CONTACTBABEL

The UK Contact Centre Decision-Maker's Guide 2018-19

(16th edition)

The PCI Compliance & Card Security Chapter

Sponsored by

ENCODED

secure automated payments

"The 2018-19 UK Contact Centre Decision-Makers' Guide (16th edition)"

ENCODED
secure automated payments

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
- Virtual Terminal Payments
- Web Payments

Contact: Robert Crutchington

t: + 44 (0)1293 229 700

e: sales@encoded.co.uk

w: www.encoded.co.uk

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

ENCODED
secure automated payments

Encoded's Customer Engagement Platform

Make it easier for customers to pay via Instant Messaging

A secure, reliable, cost-effective solution

Instant Messaging is widely accepted as a non-intrusive, convenient method of communication. Using Encoded's highly secure Customer Engagement Platform your customers can make payments by simply replying with the word 'pay'.

The new payment solution:

- Streamlines your payment process
- Frees your agents from chasing late or non-payments by telephone
- Works with other Encoded payment services
- Aids PCI DSS and GDPR compliance
- Operates over SMS, voice, email, Facebook Messenger and many other messaging platforms

Agent Assisted

IVR payments

Mobile App

SMS Chat

Web payments

And there's more...

You can use the customer engagement platform to:

- Promote the use of other online services
- Broadcast the release of your latest mobile App
- Invite customers to download your latest PDF

To learn more about how the Customer Engagement Platform can reduce levels of debt, make it easier for your customers to pay and to keep them updated watch the **movie here.**

Keep it simple – Keep it secure

Talk to Encoded to discover a more engaging and cost-effective route to payments

Encoded is a Level 1 PCI DSS Service Provider
For more information on products and services please call 01293 229 700
email sales@encoded.co.uk or visit encoded.co.uk

PCI Compliant
Level 1 PCI-DSS Service Provider

PCI DSS BACKGROUND

The Payment Card Industry Data Security Standard (PCI DSS) is the creation of five of the largest payment card providers: VISA, MasterCard, American Express, Discover and JCB International, which together have named themselves the PCI Security Standards Council (PCI SSC). The council wished to clarify and align their various fraud prevention measures and regulations into a single agreed global framework. PCI DSS provides guidance to merchants as well as payment card processors around how to process, store and transmit information about the payment card and its owner, with the aim of reducing the incidence of card fraud and promoting best practice in information security. Although compliance with PCI DSS is not enforced by law, the card brands may fine those which do not follow its regulations, or even deny the merchant the ability to take card payments at all. At the time of writing (October 2018) , the current standard is PCI DSS 3.2.1, which was released in May 2018 and supersedes version 3.2 which is to be retired at the end of 2018.

There are 12 requirements to fulfil in order to achieve PCI DSS compliance (full details are available here[1]), with many specific sub-requirements within them, although for many businesses a large proportion of them may simply not apply. In version 3 of the standard additional self-assessment questionnaires (SAQs) were introduced to assist merchants and service providers to report the results of their PCI DSS self-assessment.

Depending on the merchant level (i.e. how many card payments are taken), businesses can 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 transactions per year or 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) now available in current PCI DSS standards.

A formal Attestation of Compliance (AOC) which is usually signed by the Financial Director 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. Each card brand provides a list of compliant service providers on its website. 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.

The vast majority of contact centres do not require a full audit, and self-assessment questionnaires are becoming far more popular. The PCI DSS 3.0 standard introduced a number of different types of SAQ, 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.

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

SELF-ASSESSMENT QUESTIONNAIRES (SAQS)

SAQs have become channel-related, rather than merchant-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.

SAQ-A is relevant to card-not-present merchants (including contact centres) who have outsourced all cardholder data functions to a 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.

However, this method of handling card payments risks cutting out those customers who are unable to complete card payments via touchtone (i.e. relevant in contact centres using DTMF suppression) and 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 CVV code), 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.

SAQ-C-VT is an alternative option for those contact centre operations that wish to offer a manual payment service for customers unable or unwilling to use a keypad to enter their card information. While there are more requirements to complete within this SAQ, organisations should consider the overall ongoing cost and effort involved in implementing the technology and processes required for each SAQ to be completed successfully, as well as how to deal with customer exceptions. Completing SAQ C-VT successfully will involve encrypting card details in transit, training staff in data protection, and making sure that no card details are recorded, but does give the option of manually taking card payment details over the phone.

It is important for businesses to understand that there is no single right way of handling card payments. 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.

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.

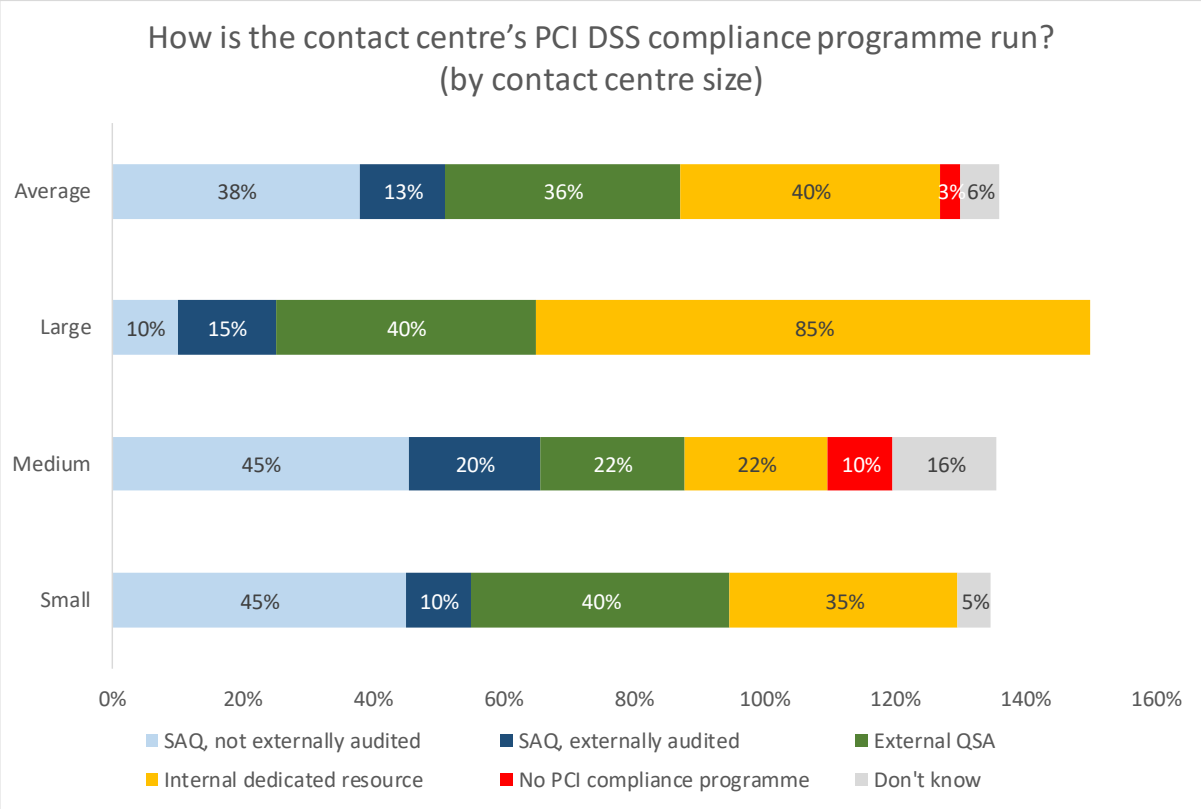
Proving compliance is also about understanding which parts of the business fall into the scope of the PCI compliance audit. It is important that whoever runs the PCI compliance programme, whether internal or external, is experienced in interpreting it fully. QSAs should look at intent and risk - what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

12% of small operations and 15% of medium-sized operations state that they have no PCI compliance programme at all, which is a concern.

Small operations are most likely to use self-assessment questionnaires, quite evenly split between externally audited and internal-only. Larger operations are more likely to use dedicated internal resource and/or an external Qualified Security Assessor (QSA).

Neither SAQ-A or SAQ-C-VT require an external audit.

Figure 1: 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.

PCI DSS REQUIREMENTS

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. It is generally considered that Requirements 3, 4 and 12 may have the greatest relevance. It should also be noted that sections 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 such as the card verification code 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 there is an increased use of RAM scrapers, which is 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.

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

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 regulations, 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 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 various elements of card data may be handled in different ways.

Figure 2: Data elements and storage in PCI DSS

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

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

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

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

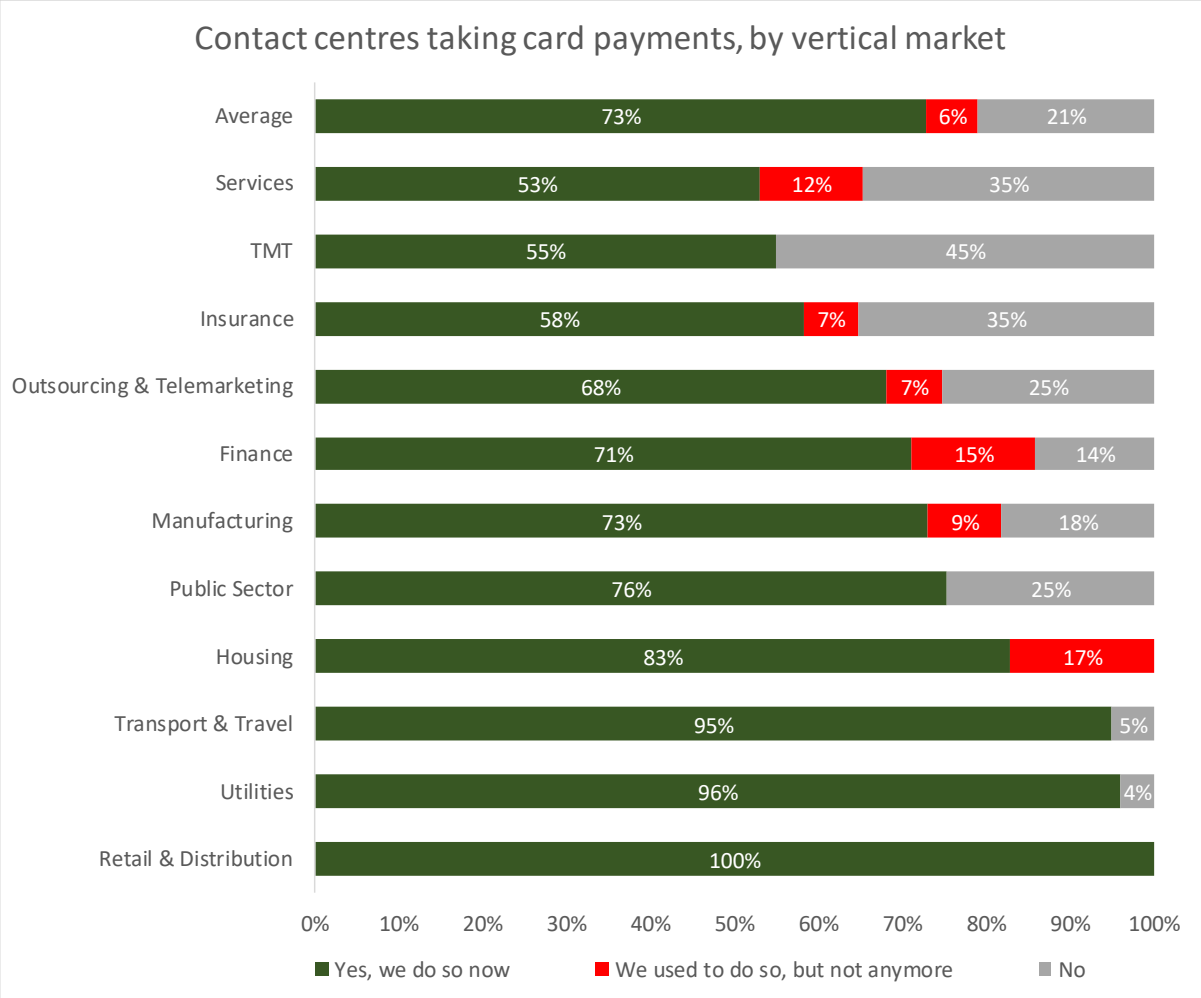
THE USE OF PAYMENT CARDS IN THE CONTACT CENTRE

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 6% of respondents no longer doing so. This is especially the case for respondents from the housing, finance and services sectors.

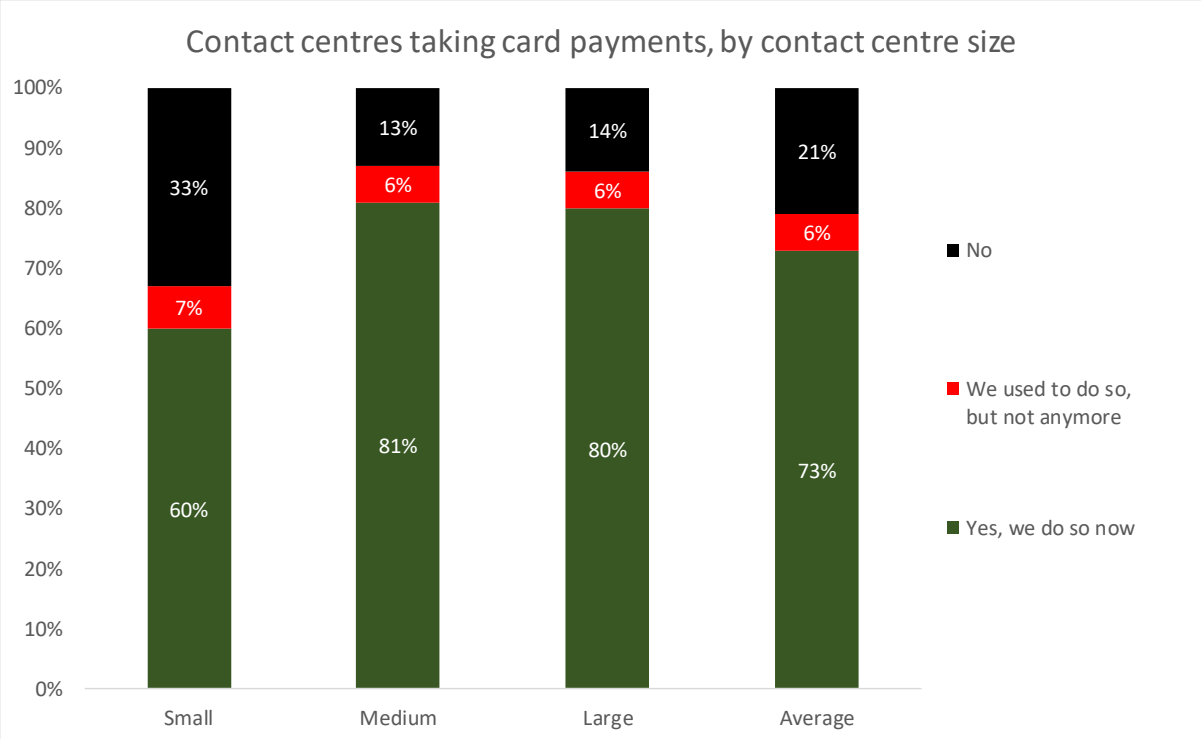
Although the survey does not ask for the specific reasons why card payments are no longer taken, it is unlikely to be the case that customers now prefer to pay via other methods. More likely, the increasing requirements and costs associated with more stringent payment technology, processes and training 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 3: Contact centres taking card payments, by vertical market



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 4: Contact centres taking card payments, by contact centre size

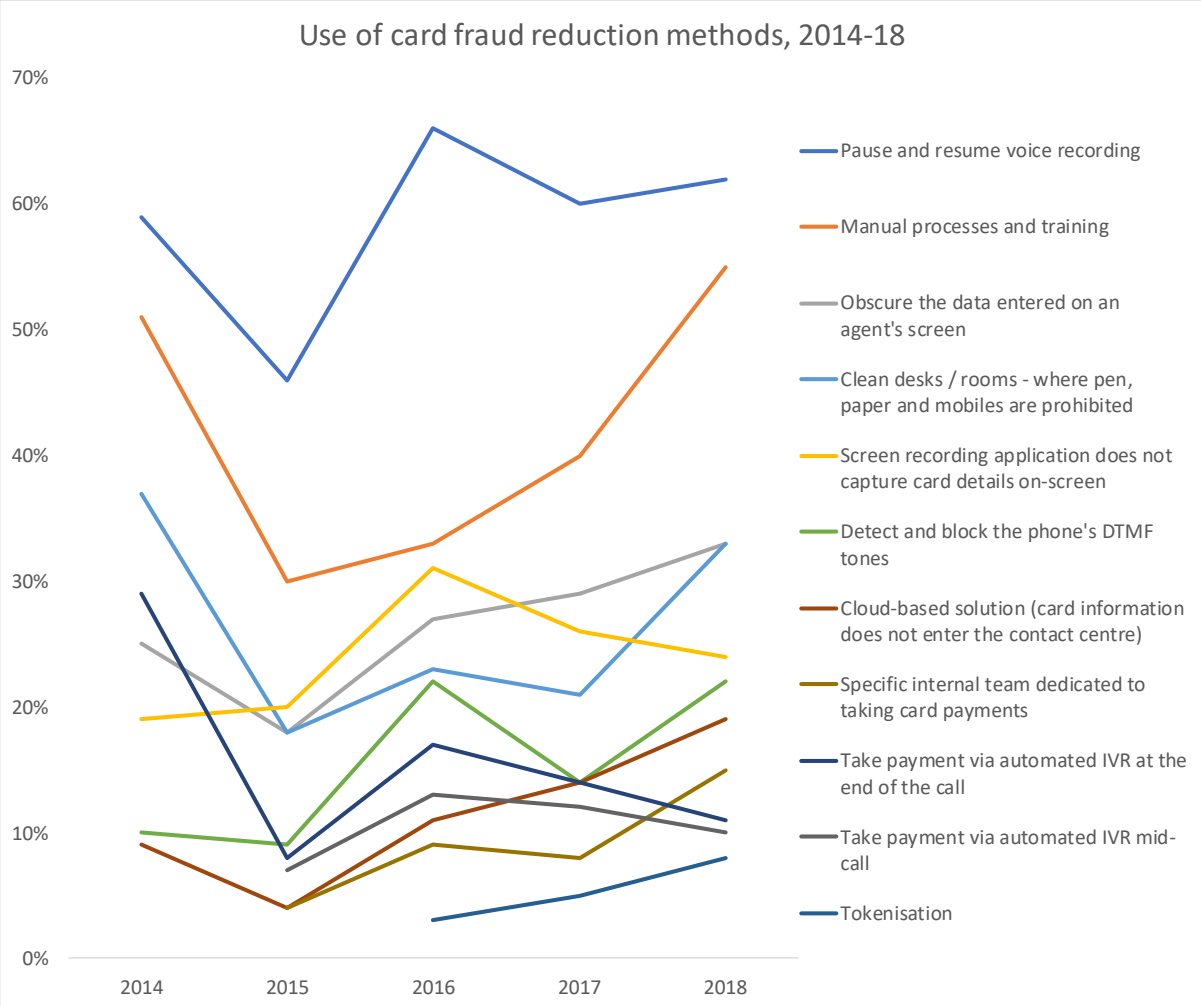


THE USE OF CARD FRAUD REDUCTION METHODS

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 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 5: Use of card fraud reduction methods, 2014-18



ENCODED
secure automated payments

Think security not just compliance

Robert Crutchington at Encoded shares 3 Tips for contact centres

The payment industry is changing. While contact centres have been grappling with issues such as PCI DSS compliance and data security, particularly with recent GDPR regulation, new challenges are now emerging. More tech disruption is on the way as blockchain and crypto currencies gain ground.

The payment industry players are already heavy investors in this area and it will ultimately threaten the existing four party card payment model i.e. that of the card holder, the card issuing bank, retailer and retailer's bank. With this more volatile environment on the horizon in terms of payments, contact centres need to start to think more about security, not just PCI DSS compliance.

Focus on Data Security

With an ICO report[i] claiming "Accidental disclosure or human error is a leading cause of breaches of personal data", it makes sense for contact centres to review how they take payments and deal with customer data. While agents handling transactions still play a key part, there are other methods that offer faster and more secure payments, such as automated payments and tokenisation, which is widely used to take repeat card payments with encryption.

Customers are increasingly choosing to pay using their mobile devices, which means offering secure payment has never been more important. Instant Messaging is now widely accepted as a non-intrusive and convenient method of communication and has risen in customer preferences as a method to pay while on the move.

So what does this mean for contact centres? In last year's ContactBabel Decision Makers Guide 53%[ii] of contact centre respondents survey stated that they offer mobile functionality for customer service, with a further 26% with plans to do so.

Three tips when thinking security

Offering different payment options means checking every possible area of security exposure in the process. Here's a quick checklist to help navigate the options when thinking security:

1. **Look outside for solutions –** don't try and go it alone start talking to third parties with the relevant certifications and experience. Choosing a PCI DSS Level 1 payment services provider that is Data Protection Act compliant helps tick two boxes and gives reassurance that they are already adhering to security standards.

2. **Utilise the latest mobile services functionality –** enabling customers to make payments via Instant Messaging streamlines the payment process and has benefits for contact centres - by allowing mobile payments outstanding debt levels can be controlled and agents spend less time chasing missed or non-payments and can therefore focus on more positive revenue generating activities.

   As an example, Encoded's Customer Engagement platform works with other Encoded payment services, which means if a customer has stored card details previously, payment can be taken immediately, with a simple text. Plus, the platform enables customers to be updated of product promotions and account balances, while comprehensive reports provide details of all interactions.

3. **Widen your scope –** as well as ensuring compliance, a third party Payment Service Provider can help look at your whole eco system and not just the implications of compliance, to put the right security infrastructure, polices and processes into action.

When it comes to taking customer payments, now is the time to take security seriously to give your customers confidence in your contact centre operations, safeguarding both their details and your business from cyber theft.

[i] Data protection - A practical guide to IT security, 6 January 2016
[ii] The UK Contact Centre Decision-Makers' Guide (15th edition - 2017-18) www.contactbabel.com/reports.cfm

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

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

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. Pause and resume may be agent-initiated, act for a fixed time period (e.g. stopping recording for a minute), or be fully automated. The PCI DSS standard is interpreted as preferring automation over manual intervention to avoid human error. Automated pause and resume may use an API or desktop analytics to link the recording solution to the agent desktop or CRM application, being triggered when agent navigates to a payment screen, for example. The recording may then be paused, to be resumed at the time when the agent leaves the payment screen, which in theory should remove the period of time whereby the customer is reading out the card details. This method, consistently the most popular, has several obvious benefits, not least of which include a very low set-up cost and the speed of implementation. However, breaking a recording into two parts makes it difficult to analyse the entire interaction, and goes against some industry-specific regulations, e.g. any financial services regulations which require a record of the full conversation, so some contact centres prefer to mute the recording or play a continuous audio tone to the recording system while payment details are being collected, meaning that there is still a single call recording which can be used for QA and compliance purposes. This principle is similar to that applied to **screen recording** applications, where 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 copies being made.

Improving Manual Processes and Agent Training (55%)

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

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

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

A minority of respondents, especially those with a large contact centres, using automated IVR process to take card details from the customer, cutting the agent risk out of the loop entirely. Mid-call IVR (or agent-assisted IVR) is seen as a more customer-friendly approach than post-call IVR: the caller may have additional questions or the requirement for reassurance and confirmation after the payment process, perhaps around delivery times or other queries not related to the payment process. However, the card data is still within the organisation's network, so although this approach takes the agent out of scope, it does not in itself ensure PCI compliance.

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

22% of this year's respondents use DTMF suppression 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.

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 intercept card data at the network level means that no cardholder data is passed into the contact centre environment, whether infrastructure, agents or storage. As such, this 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.

Tokenisation (8%)

In this discussion, the practice of **tokenisation** should also be mentioned, although it is used in only 8% of respondents' operations. Tokenisation takes place in order to protect sensitive card information such as the PAN (primary account number or 'long card number') by replacing it with non-sensitive data which merely represents the initial data. The purpose of this is to devalue the data so that even if it is hacked or stolen, it is of no use to a criminal. One of the main benefits to tokenisation is that it requires little change to the existing environment or business processes, as apart from the addition of a decoding mechanism, the flow of data, its capture and processing works in the same way as if it were true card information coming into the contact centre environment.

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

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

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

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

Of course, cardholder data is not the only DTMF-provided information coming into the contact centre environment, as other data such as IVR routing options and the entry of account numbers often requires capture of DTMF tones as well. Various configuration options exist within solutions, based upon the specifics of the business in order to circumvent confusion. Customers should check that any hosted tokenisation solution will not alter the performance of any required card number validation checks, including card length, range validation and 'Luhn' checks (to make sure a card number 'looks right' before presenting it to the payment services provider). The PCI SSC has published tokenisation product security guidelines[2].

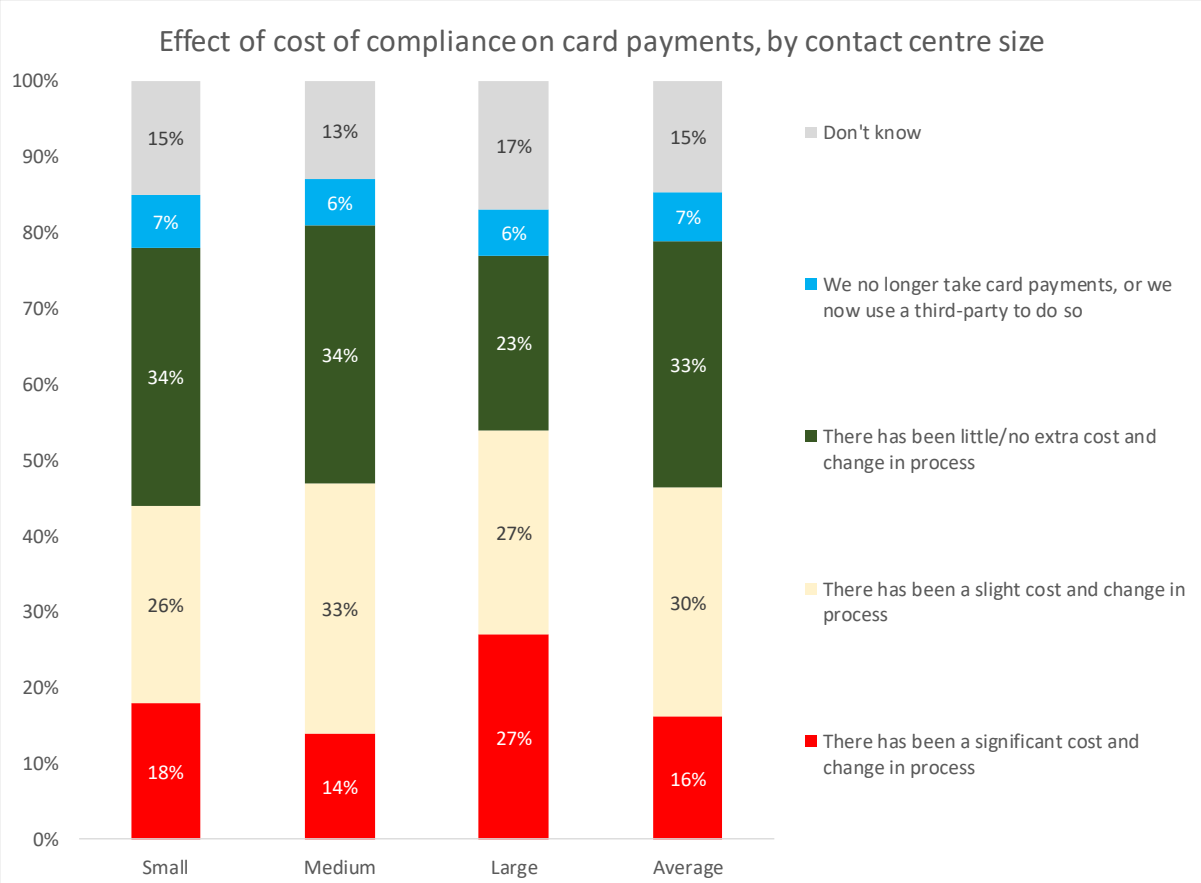
[2] https://www.pcisecuritystandards.org/pdfs/15_04_02%20PCI%20Tokenization%20Product%20Security%20Guidelines_Final%20Press%20Release.pdf

THE COST OF PCI DSS COMPLIANCE

The following chart shows that a significant proportion of contact centres have found that the cost of PCI DSS compliance is very considerable, with 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. 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.

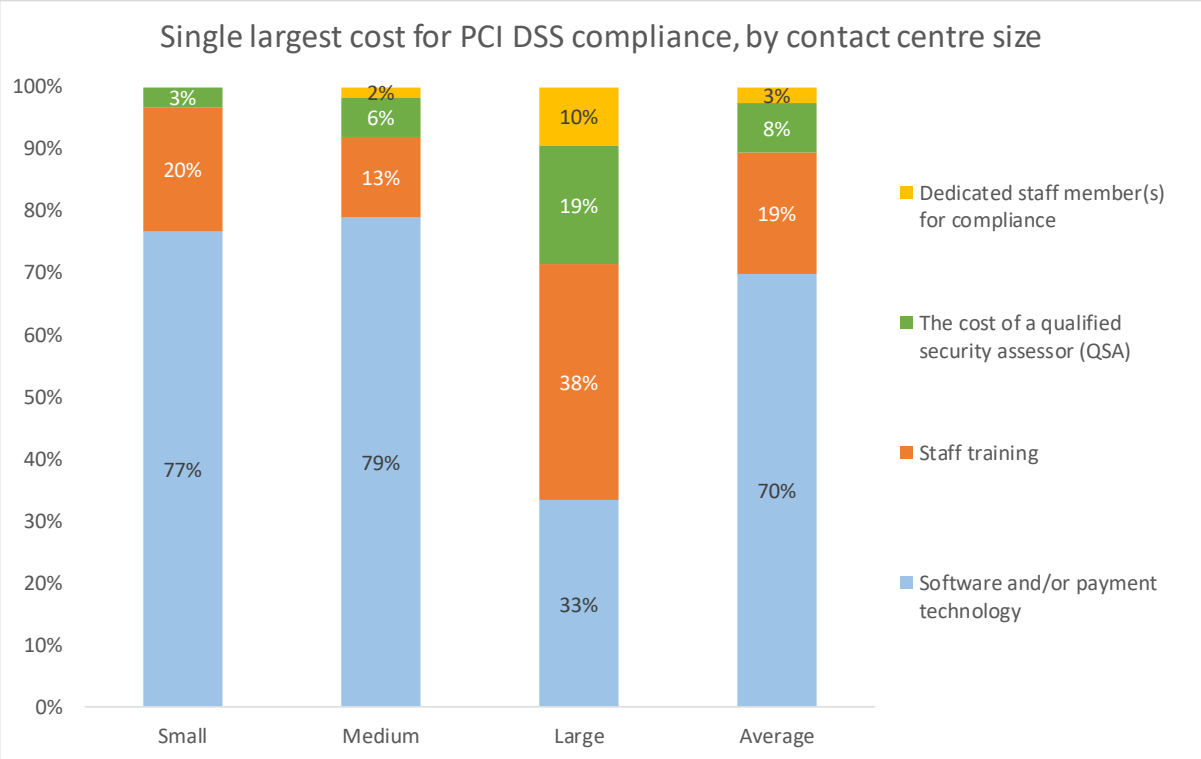
Figure 6: Effect of cost of compliance on card payments, by contact centre size



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

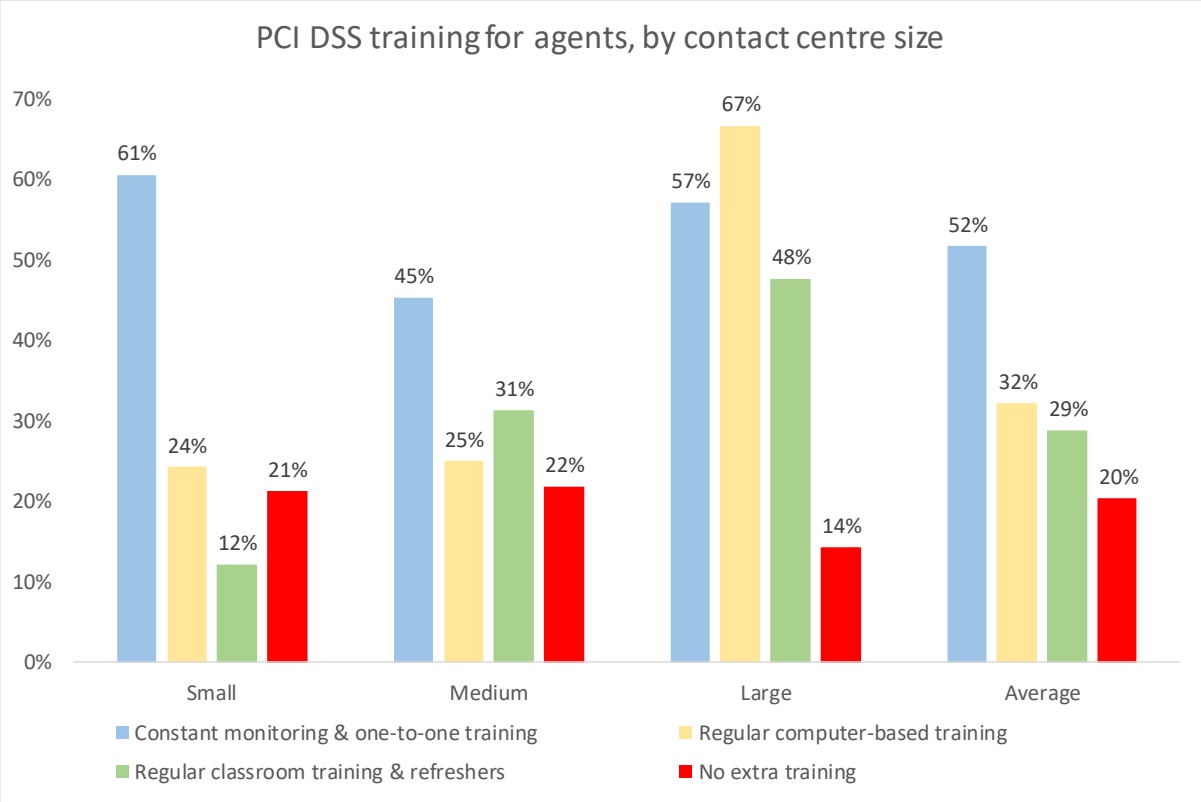


The cost of staff training is reported to be a major drain on resources for large contact centres in particular, and the following chart shows that such operations are providing higher levels of both computer-based and classroom-based training for their agents than is the case in small and medium-size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

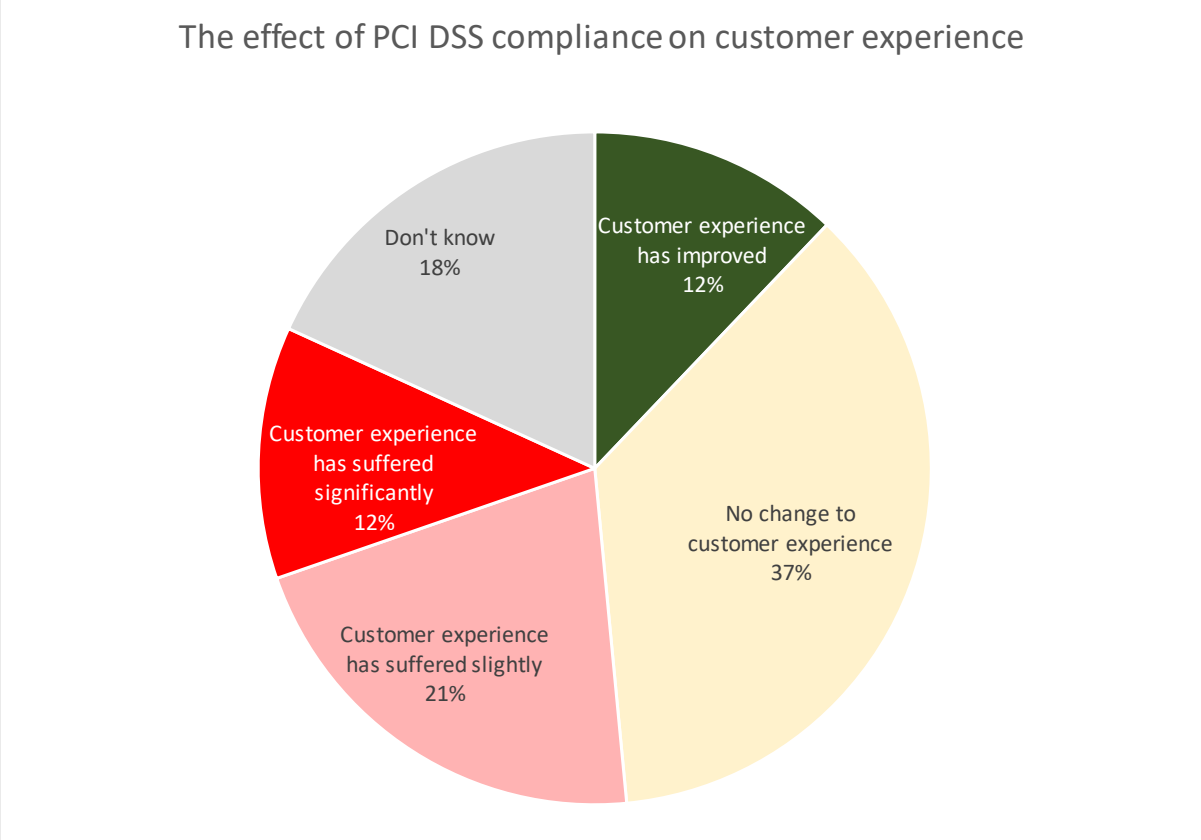


Many PCI DSS compliance and card fraud reduction methods are likely to have an impact upon the customer, in terms of increased effort or inconvenience (e.g. having to type in a card number can be awkward if using a smartphone, as navigation through screens will be required while holding the phone away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

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

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.

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



ABOUT CONTACTBABEL

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

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

To download the full "2018-19 UK Contact Centre Decision-Makers' Guide", free of charge, please visit www.contactbabel.com