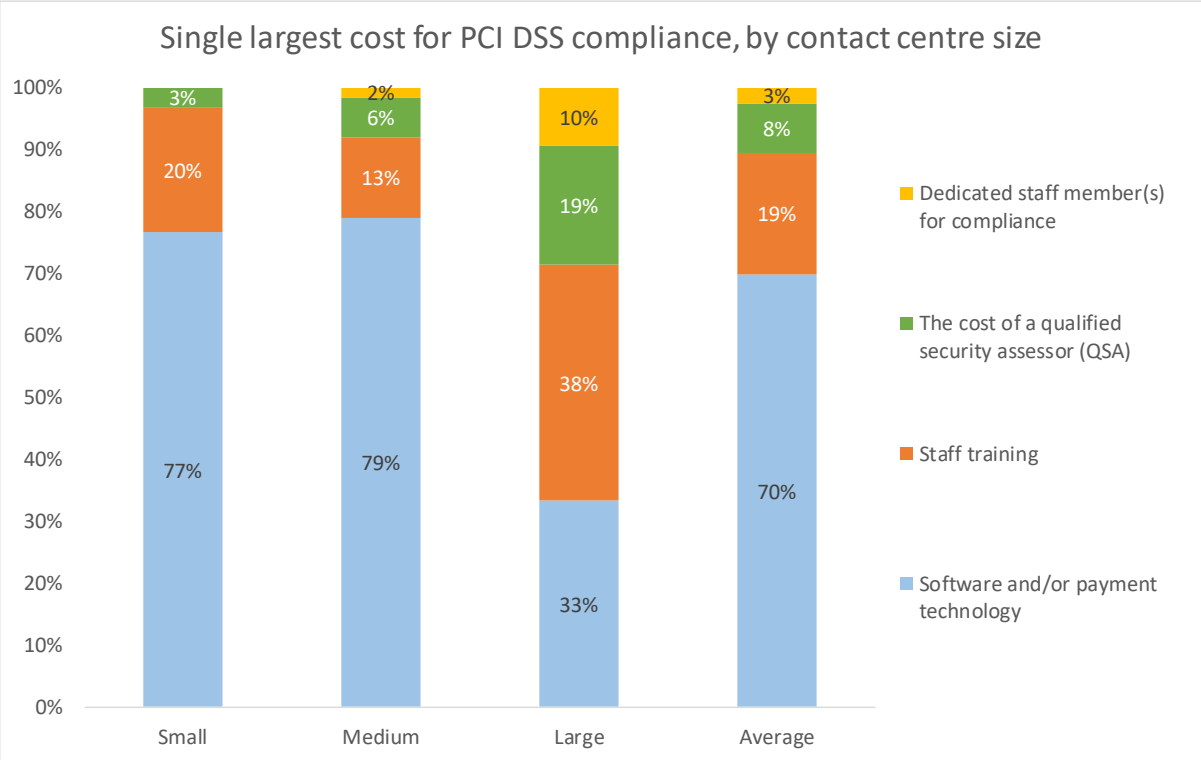
Figure 5: Effect of cost of compliance on card payments, by contact centre size



70% 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 38% of cases. Large operations are also most likely to note the high cost of bringing in external qualified security assessors (QSAs).

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

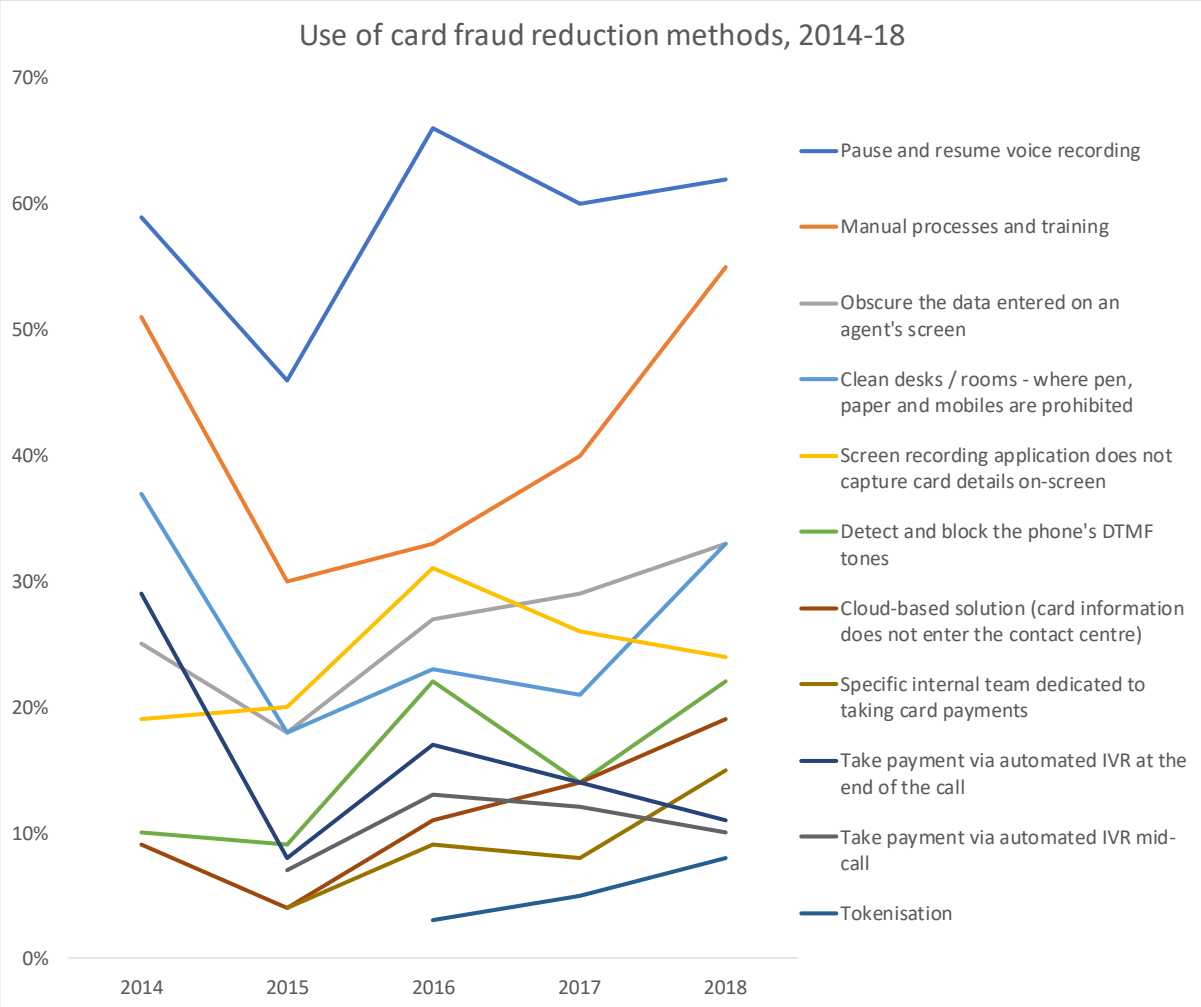


CARD PROTECTION TECHNIQUES AND TECHNOLOGIES

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 some 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 fully out of the scope of PCI. Respondents used a mean average of 2.5 card fraud reduction methods.

The chart below shows the use of card fraud reduction methods over the past five years. Pause & resume voice recording and manual processes & training are consistently the two methods most used. Cloud-based solutions and tokenisation show consistent growth.

Figure 7: Use of card fraud reduction methods, 2014-18



Looking at trends for these data in the chart above, only the use of end-call IVR and clean rooms were on a downward trend. Cloud and tokenisation were amongst the fraud reduction methods with the strongest upward trend. It should be noted that data can alter considerably from year to year as many of the survey respondents are different, and that changes from year to year should be viewed in the context of the longer-term.

END-USER QUESTION 2:

WHAT'S THE MOST COST-EFFECTIVE WAY TO TAKE CARD PAYMENTS AND BE PCI COMPLIANT, THAT WON'T DISCRIMINATE AGAINST ANY OF MY CUSTOMERS? (E.G. THOSE THAT CAN'T USE TOUCHTONE)

What is deemed as "Cost-effective" can vary from organisation to organisation and takes into account multiple factors. It's safe to say there is no single method of taking card payments that will completely avoid discrimination against all customer demographics. Therefore the best option is to offer multiple payment channels. A simple option for example, might be giving customers the ability to speak to an agent followed by IVR payment at the end of the call. For those happy to use their mobile devices or email use a "Pay-by-Link" option where the customer receives a one-time short code link. Using either of these methods helps to achieve PCI DSS SAQ-A which is relevant to card-not present transactions.

In industries where call recording is mandatory sticking with "pause and resume" recording can remove the need for customers to use touchtone. Alternatively SAQ C-VT for those who want to offer a fully manual option is available but involves encrypting card details in transit, training staff regularly and making sure no card details are recorded and therefore unless you are processing volumes of payments SAQ C-VT is not particularly cost effective.

TECHNOLOGY

IVR

IVR Payments – post-call (11%) and mid-call (10%)

A minority of respondents, especially those with a large contact centre, use an automated IVR process to take card details from the customer, descoping the agent environment.

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.

Many businesses which use IVR for payment will use a third-party provider and this will take the card data out of the organisation altogether. If they do not, the card data will still be within the organisation's network, so although this approach takes the agent out of scope, it does not in itself ensure PCI compliance.

While third-party IVR payments are an effective way of descoping a contact centre, there is the issue of customer experience to be considered: IVR is not suitable for all customers – those without DTMF-based phones or with poor eyesight may struggle to type in long card numbers effectively, especially if they have to take their phone away from their ear to do so, which means they potentially miss audible cues on what to do next. The same issue applies to DTMF masking and suppression (below).

DTMF SUPPRESSION & MASKING

Detect and Block the Phone's DTMF Tones (22%)

22% of this year's respondents use DTMF suppression (also known as masking) in order to assist with card fraud reduction. 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 is growing in popularity, it is one of the more expensive card fraud reduction methods to implement. Like IVR payments, there is also the risk that not every customer will be comfortable or capable of using touchtone to give their card details.

The PCI SSC notes[5] that "some implementations of DTMF masking rely on DTMF-detection - this may introduce a delay in the masking, and the initial portion of the DTMF tones may not be masked (this is called "DTMF bleed"). It is important to ensure that all DTMF tones, including any initial small portions of "DMTF bleed" that may be inadvertently allowed through a masking process, are not present in the environment.

"A properly designed and deployed DTMF-masking solution can take not only the telephony environment, but also the agent environment and CRM system out of scope. Entities should avoid solutions that leave agent environments in scope unless there is an unavoidable business requirement to do so."

TOKENISATION

Tokenisation (8%)

Tokenisation takes place in order to protect card information by replacing it with non-sensitive data which merely represent 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.

[5] PCI SSC Information Supplement • Protecting Telephone-Based Payment Card Data • November 2018 p33

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[6].

Apart from the replacement of sensitive card data, tokenisation is of great use for taking recurring payments (e.g. for a monthly subscription). Once the initial transaction is completed, the card becomes trusted and subsequent payments do not require the details to be taken again. In cases where the payment fails, neither merchant or cardholder are penalised with fees (unlike with direct debits).

[6] https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

ENCODED
secure automated payments

Card fraud reduction in contact centres: Take your pick

Robert Crutchington at Encoded recommends asking three simple questions when deciding which fraud control method to use

Many methods of taking card payments have emerged over the years as companies strive to be PCI DSS compliant. When the standard was first created the aim was to clarify and align various fraud prevention measures and regulations into a single agreed global framework. Therefore, it comes as a real surprise that in the latest UK Contact Centre Decision-Makers' Guide (DMG), published by analyst ContactBabel, eleven different ways are listed as to how contact centres attempt to reduce card fraud.

The research outlined that respondents use on average 2.5 different fraud reduction methods from the following list (in descending order of popularity):

- Pause and resume recording
- Manual processes and training
- Obscure the data entered on an agent's screen
- Clean desks/rooms – where pens, paper and mobiles are prohibited
- Screen recording application (that does not capture card details on-screen)
- Detect and block the phone's DTMF tones
- Cloud-based solution (card information does not enter the contact centre)
- Specific internal team dedicated to taking card payments
- Take payment via automated IVR at the end of the call
- Take payment via automated IVR mid-call
- Tokenisation

Time to take your pick – 3 questions to ask first

The ContactBabel survey showed that software and/or payment technology is the single biggest cost associated with fraud protection and PCI DSS compliance for almost three-quarters (70%) of survey respondents. Only reported that they hadn't had to increase their costs or change the way in which they operated for compliance.

Therefore it is important to ask yourself these three questions before deciding which route to take:

1. **What are we trying to achieve?** While understanding the importance of protecting customer data from fraud and cybercrime, not all contact centres realise that in the event of a security breach the buck stops with the merchant and it will be the organisation that is fined. However, there are ways to reduce the scope of the cardholder data environment. When choosing from the various fraud reduction methods it's important to establish what you are trying to achieve. Typically the answer is to prevent lost data and to make PCI DSS compliance easier and less costly.

2. **Is this good for the customers? How will customer service be impacted?** While there are many different glossy systems to choose from it is important to think about how your customers will react. Will partially sighted, elderly or disabled people be able to use the service? Sometimes simple is best, for example "pause and resume" recording, which is still used by over 60% of survey respondents, caters for everyone, is typically cheaper to implement than other options and offers the highest level of customer service.

3. **How much is it going to cost?** There is no such thing as a PCI DSS compliant technology solution. However technology can help achieve compliance. It is important to check that any third party payment service provider is able to prove it is PCI DSS compliant. While a third party cloud-based payment solution can remove cardholder data from the contact centre, the security processes and operational effectiveness of the provider must be checked. Remember compliance is ultimately the responsibility of the merchant. One of the most cost effective methods of dealing with payments is an automated IVR process to take card details from the customer while removing agent risk entirely. Often the simplest ways are also the least expensive, but just as effective.

Whatever method of card fraud reduction is chosen, by complying with PCI DSS, merchants and their service providers meet their obligations to the payment eco-system. They also help to build a culture of security and confidence that benefits customers and contact centres alike. The key is to ask the right questions and choose carefully.

For more information call +44 (0)1293 229 700, email sales@encoded.co.uk or visit www.encoded.co.uk

Pause and Resume (62%)

'Pause and resume' or 'stop-start' recording aims to prevent sensitive authentication data and other confidential information from entering the call recording environment, although does not stop the card data from entering the spoken / agent 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 SSC recommends "verifying that the call recordings do not contain CHD or SAD be undertaken on a regular basis – preferably weekly". (CHD – card holder data; SAD – sensitive authentication data – e.g. CVC), particularly in cases where pause and resume is agent-initiated.

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 or a specific field, 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 principle is similar to that applied to **screen recording** applications, where 24% of respondents stated that their application does not record card details from the agent's screen. 33% of respondents **mask card details** on the agent's screen, to prevent photographic copies being made.

Pause and resume is historically the most popular method of assisting with PCI compliance, and has several obvious benefits, not least of which include a 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.

More pertinently, PCI DSS 3.0 guidance states that "Pause-and-resume technologies may be manual or automated, and whilst a properly implemented pause-and-resume solution could reduce applicability of PCI DSS by taking the call recording and storage systems out of scope, the technology does not reduce PCI DSS applicability to the agent, the agent desktop environment, or any other systems in the telephone environment."

The new PCI guidelines have moved away from just securing recorded card data, to securing **spoken and recorded** card data, the former of which pause and resume cannot assist with. Pause and resume takes the recording and storage part of a call out of scope, but still leaves the agent, the agent desktop environment and other systems in the telephony environment in scope for PCI.

MANAGING LEGACY CALL RECORDINGS

The PCI standard (FAQ 1280) states clearly that the CVC and other sensitive authentication data (SAD) must not be retained post-authorisation, regardless of whether it is encrypted. If the removal of SAD from recordings is not possible (perhaps due to other regulatory constraints), the organization must discuss this with the acquirer or card brand to agree upon a solution and ongoing risk assessment and testing regime. In any case, SAD must not be available to be queried or retrieved by a search tool.

If necessary, speech analytics may be used to identify SAD such as CVCs in legacy recordings, which may then be rerecorded using pause and resume-type technology, or have tones placed over the top of a new recording to make the numbers unidentifiable.

Automated pause-and-resume removal of card data from legacy recordings may not be considered to affect the integrity of the original call materially; there is a balance of compliance, risk and cost. It's important to note that the value and risk of stored call recordings decreases over time, as card expiry dates are reached: eventually, there will be no value to criminals in these.

The encryption of PANs (the long card numbers) in call recordings may require ongoing changes to encryption keys, which can cause significant additional time and effort.

PCI DSS compliance requires 100% accuracy: if a single instance of unencrypted cardholder data or any sensitive authentication data is left, then the whole operation is not PCI compliant. While this may seem an extreme statement, an organisation as either compliant or it is not. As such, organisations may choose to use multiple solutions to reduce the risk, rather than relying upon a single one.

DIGITAL PAYMENTS

Businesses that wish to take card payments, but not have any spoken or recorded card data in their telephony or agent environment have a number of choices of solution, including IVR and DTMF suppression/masking. (While pause/resume removes card data from the recorded environment, it still leaves the agent in scope).

An alternative to these solutions is to send the customer a secure hyperlink via SMS, email, chat or social media which directs them to key in their card details, potentially treating this as a 3D Secure ecommerce payment rather than a MOTO payment (which are likely to be treated as non-secure payments by card brands), attracting lower fees and protecting the merchant against fraud-related chargebacks.

While this method takes the voice channel out of scope, this may not work for customers who do not have access to a device that allows them to pay online, who are prevented from doing so by disability, or who see online payments as insecure and refuse to use this option. Alternative measures should be put in place to handle these payment exceptions.

CLOUD

Third-Party Cloud-Based Payment Solution (19%)

19% of this year's respondents use third-party cloud-based payment solutions. Using a hosted or cloud-based solution to collect 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 can be seen to de-scope the entire contact centre from PCI compliance.

Like any cloud or hosted 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 most seem to be engineered in such a way as to minimise changes to the contact centre systems, processes or agent activities.

Level 1 PCI DSS cloud-based payment service providers have to meet very specific standards on a regular and ongoing basis, which may well be in excess of what a merchant / organisation is set up to do:

- 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.

Cloud-based payment service providers offer the ability to scale up and down, depending on business requirements, and allows payments to be taken from any location (including homeworking) through a virtual terminal payments solution. This also means that the payments element of disaster recovery is covered.

A cloud-based payments provider can also offer a number of payment channels (e.g. web, IVR, SMS, live phone, etc.), and enable recurring payments to be made securely without having to repeat card entry, through tokenisation.

PEOPLE & PROCESS

The PCI SSC Information Supplement states that "people represent the highest risk when it comes to the security of data, whether compromises are intentional or accidental."

Some of the risks involved include:

- Misuse of data and access privileges (insider's threat)
- Employees being compromised by external criminals (e.g. through blackmail or threats)
- Copying of card data through removable hardware, keylogging software or photographing screens / copying onto paper, handheld recorders etc.
- Opening of fraudulent phishing emails which install malware or look to steal data. 'Spear phishing' is targeted towards a specific individual or business, and may come from an ostensibly trustworthy source.
- Homeworkers' physical locations are likely to be accessible to non-employees.

Businesses must be aware that PCI compliance and general data security is not just about implementing technology, but also requires ongoing training, reminders and checks on what employees are doing.

IMPROVING PROCESSES & TRAINING

Improving Manual Processes and Agent Training (55%)

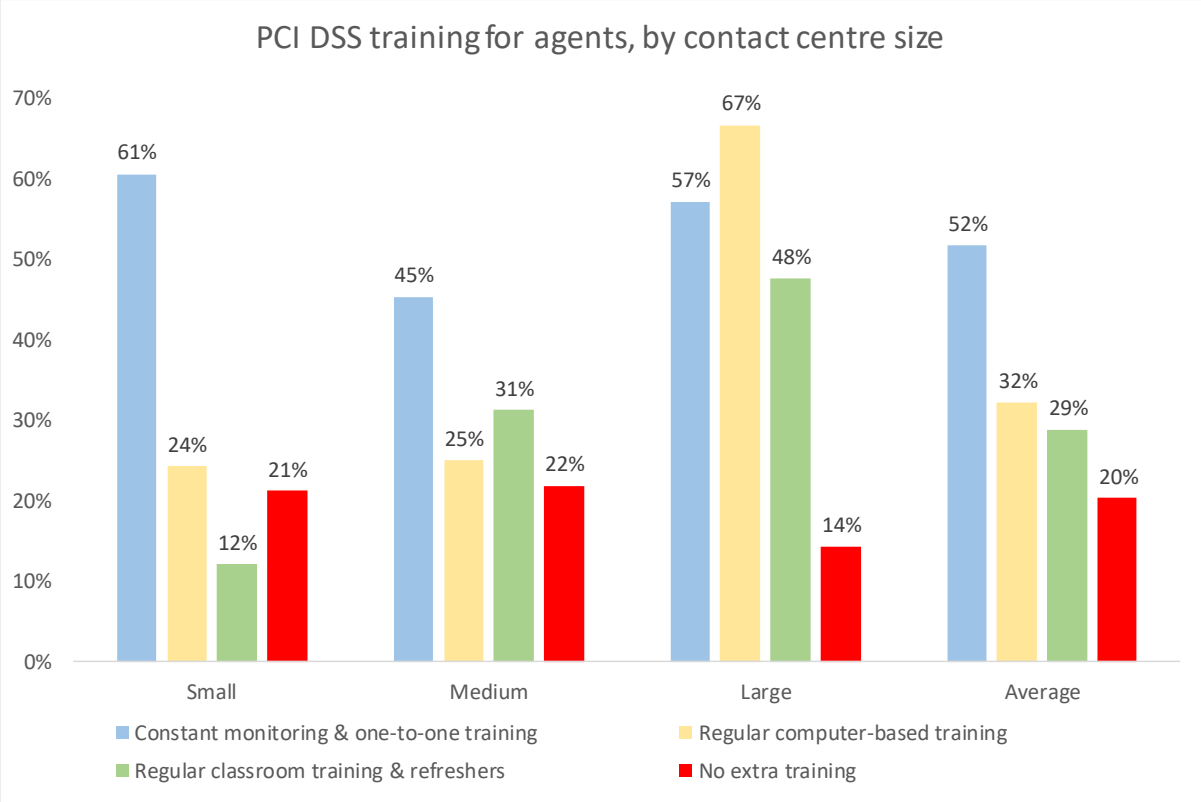
After pause and resume, the second-most widely used fraud prevention method is that of improving manual processes and agent training: the biggest risk in any organisation relating to data theft is its staff – not necessarily from fraudsters, but laxity in taking proper care of data – and the relatively 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 down the occasional card number.

The cost of staff training is reported to be a major drain on resources for large contact centres in particular, and the following chart shows that such operations are providing higher levels of both computer-based and classroom-based training for their agents than is the case in small and medium-size contact centres. 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 is a reason it is seen in large contact centres more frequently.

Agents in small operations are more likely to be receiving monitoring and one-to-one training, a level of support which is also seen in around half of larger contact centres.

20% of survey respondents do not provide any additional PCI DSS or card fraud reduction training for agents whatsoever, and this is somewhat more likely to be the case in smaller operations.

Figure 8: PCI DSS training for agents, by contact centre size



HOMEWORKING

On the face of it, homeworking presents an increased risk for businesses, for the simple reason that if card details are being read out within the call, no-one can physically verify whether the homeworker is writing these down.

There is also a greater risk from the potential use of unsecured, unencrypted data and voice transmissions using the public Internet or low-grade Wi-Fi security protocols. Even if the agent is blameless, it is possible for others in the environment to eavesdrop on the conversation or otherwise have access to records if the agent steps away from the desk for a moment, or even to install keylogging software or hardware.

As such, businesses should make sure that a strongly encrypted virtual private network is used for the transmission of voice and data traffic, and that personal firewalls, malware and virus protection software are fully operational and up-to-date, without requiring any manual intervention from the agent. Of course, voice and screen recording should be compulsory, and the hardware should not allow the storage of data on unencrypted or removable media such as memory sticks.

Some of the best practices around managing homeworking agents in a PCI DSS compliant way include:

- agent hardware needs to have the same level of malware, antivirus and firewall protection as computers used within the contact centre environment, and these need to be automatically updated and security patched without the agent being able to disable or delay any updates. Where possible, agent hardware should not have any capability to move data onto removable hard drives

- agents should have clearly-defined responsibilities regarding the physical security of all equipment in their homes, and understand the importance of keeping the workspace secure (e.g. not using sticky notes to write passwords on)

- Wireless network, VoIP and network encryption protocols used should be up to the current published standards, as these frequently change. Any supporting hardware or infrastructure should be upgraded or changed at the same time as the central contact centre's infrastructure. The public Internet should not be used for the transmission of voice, with analogue landlines being preferable if encrypted VoIP systems are not available

- Agent user IDs and passwords should be changed frequently, with multi-factor authentication being used, in order to verify that the person typing the password is actually the authorised user (this may be an additional requirement to those normally needed within the contact centre, where other employees will be immediately aware of the presence of an unauthorised user)

- Regular on-site visits to the home environment are necessary to identify any other potential risks.

END-USER QUESTION 3:

IS THERE ANYTHING DIFFERENT WE NEED TO DO ABOUT HOMEWORKING AGENTS WHERE PCI AND SECURITY IS CONCERNED?

ENCODED
secure automated payments

PCI DSS doesn't currently recognise the difference between home or on-site workers - it is all about maintaining the standard. The same checks and security are required regardless of where the payment is taken bearing in mind it is the organisation or entity that needs to prove PCI DSS compliance not the systems used or individual agents. It is advisable to use a strongly encrypted virtual private network if home workers are to take payments.

With home working it is even more relevant to ensure agents do not have access to card data therefore methods of payment such at IVR mid-call or at the end of call are good options to maintain compliance. For mobile or email payments offering a "Pay-by-Link" option where a one-time short code link is sent to the customer takes card details out of scope for PCI DSS purposes and protects both the customer and the agent.

Clean Rooms (33%) and Dedicated Payment Teams (15%)

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. For the agents, a clean room is generally not seen as being a particularly pleasant working environment, being spartan of necessity, and raises staff attrition levels as a result. 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.

The PCI SSC notes that "physical segmentation approach can be valid to deal with 'exceptions' even when technology to prevent spoken card data is deployed". For example, in the case where a customer is unable or unwilling to use DTMF to input their card details, a dedicated team can be used to handle these, although the SSC is very specific that sensitive authentication data (e.g. CVC) must be deleted immediately.

The PCI SSC information supplement[7] suggests ways of doing this with controls based on PCI DSS requirements:

Physical controls

- The room is a secure physical area where payment details are taken over the telephone and processed.
- Physical access to the secure room is limited, controlled and monitored.
- Physical access rights are granted based on individual job function, regularly reviewed, and revoked immediately upon termination.
- The customer service representative (CSR) must use one or two authentication factors e.g., token, swipe card, personal code through an access-control device to enter the room (note that while PCI DSS Requirement 9.1 mandates only one authentication factor, using multi-factor authentication is considered best practice).
- Physical access is monitored using an access-control mechanism or a video camera (or both), and the records are stored for at least three months unless legal restrictions apply.
- The access-control and monitoring systems must be protected against tampering or disabling.
- Any workstation in the secure room is locked to prevent unauthorized use.
- The CSR is not allowed to take into the room personal electronic devices; any pens and paper are replaced with personal whiteboards and dry-wipe marker pens.
- The room has no printing facilities beyond the payment terminal/POS receipts.

[7]Information Supplement, p39

Procedural controls

- To enforce compliance, the CSR in the non-restricted area is not allowed to receive cardholder data from the customers.
- At the point of transaction, the CSR either transfers the call to a CSR in the secure room (potentially leaving the PBX in scope for PCI) or informs the customer that they will call them back.
- The secure room CSR either calls the customer back through a separate VoIP or POTS connection or picks up the call, which is transferred from the PBX to the secure room.
- When in possession of the card data, the secure-room CSR processes the payment via a payment terminal or a virtual terminal connected to a payment service provider. Following this, the CSR can record the transaction details on the CRM system and securely dispose of or file any paper record or receipt.

THE EFFECT OF PCI COMPLIANCE & CUSTOMER EXPERIENCE

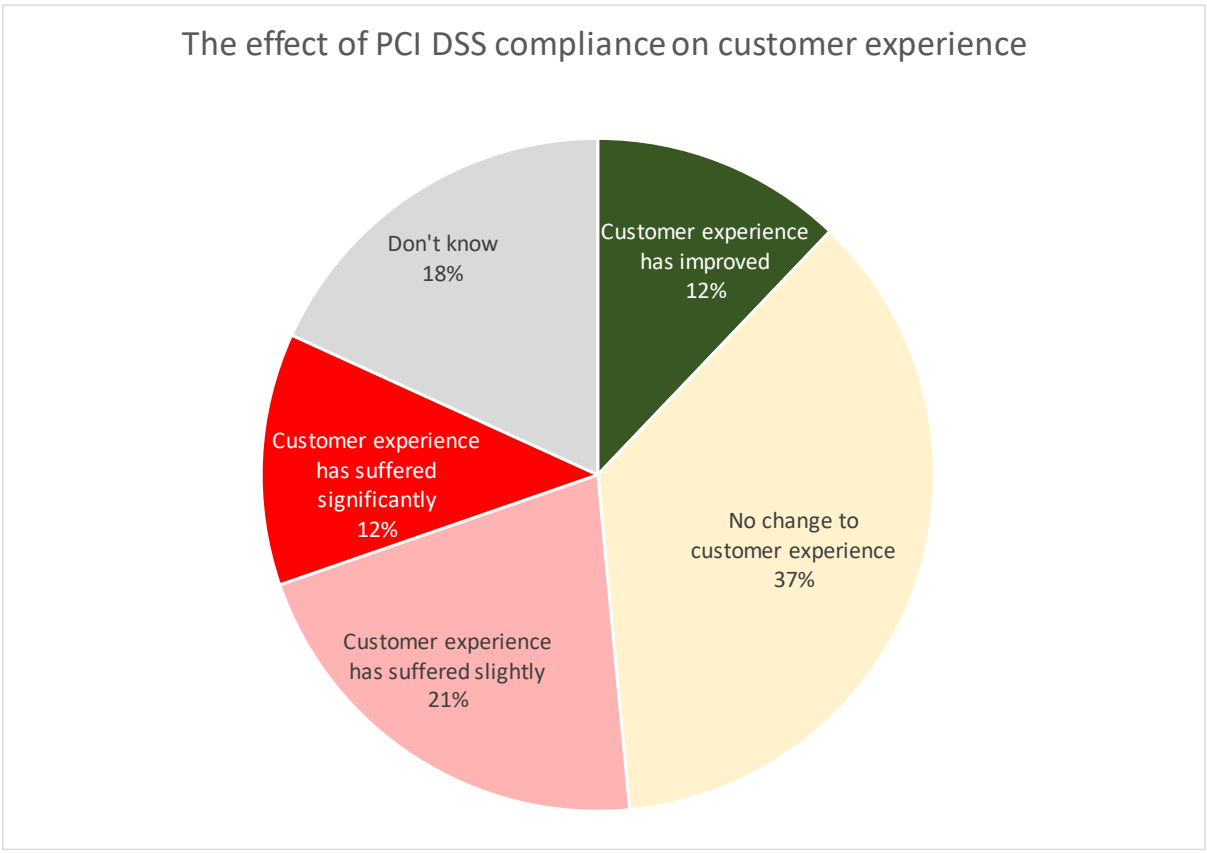
Many PCI DSS compliance and card fraud reduction methods are likely to have an impact upon the customer, in terms of increased effort or inconvenience (e.g. having to type in a card number can be awkward if using a smartphone, as navigation through screens will be required while holding the phone away 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 average customer's perspective.

Organisations should consider what the preference of their customer base is likely to be: a younger demographic may prefer mobile or web billing, whereas older demographics may want to speak to an agent – and may not be comfortable with an IVR-based payment solution being introduced within the call. It may well be the case that multiple payment solutions have to be offered: while this can seem like an inefficiency – and may require most complicated SAQs to be completed – the organisation should consider the positive effect that this can have on the customer experience, and thus loyalty.

Currently, 33% of respondents stated that PCI DSS compliance had a negative effect on the customer experience, with 12% believing that there had been an improvement, suggested that customers may have gained from improved security, but at an expense to the customer experience.

Figure 9: The effect of PCI DSS compliance on customer experience



CUSTOMER AUTHENTICATION

Customer security processes are generally asking two questions: 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, strong identity verification processes are now seen as critically important and most calls that are not merely initial enquiries will need to verify a caller's claimed identity by asking for additional information that only the real customer should know. 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.

Due to the increase in the use of P2Pe (point-to-point encryption, a security standard that requires payment card information to be encrypted upon initial swipe and then securely transferred directly to the payment processor before it can be decrypted and processed) and chip & PIN payment, fraudsters have been looking at easier targets, with the voice channel being seen as being an attractive opportunity. This is particularly the case as contact centre agents are likely to want to help a customer, and may be more likely to be 'socially engineered' – i.e. conned – into assisting fraudsters without realising it.

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 have responded by introducing ever more complex identity verification processes, which have driven up the length and cost of calls, and decreased the quality of the customer experience. And still, fraud continues to happen.

END-USER QUESTION 4:

WHERE DO THE GREATEST FRAUD AND SECURITY THREATS COME FROM? APART FROM FOLLOWING PCI DSS, GDPR AND OTHER REGULATIONS, WHAT ELSE SHOULD COMPANIES BE DOING?

Security commentators typically report human error as the main cause of data breaches. In fact The Cyber security breaches survey 2017[8], conducted by Ipsos Mori on behalf of the UK Government, revealed that 72% of reported breaches related to staff receiving fraudulent emails. This highlights the need for regular staff training and this Inner Circle report shows that after pause and resume recording, the second most widely used fraud prevention method is improving manual processes and staff training as reported by 55% of respondents.

Encoded also recommends organisations undertake ISO 27001 certification, this is an information security standard. In addition, companies should implement an information security management system (ISMS) which is a framework of policies and procedures that includes all legal, physical and technical controls involved in the organisation's risk management processes. Finally working with Encoded to use technology to de-scope your contact centre from PCI DSS is a cost effective method to prevent falling foul of fines and compliance regulations. Preparation and prevention certainly pays off when it comes to payment and cyber security in contact centres.

[8] Cyber security breaches survey 2017
https://www.cyberaware.gov.uk/sites/cyberstreetwise/files/cyberstreetwisesmallbusinessreputationreport-2016-02-08.pdf

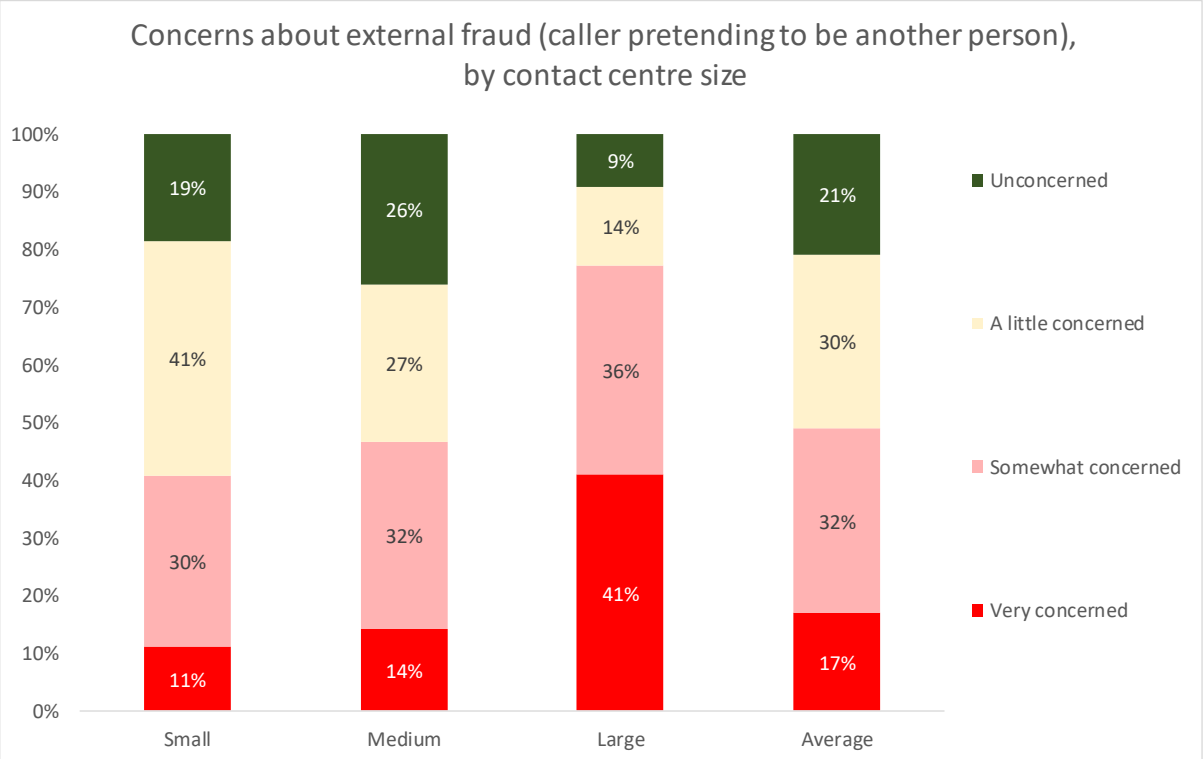
THREATS FROM FRAUD

The widespread rollout of chip-and-PIN cards, and growing uptake of point-to-point encryption means that criminals are looking for easier targets for their fraudulent activities, and the 'Card Not Present' channels such as the MOTO (mail order / telephone order) channel have become more heavily-targeted.

Survey respondents from contact centres were asked to rate the level of concern they had about the possibility of fraud originating from various sources.

41% of respondents from large (200+ seat) contact centres stated that they were very concerned about external fraud, defined within the survey as the caller pretending to be another person. This shows that customer identity verification is taken very seriously, and that many large organisations do not feel that they have an acceptable level of fraud control.

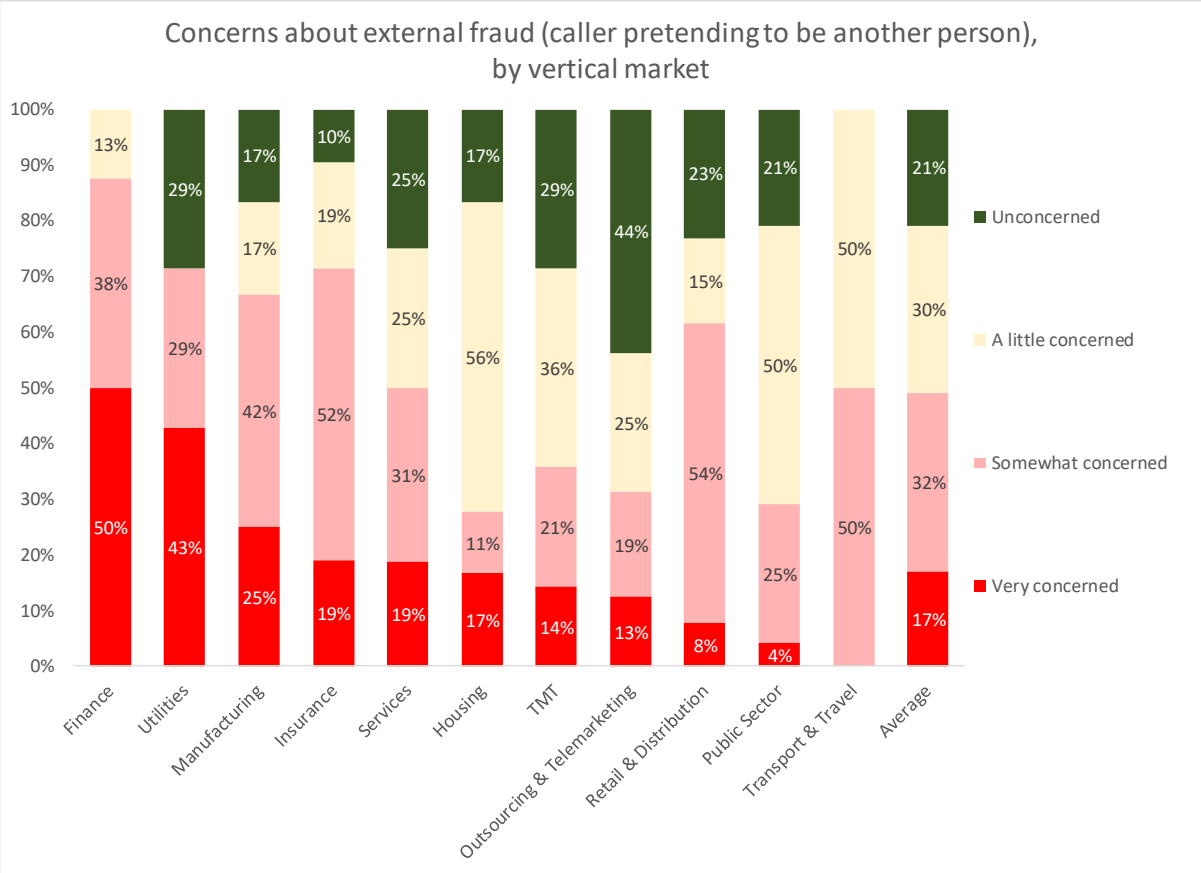
Figure 10: Concerns about external fraud (caller pretending to be another person), by contact centre size



Although some of the vertical markets studied within the survey did not provide enough responses for a rigorous statistical assessment, it is still worth looking at concerns over external fraud by vertical market.

As might be expected, the finance sector reports the greatest concern over external fraud threats, as it is the most likely target for financial fraudsters. We would not expect many of the other vertical markets to display particular concern, as the potential financial gain for a fraudster imitating a single customer is too limited in many cases.

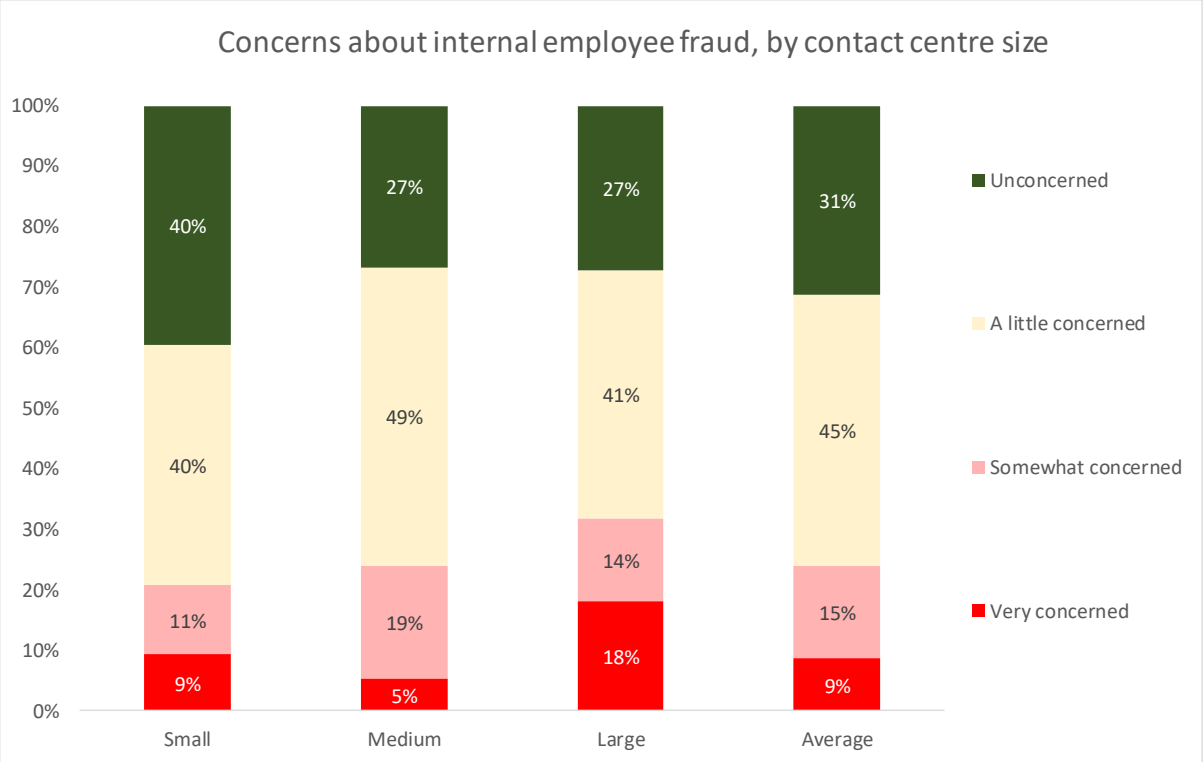
Figure 11: Concerns about external fraud (caller pretending to be another person), by vertical market



Levels of concern about internal employee fraud were generally much lower, although 32% of respondents from large contact centres were either very or somewhat concerned about this.

This lower level of concern may be related to the feeling that PCI compliance goes a long way to reducing the opportunities that an internal fraudster has for financial gain or the theft of data.

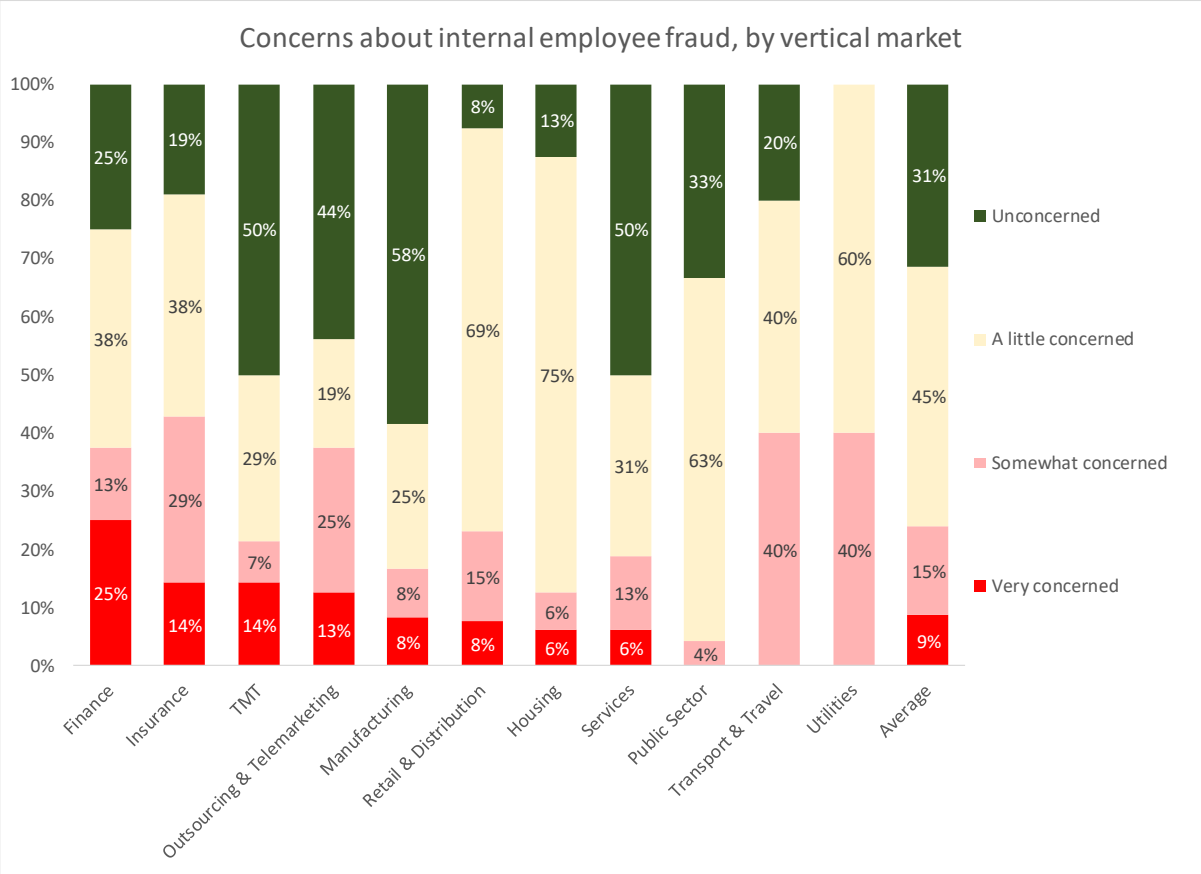
Figure 12: Concerns about internal employee fraud, by contact centre size



Looking at a vertical market level, the finance and insurance respondents had the greatest worry about internal fraud, with the public sector having the least.

This concern is probably more related to the potential gains that a fraudster in the financial service sector can achieve, rather than the internal security in a finance contact centre being of a lower standard than in other vertical markets.

Figure 13: Concerns about internal employee fraud, by vertical market

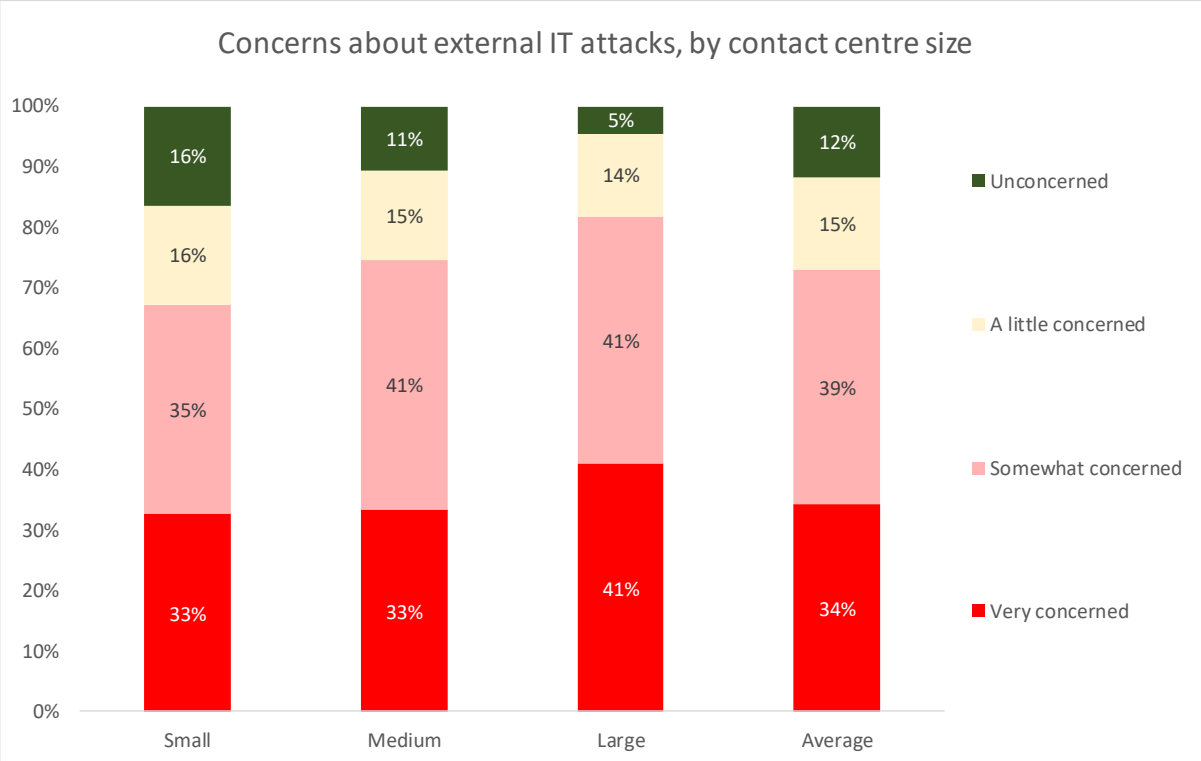


Concerns about external IT attacks were consistently significant across all size bands.

External IT attacks may go after databases of customer details. If PCI compliance is fully achieved, the chances of getting useful payment card data should be minimal: PANs (long card numbers) are encrypted, and sensitive authentication data such as CVCs are forbidden to be stored in any form, encrypted or otherwise.

External IT attacks may not just be related to card data of course, and the general concern across the board reflects this widespread fear of cyber attack.

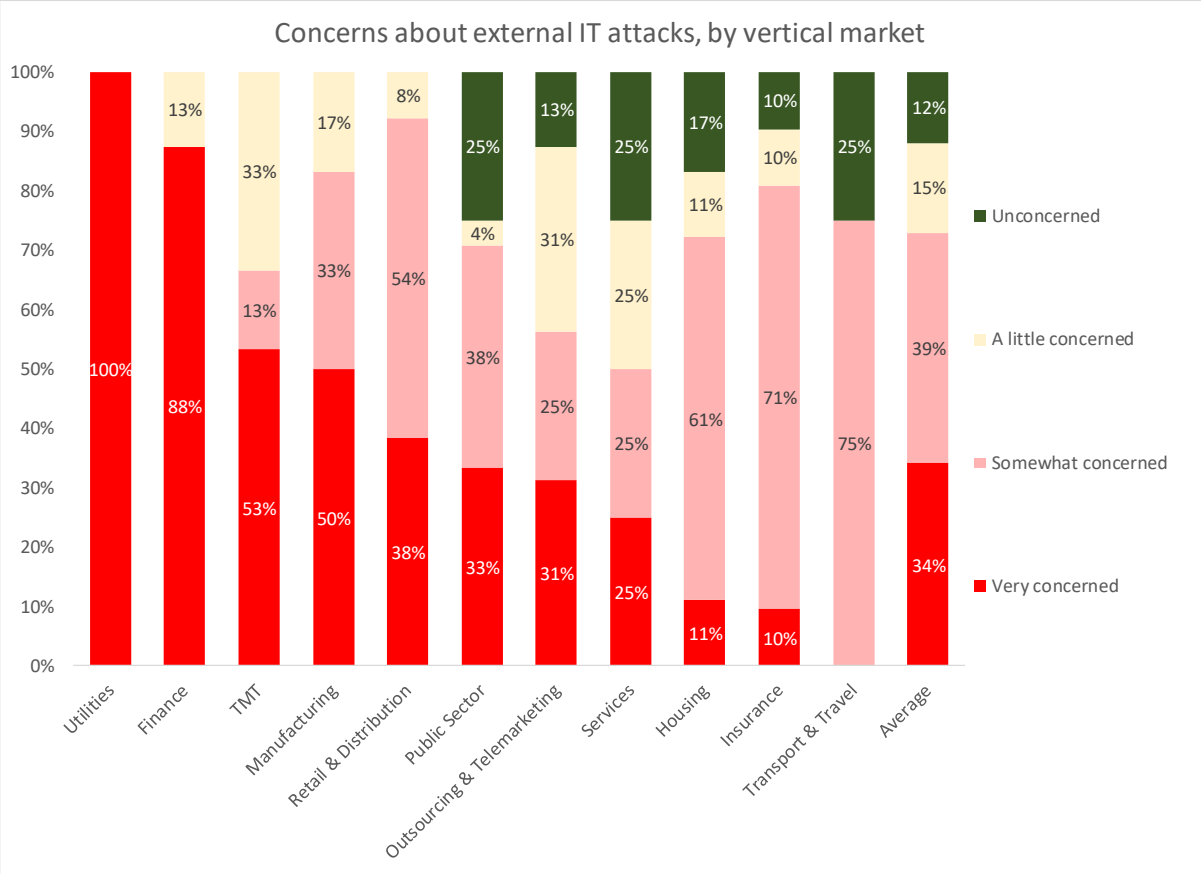
Figure 14: Concerns about external IT attacks, by contact centre size



The utilities and finance sectors show very deep concern about the possibility of external IT attacks on their business, with a majority of respondents in all sectors showing significant levels of worry about this form of incident.

Utilities companies tend to have millions of customers, and at the very least, a large-scale data breach would be extremely damaging for the brand reputation.

Figure 15: Concerns about external IT attacks, by vertical market

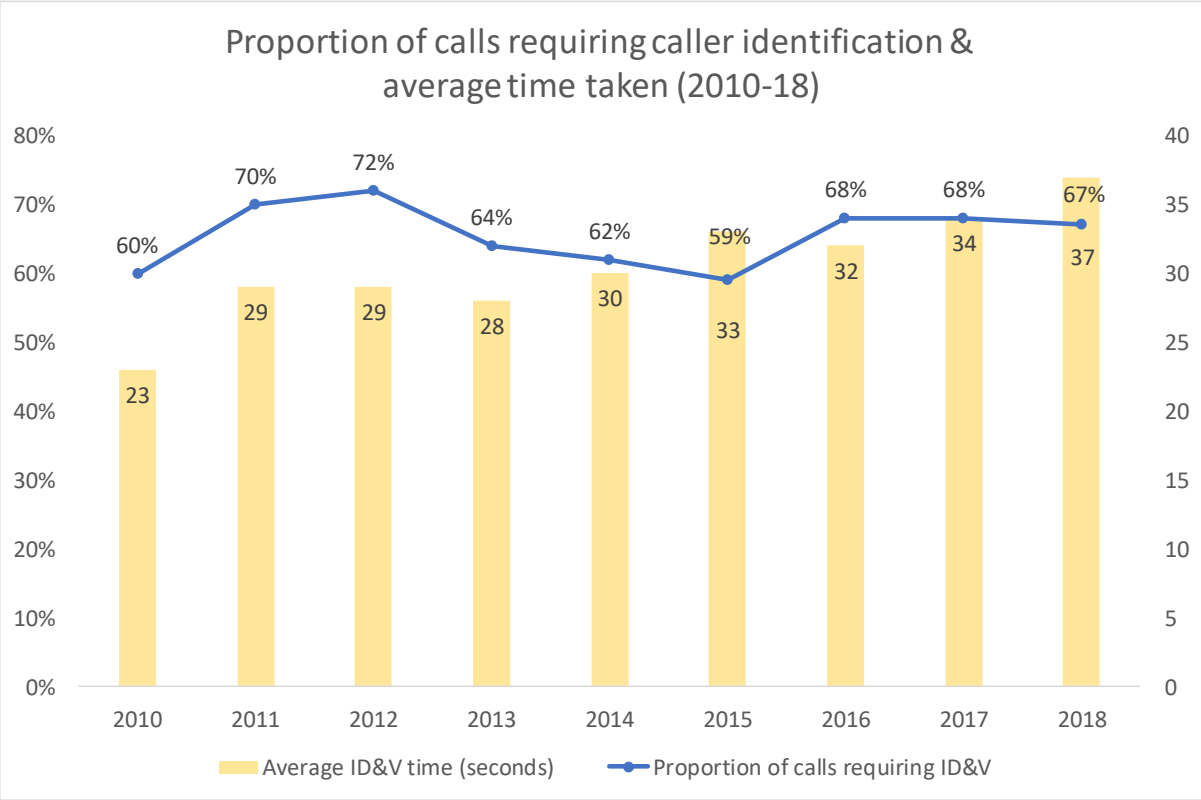


THE COST OF IDENTITY VERIFICATION

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 50% since 2010). Please note that these figures are mean averages: some businesses can take two minutes or longer to authenticate their customers.

Although in-call efficiency has improved, identity verification is generally no faster than it ever was: all factors which drive up the cost of initial identification.

Figure 16: Proportion of calls requiring caller identification & average time taken



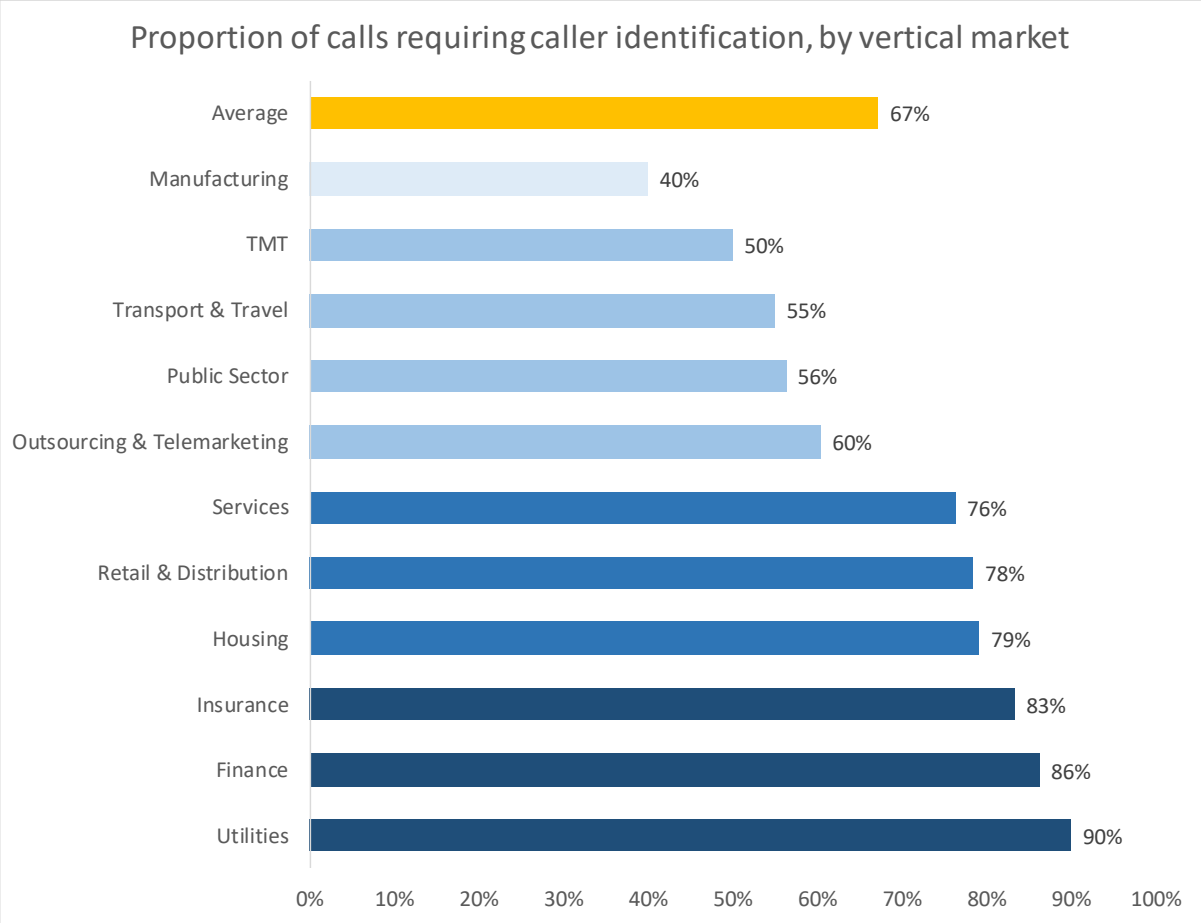
Industry-wide, a mean average of 67% of UK inbound calls are stated to require caller identity verification.

38% of respondents state that all calls are subject to identity verification, with 18% stating that none are.

Insurance, finance and utilities operations are the sectors most likely to require identity verification. Transport & travel respondents (which include travel information lines) and manufacturers (often B2B account management and product support) are the least likely, with the IT helpdesk portion of the TMT sector also less likely to require customer 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 17: Proportion of calls requiring caller identification, by vertical market



93% of respondents who authenticate identity do so through human means, taking an average of 37 seconds to do so.

In a large proportion of instances, respondents that use IVR or speech recognition also use the agent to double-check customer identity, wasting the caller's time and increasing the contact centre's costs.

Figure 18: Caller identity authentication methods (only those contact centres which authenticate some or all calls)

Identification method	Proportion of callers identified using this method
Agent	93%
DTMF IVR (touchtone)	7%
Speech recognition	2%
Voice biometrics	1%

The mean average time taken to authenticate using an agent remains fairly steady, at 37 seconds (38 seconds in 2017).

The time taken to authenticate using an IVR is very slightly less: the main difference is that the agent's time is not used, so the call duration (from the operation's perspective) and cost per call is reduced.

Figure 19: Time taken to authenticate caller identity using an agent (seconds)

	Seconds to authenticate caller identity using an agent
1st quartile	16
Median	25
3rd quartile	50
Mean	37

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 only as such, rather than being definitive.

67% of all calls require a security and identification process to be completed first. This year, 93% of calls were reported to be authenticated by agents. On average, it takes 37 seconds to go through security. 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): 7.06bn[9]

Proportion of inbound calls that require security and identification checks: 67%

Average length of agent-handled security and identification check: 37 seconds

Average call duration: 5m 29s (329 seconds), therefore 11.2% of the call is ID&V

Mean average cost per inbound call: £4.27

Cost of time spent on agent-handled security and identification check: 47.8p per call

Proportion of calls requiring ID&V: 67%, of which 93% require an agent

Therefore, overall cost of agent-handled security and identification checking: £2.1bn per year

[9] ContactBabel, "UK Contact Centres 2018-2022: The State of the Industry"

IMPROVING IDENTITY VERIFICATION

Identity verification through agents is slow, expensive, prone to error, open to fraud and disrupts the customer experience.

To improve customer authentication, solutions and processes have to address the following issues:

- businesses want to reduce the cost of fraud, and the attendant brand damage
- customers want convenience, but also expect that their personal information and assets will be protected
- businesses need to comply with existing and new laws & regulations
- the contact centre industry spends excessive amounts of money on identifying and verifying customer identities
- using a single method of customer identification relies heavily on it being foolproof
- 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.

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. Customers can undergo a 'Spanish Inquisition' before being permitted to make their enquiry or place their order – not only reducing customer satisfaction, but also costing businesses time and money. It takes an average of almost 40 seconds to verify a customer's identity manually, and this mounts up considerably: 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. Many customers struggle to remember multiple passwords, and with numerous website hacks taking place, passwords that are used for more than one activity risk being exposed and used by fraudsters.

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 the customer's smartphone.

Combining these factors creates a more complex, and potentially more secure two-factor or three-factor authentication process, although being able to rely upon a previously enrolled voiceprint 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.

An increasing amount of authentication is done through face recognition (e.g. logging into apps on a smartphone), and security solution providers have built in functionality to avoid high-resolution photos being used, in the same way that voice security requires solutions to be able to identify recorded or synthetic voices.

Voice biometrics are now used in many large businesses, especially those in financial services, and go a significant way to improving both security and customer experience.

VOICE BIOMETRICS

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 some businesses now allow thumbprint-enabled smartphones 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 and speech rate. 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 utilising voice biometrics to authenticate customers within the course of the conversation.

With this technology, contact centres can:

- Voiceprint the vast majority of customers for seamless passive enrolment: in the course of a conversation, a voiceprint is created for that customer which lies on record for them to be authenticated against on the next call
- Securely authenticate customers with no customer effort: the first few seconds of a call should be enough to match the customer's voiceprint against those on record
- Open up wider options for self-service as the business can be sure about who the customer is
- Cut seconds off average handle time: no need for customers to answer numerous security questions as the conversation they are having provides enough information to identify them
- Significantly reduce fraud risk for all customers, and deter fraudsters when combined with other layers of security, for example, phoneprinting, which analyses the background audio of the call
- avoid bad publicity for your brand through high profile data breaches.

The customer's experience of voice biometrics should be positive: since speaking is natural and intuitive, a well-planned implementation can result in a better customer experience that eliminates the need for PINs or passwords.

It is worth mentioning that some businesses have found that their calls-per-customer figure increases once they make contacting the organisation a less unpleasant experience. This may drive up call volumes to some extent, but also provides agents with more chance to build brand loyalty and to cross-sell and upsell.

Methods of gathering and using customer voiceprints include:

- In the case of text- and language-independent authentication, the customer's voiceprint (collected on previous calls) is authenticated in the background during the natural course of conversation with an agent, while simply outlining their service request - minimizing both customer effort and time-to-service. There is no need to remember PINs or passwords, which greatly improves the customer's experience
- 'Account Number'-based voice verification - the caller is asked to speak their account number. The account number identifies the caller, and the spoken words are used to generate a voiceprint that verifies the caller is the account holder
- 'Challenge Response'. Typically, the customer is asked to repeat a series of numbers, e.g. "Please say 'one seven three four'". The spoken words are used to generate a voiceprint. The numbers spoken are usually different each time the caller phones and can be used to avoid instances where the fraudster has recorded the customer's voice.

In cases where a two-factor authentication process is required, voice verification can be combined with a 'something you know' - such as an answer to a memorable question. Real-time agent guidance can prompt agents to ask a further security question within the call if the process requires it. Some biometric solution providers offer continuous authentication throughout the call, rather than assuming that the person initiating the call is the same as the one who is asking to transfer money into a different account, for example.

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 ANI) 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.

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.

Voice biometrics, while an excellent authentication tool, is not in itself enough to deter fraud attacks. In fact, researchers at the University of Alabama[10] 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. A similar example of this can be viewed here[11]. As voice is a characteristic unique to each person, such attacks essentially give the attacker the keys to that person's privacy.

Obviously, solutions are improving all of the time, 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.

Biometrics can go beyond voice, with some solutions able to identify how a customer typically types, uses a mouse or the type of language that they use, flagging up suspicious activity if this deviates from the norm. Keyword spotting is also employed: the identification of words associated with a significant level of fraudulent activity, for example "I want to move money from my personal account to my credit card", or "my address has just changed and I'd like a new credit card sent there".

Contact centres wishing to deter fraud should consider combining voice biometrics with phoneprinting or call signalling analysis for a multi-layered solution. These solutions rely upon 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 would have missed, and are considered later in this section of the report.

[10] http://www.biometricupdate.com/201509/uab-researchers-find-that-automated-voice-imitation-can-spoof-voice-authentication-systems
[11] https://www.digitaltrends.com/cool-tech/baidu-ai-emulate-your-voice/

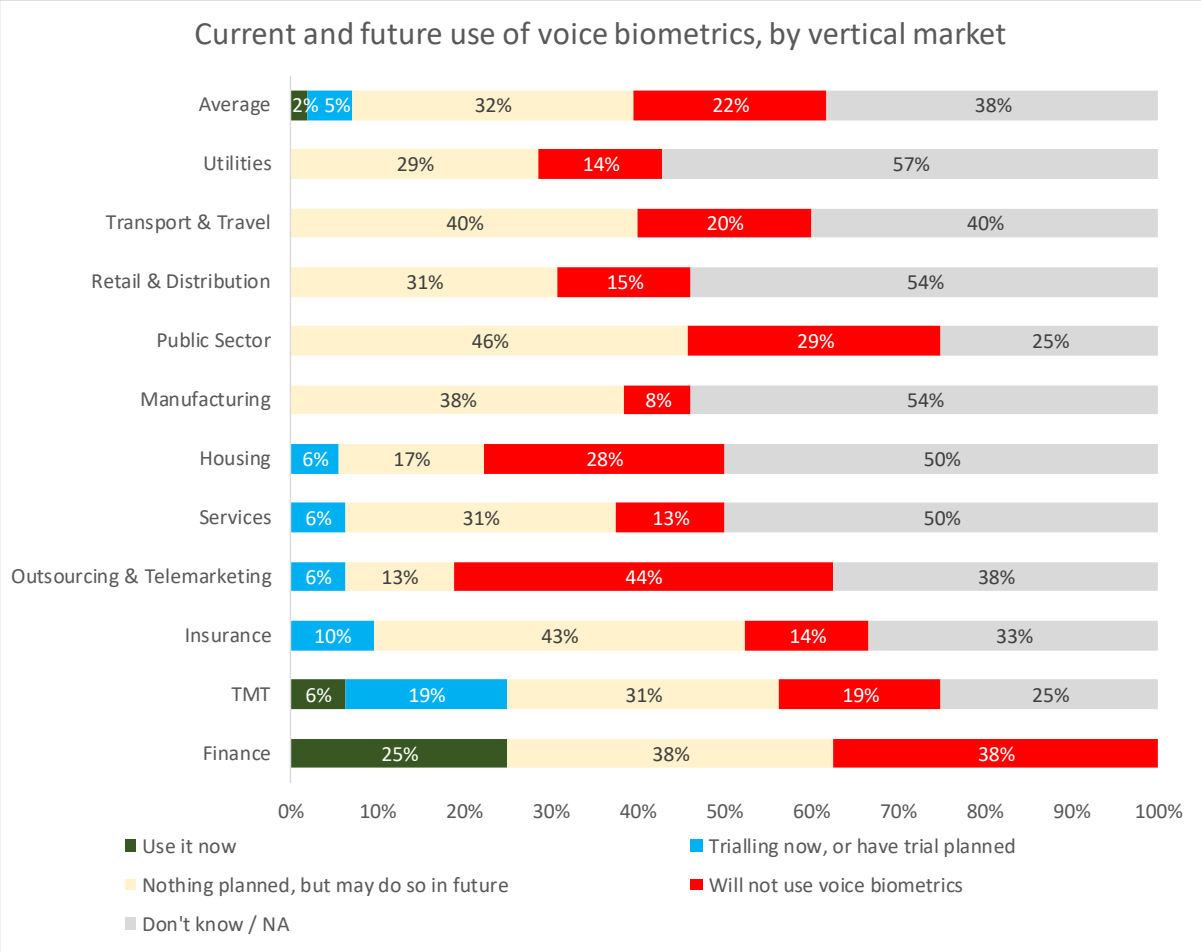
PLANNED AND CURRENT USE OF VOICE BIOMETRICS

The interest in using voice biometrics for customer authentication is tipped more towards larger operations, which are more likely to have high call volumes, meaning that 40 seconds or more cut from each call would add up to a very considerable saving, without affecting the customer or agent experience negatively.

Finance and TMT respondents have been most likely to look favourably on voice biometrics, and although the argument has certainly not yet been won, there is a very significant increase in interest compared to previous years.

A significant number of respondents from the insurance and TMT sectors are planning trials in the near future, and 25% of this year's finance respondents are actually using voice biometrics.

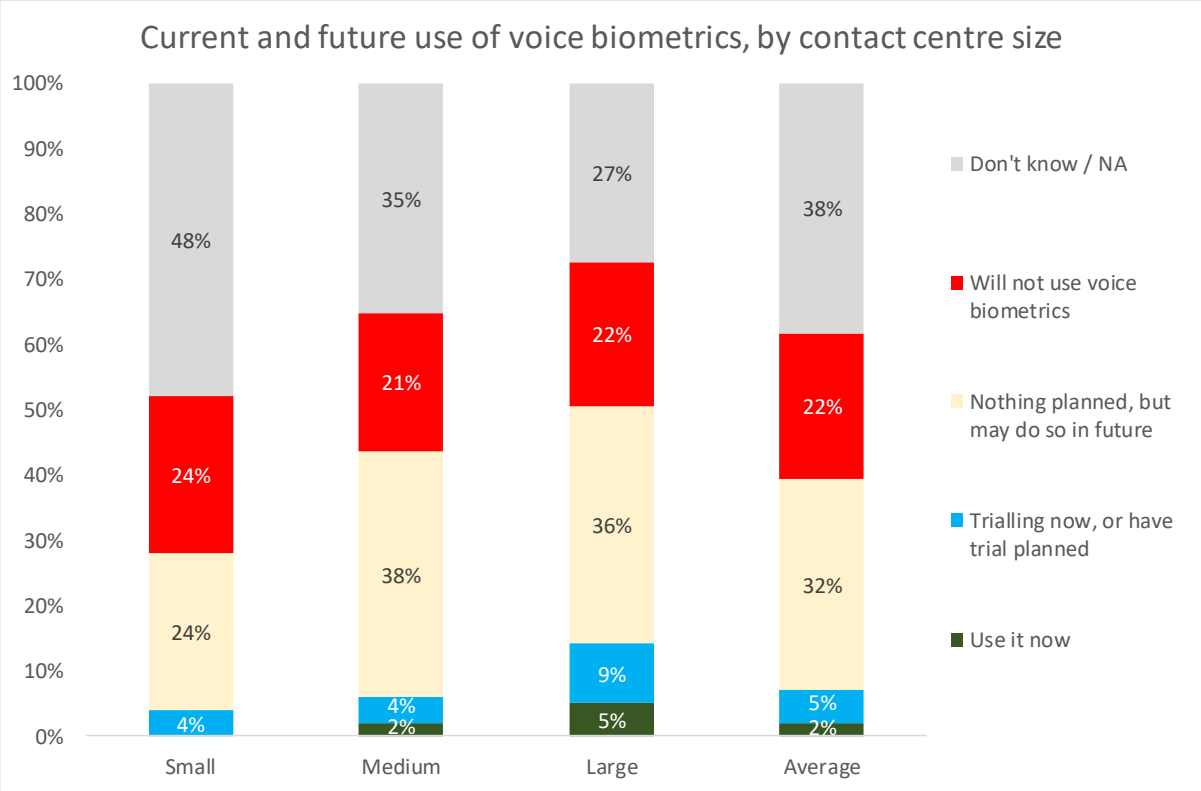
Figure 20: Current and future use of voice biometrics, by vertical market



As would be expected, it is respondents from the largest contact centres, with the greatest call volumes who are most interested in voice biometrics.

Such operations can benefit not just from fraud reduction, but also from the significant cost savings associated with secure customer authentication on a large scale.

Figure 21: Current and future use of voice biometrics, by contact centre size



INHIBITORS TO VOICE BIOMETRICS

When survey respondents were asked, the main inhibitor 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 will likely be applicable to 50% or less of customers and that a majority of customers will never be enrolled, leaving them vulnerable to fraud attacks. There is also the risk of the initial enrolment itself being fraudulent.

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.

Voice biometrics can be a useful tool, especially for larger contact centres through cutting call lengths and costs, and improving customer experience. However, it may not always be enough against a fraudulent attack or series of attacks.

Solutions that focus on identifying potential fraudulent callers don't rely solely on matching the voiceprint, which is not an infallible method of authentication, as can be seen below. Using biometrics in association with other security measures, such as 'phoneprinting' or call signalling analysis.

Biometric security fooled by twin's voice

In May 2017, the BBC carried a story[12] about an experiment that a BBC reporter and his twin had tried on a UK bank. The reporter had enrolled in a bank's voice identification system, but his twin was able to access the account after ringing the bank and pretending to be his brother.

The security breach did not allow the twin to withdraw money, but he was given access to some of the account's functionality. The twin took eight attempts to access the account, which is a failing in the implementation process rather than the technology – most typed passwords will allow perhaps three failures before the user is locked out.

Experts stated that although each voice is unique, if the system has been implemented to allow too much leeway when detecting some of the 100+ characteristics of the voice, then it would not take an exact voiceprint match to access the account.

The expert noted that if the voiceprint was hacked or copied, the genuine account holder would not have the option to change their voice like they would change their password.

Voice replication software was also noted to be becoming increasingly sophisticated, and the general feeling was that alternative methods of security would be required alongside voice biometrics.

[12] http://www.bbc.co.uk/news/technology-39965545

CALL SIGNALLING ANALYSIS & 'PHONEPRINTING'

An alternative – or rather, additional method of customer identity verification is 'phoneprinting' or call signalling analysis, which is perhaps 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), CLI (the calling number), 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 CLI may be collected from the call at carrier-level compared to the presentation CLI - 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 CLI
- network CLI
- 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 recognised, 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. CLI 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, meta data 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 - despite 60% of forthcoming through the phone 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. The solution provider takes the audio recordings identifies the 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 optimise the voiceprint so that they are more likely to be identified correctly in future.

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.

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.

We help the biggest and most successful vendors develop their contact centre strategies and talk to the right prospects. We have shown the UK government how the global contact centre industry will develop and change. We help contact centres compare themselves to their closest competitors so they can understand what they are doing well and what needs to improve.

If you have a question about your company's place in the contact centre industry, perhaps we can help you.

Email: info@contactbabel.com

Website: www.contactbabel.com

Telephone: +44 (0)191 271 5269