CONTACTBABEL

The US Contact Center Decision-Makers' Guide 2019-20

The PCI Compliance & Card Fraud Reduction Chapter

Sponsored by

pcipal®

"The 2019-20 US Contact Center Decision-Makers' Guide (12th edition)"

PCI ASSURANCE FOR THE INSURANCE INDUSTRY

Verex Group has taken steps to not only secure sensitive payment data and comply with PCI DSS rules, but to provide a quality experience for their customers.

THE CHALLENGE

Who is the Verex Group? With 70+ contact center agents located across two sites in the UK, along with several remote home-based workers, Verex handles more than 300 telephone-based payment transactions every day. A mid-call Interactive Voice Response (IVR) system was previously deployed, there was however several issues arising from this method that needed to be addressed, as Jack Davis, Salesforce & Omnichannel Development Manager for Verex Group explains: "We were finding that a high percentage of callers would drop out of the payment process; between 20% and 30% of payments by phone would fail at the first attempt. A key issue was that if a customer had a query or inputted their card details incorrectly, there was no way of them communicating with us at the time, so they would drop off the call and, hopefully, try again.

"Not only did this mean high failure rates, but it also meant that if the customer called back, there was no guarantee that they would speak with the same agent. As our agents are rewarded for successful customer outcomes upon completion of each transaction they personally handle, this was a major frustration for our team. We needed to identify an assisted mid-call solution that would overcome this problem, while also ensuring we remain PCI DSS Compliant in the way our customers' payment details are handled."

THE SOLUTION

NewVoiceMedia, which handles the contact center telephony solutions for Verex, recommended PCI Pal's Agent Assist solution - a true cloud secure payments solution that is fully integrated with NewVoiceMedia.

Originally the team assessed three solutions; an alternative mid-call solution, PCI Pal's Agent Assist and a 'pause and resume' option. Confirms Jack, "The assisted option was the best as it would enable us to provide a personalised approach on every customer interaction. With Pause and Resume, there's a huge reliance on staff to get this right as if they forget to pause, we're in breach. Also, if they forget to un-pause and we haven't recorded the terms and conditions being read for example, and there's a claim, we don't want to be hit with a £1M claim as this wasn't recorded! We operate in a highly regulated industry and so it's vital that we're on top of our game here; we felt PCI Pal's solution removes this issue for us completely."

Instead, Agent Assist appealed to Verex as it would allow them to take card payments securely while the agent and customer remained in conversation. With no call transfers required, the customer inputs their card details using their keypad. If assistance is needed, the agent is there to help, meaning fewer dropped calls, faster transactions and greater service continuity.

It also means that no card details are verbally provided, so the threat of potential insider frauds is not present.

Once the customer has provided their details, the agent simply presses the 'process card' payment button and it instructs the PCI Pal solution to send the transaction to the payment provider for processing. No card details are seen or heard by the agent, and no data enters Verex's infrastructure, reducing the scope of PCI DSS compliance.

THE RESULTS

With data security high on the agenda for Verex, payment card security is assured thanks to Agent Assist.

Confirms Jack, "Since launching Agent Assist we have seen call drop-out rates fall from up to 30% to just one or two per cent. Now, agents can interact directly with customers and so the points of failure are far less. They are there to hand-hold customers through the experience, whereas before if a customer mistyped their details or were unsure about something they had to start again, which was frustrating for them and our agents."

Tom Bowen, a Senior Database Architect for Verex, adds "There's certainly less margin for error and since Agent Assist went live. We're faster at processing payments and so on average we've seen our calls reduce, on average, by at least 30 seconds, which adds up when you're working with the volumes that we do."

Explains Jack, "All agents have said they prefer the new system; it's improved their efficiency, they haven't had to dramatically change the way they work."

Concludes Jack, "The process of buying a policy is now easier, so customers are less likely to drop out. Ultimately, our agents prefer it, our customers prefer it and we are seeing a big jump in efficiencies all round."

To discuss your own compliance requirements, get in touch:

info@pcipal.com +1 866 645 2903 www.pcipal.com

Our mission at PCI Pal is to safeguard reputation and trust by providing our customers with secure Cardholder Not Present payment solutions for contact centres and businesses.

Our globally accessible cloud platform enables secure payments without bringing organisations into scope of PCI DSS and relevant security rules and regulations.

With the entire product portfolio served from the cloud, integrations with existing telephony, payment, and desktop environments are flexible, ensuring no degradation of service while achieving security and compliance.

Contact:

e: ava.kammer@pcipal.com

w: www.pcipal.com

LinkedIn

Twitter

t - US: +1 866 645 2903

t - UK: +44 330 131 0330

PCI DSS BACKGROUND

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

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

Compliance to the PCI DSS is a contractual obligation by the Merchant to either the scheme or the acquirer (in the UK, to the acquirer; in the US to individual schemes and/or acquirer). Penalties are levied by the schemes in the event of a data breach, and may even deny the merchant the ability to take card payments at all. At the time of writing (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 organization that they represent meets the requirements of the standard. Third Party Service Providers (included hosted contact center 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 organizations, 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 organization. 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 organization has not also considered their PCI compliance status but also the compliance status of Third Party Service Providers supporting their card payments process.

PCI DSS REQUIREMENTS

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.

- 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.

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

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

- 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 centers 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 center 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 minimizing the holding of any unnecessary data as well as reducing the value of any stored payment card information. Data must only be stored if necessary, and if stored must be strongly encrypted, and only kept for the period where it is actually needed, with a formal disposal procedure. Businesses should revisit the necessity of data storage on an ongoing basis, and it should be remembered that the storage of sensitive authentication data 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 centers, 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.

Organizations 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 centers 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 center 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 program 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 centers, 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 minimization 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 defense, go at least as far as the original requirement and not negatively impact upon other PCI DSS requirements.

Potential danger points within the contact center 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 emphasized 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.[2]"

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 center). The supplement also explains the processes whereby an organization 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 organization, so any third-party used must themselves be confirmed to be PCI compliant.

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

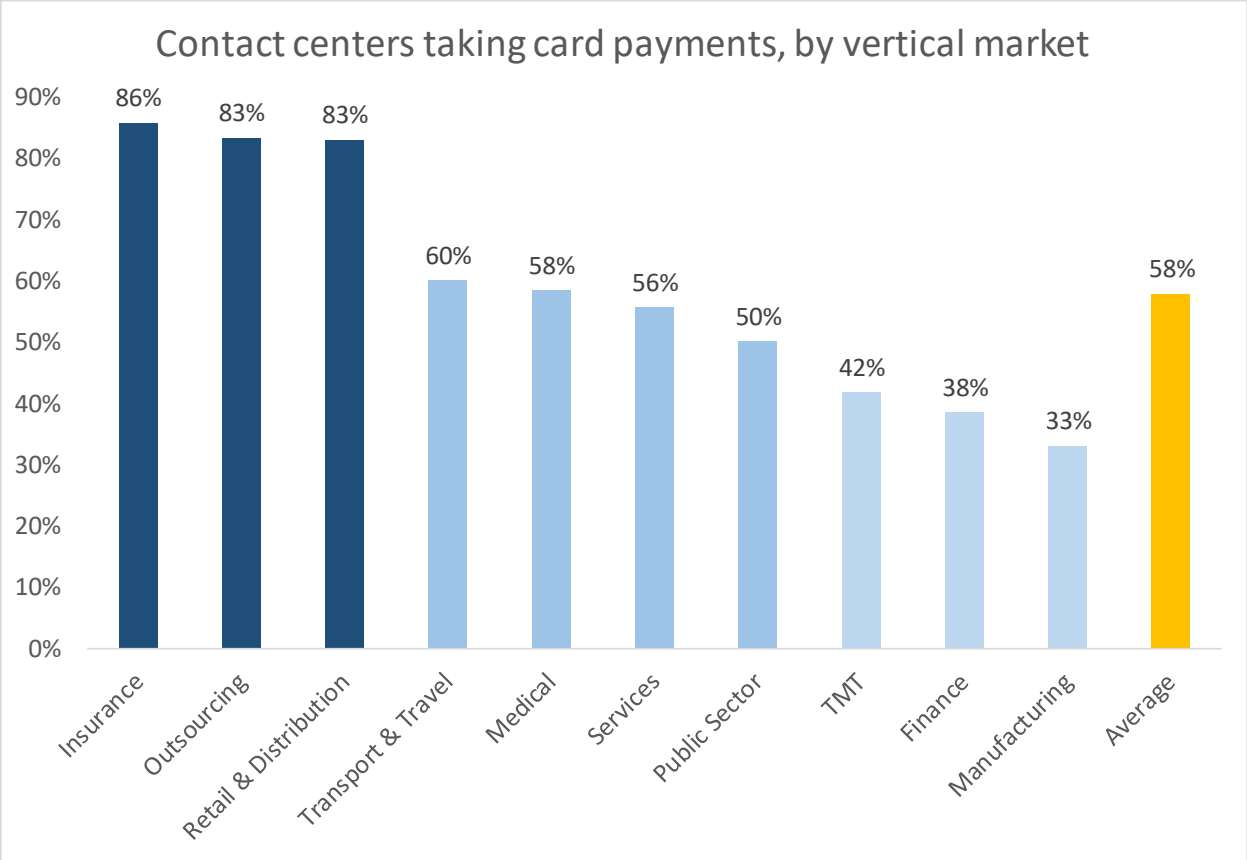
For those organizations which handle customer card data themselves, the various elements of card data are permitted to be processed and stored in different ways.

Figure 1: 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

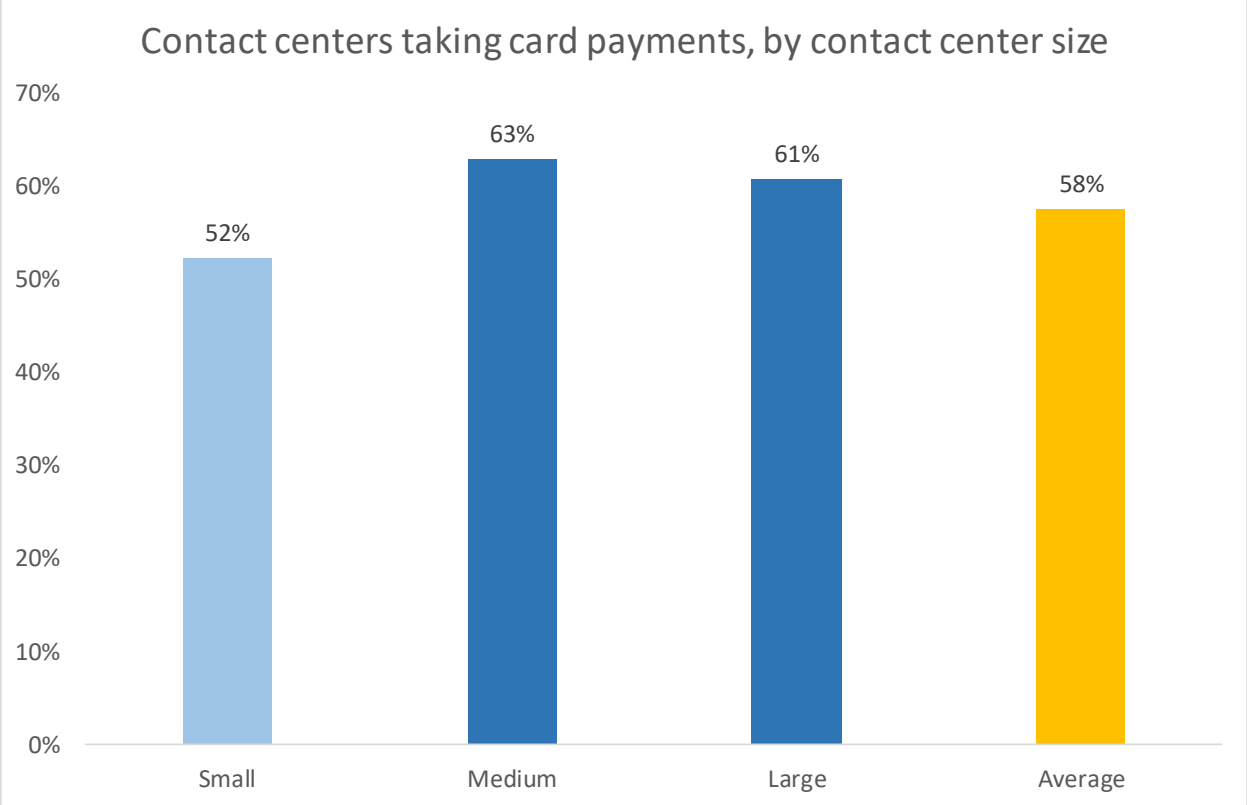
The proportion of respondents taking card payments has dropped from 56% in 2017 to 51% in 2018. While this may simply be a result of asking different survey respondents, there is some evidence from other ContactBabel research that the increasing requirements and costs associated with more stringent payment technology, processes and training outweigh the benefits of being able to take card payments over the phone.

Figure 2: Contact centers taking card payments, by vertical market



While the usual positive correlation between size and card payment is again present this year (albeit very slightly), it is noticeable that there is a drop in the figure of the largest operations which offer this facility to their customers (down from 66% in 2017 to 54% in 2018), suggesting that the cost and effort of implementing a PCI DSS compliant environment is greater than the potential benefits of being able to take card payments. Charts later in this chapter show that some large operations have in fact stopped taking card payments over the phone.

Figure 3: Contact centers taking card payments, by contact center size



Five ways contact centers can secure incoming payments

Author: Geoff Forsyth, CISO, PCI Pal

In today's modern world, significant data breaches are sadly all too common.

Since GDPR has been enforced, organizations' overall focus on data protection practices has sharpened, yet breaches are continuing to happen. Of course, the jewel of every hacker's crown is access not only to contact data but sensitive payment information such as credit and debit card numbers.

With 72 percent of contact centers accepting card payments over the phone, it is more important than ever before to standardize payment processes and secure sensitive payment data that is shared over voice channels to reduce the security risk.

Here are five tips to consider on securing incoming payments that are handled in the contact center environment:

1. Descope Your Contact Center

Payment card data is the ultimate prize for hackers, so the first step is to identify how to stop your organization from being on a target list in the first place. Rather than trying to keep hackers out, instead focus on encrypting your data and, where possible, ensure there is no data for them to take in the first place.

If de-scoping technologies are used for payments handled via a contact center, sensitive data never enters the enterprise and therefore the risk is removed.

It also means your organization is compliant with the Payment Card Industry Data Security Standard (PCI DSS), which ultimately improves the ongoing security of all telephone, IVR, web and SMS financial transactions.

2. Remove outdated 'Pause-and-Resume' Controls

In a whitepaper we produced with Verizon that examined contact center challenges in achieving sustainable PCI DSS compliance, we found that 60 percent of organizations are still using outdated 'pause-and-resume' technologies to avoid storing sensitive data on telephone call recordings.

Instead, switch to using modern Dual Tone Multi Frequency (DTMF) masking technology; it prevents contact center agents from handling any payment card data, improves the overall customer experience as the agent can continue speaking with the customer, and data cannot be compromised.

3. Utilize Cloud services to help comply with PCI DSS

PCI DSS compliance can be simpler with advanced cloud-based applications; by opting for PCI compliance solutions via cloud-based API interfaces, there is no requirement to integrate it into your organization's desktop environment. Instead, with intelligent integrations into existing telephony and payment infrastructures, the process is managed in the cloud, creating no additional IT burden or management, yet achieving improved security and PCI compliance.

4. Assess Your People Processes

According to the PCI Security Standards Council, people typically represent one of the highest risks when it comes to the security of data, whether intentional or accidental. For example, compromises can originate from inside an organization from any person who handles calls or may have access to systems and processes where telephone-based payment transactions are managed. Deploying a secure cloud-based solution, that uses DTMF keypad technology to manage phone-based transactions removes that layer of risk.

5. Review your Training

Ensure your organization regularly incorporates PCI DSS compliance training with contact center operatives, so they understand the importance of data and payment card security at all times. It is vital for staff to understand the implications of a data breach, and the overall impact it can have on an organization's reputation and trust.

Improving Processes and Agent Training (71%)

The most widely-used method of card fraud reduction is that of **improving processes and agent training**: the biggest risk in any organization 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 bigger risk than a rogue staff member writing down card numbers.

The practice of **obscuring card details (37%)** on an agent's screen as they are being typed in is a low-tech way of preventing screenshots of the card data being taken on a smartphone, for example. It can be linked to IVR data input, so that the agent can see that the card details have been entered by the caller, but not be able to see exactly what they are. **Disabling screen recording (28%)** in the card input screen also reduces the risk of card data being hacked, as it is simply not available to be stolen.

Pause and Resume (42%)

'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 could be interpreted as to prefer 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, one of the most popular, has several obvious benefits, not least of which include a low set-up cost and the speed of implementation.

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 analyze 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 centers 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.

Clean Desks / Rooms (35% / 11%)

Some organizations set up **dedicated payment teams (11%)**, 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 underutilized, 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 $3,000 per agent per year to create and maintain a clean room environment. Implementing a clean desk policy in the contact center (rather than a dedicated clean room) will reduce the opportunity for agents to write down card details, but cannot be relied upon to prevent fraud.

IVR Payments (10%)

A minority of respondents, especially those with a large contact centers, 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) (9%)** is more popular than **post-call IVR (7%)**, as it is seen as a more customer-friendly approach: 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.

Detect and Block the Phone's DTMF Tones (8%)

8% of this year's respondents use **DTMF suppression** in order to assist with their PCI compliance. 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 unauthorized 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 neutralized (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. There are anecdotal references made to an average time-saving per call of around 10 seconds if the caller types in their own card details rather than reading them out and having confirmed by an agent.

Third-Party Cloud-Based Payment Solution (22%)

22% of this year's respondents use **third-party cloud-based payment solutions**, which is far more likely to be the case in larger operations. 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 center environment, whether infrastructure, agents or storage. As such, this can be seen to de-scope the entire contact center 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 that present in-house. Some cloud-based solutions may require greater levels of integration or configurations than their on-site equivalents, but most seem to be engineered in such a way as to minimize changes to the contact center systems, processes or agent activities.

Tokenization

In this discussion, the practice of **tokenization** should also be mentioned. Tokenization 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 tokenization 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 center 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 center environment. This allows the contact center 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. Tokenization 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 tokenization 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 tokenized. Card numbers and sensitive authentication data such as card validation codes are replaced as necessary, and the new tokenized DTMF tones are played down the line to the contact center. The actual cardholder data is held temporarily within the hosted environment.

Within the contact center environment, the tokenized DTMF entry 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 tokenized 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 tokenized payment card details, the transaction is sent back to the hosted environment, where the tokenized 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 center 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 tokenization 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 tokenization product security guidelines[3].

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

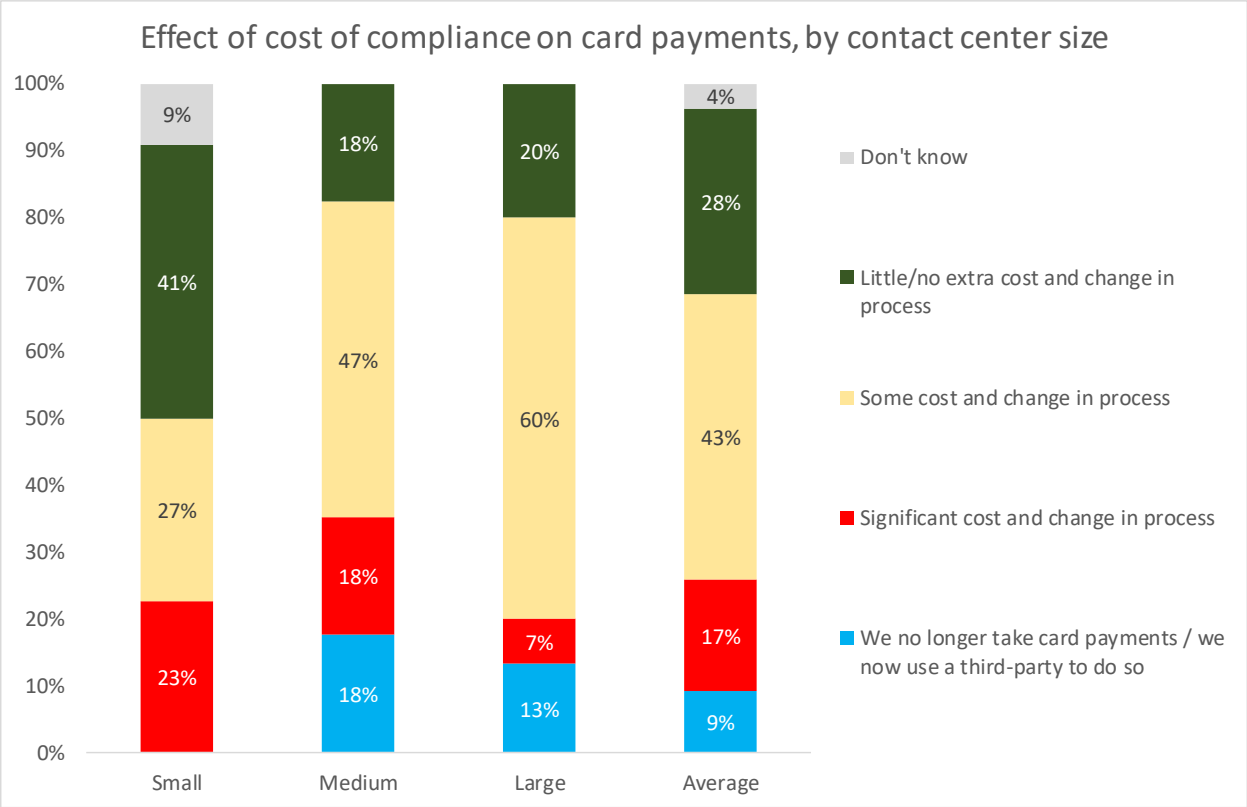
There seems to be an awareness that relying on manual processes and training is not sufficient, and methods such as third-party cloud-based card handling and field masking have definitely grown in use.

Further details about all of these methods, as well as other approaches to take, are investigated in depth in ContactBabel's free report, "The Inner Circle Guide to Fraud Reduction and PCI Compliance in the Contact Center", which is available from www.contactbabel.com.

The following chart shows that a significant proportion of contact centers have found that the cost of PCI DSS compliance is very considerable, with 1 in 6 respondents stating that they have seen a significant cost associated with compliance, particularly in small and medium operations.

Furthermore, a significant proportion of respondents from 50+ seat contact centers state that they either no longer take card payments or use a third-party to do so, in order to take the contact center out of scope. It should be noted that the sample size for this segment was fairly small, so care should be taken when extrapolating, but it is certainly worth attention.

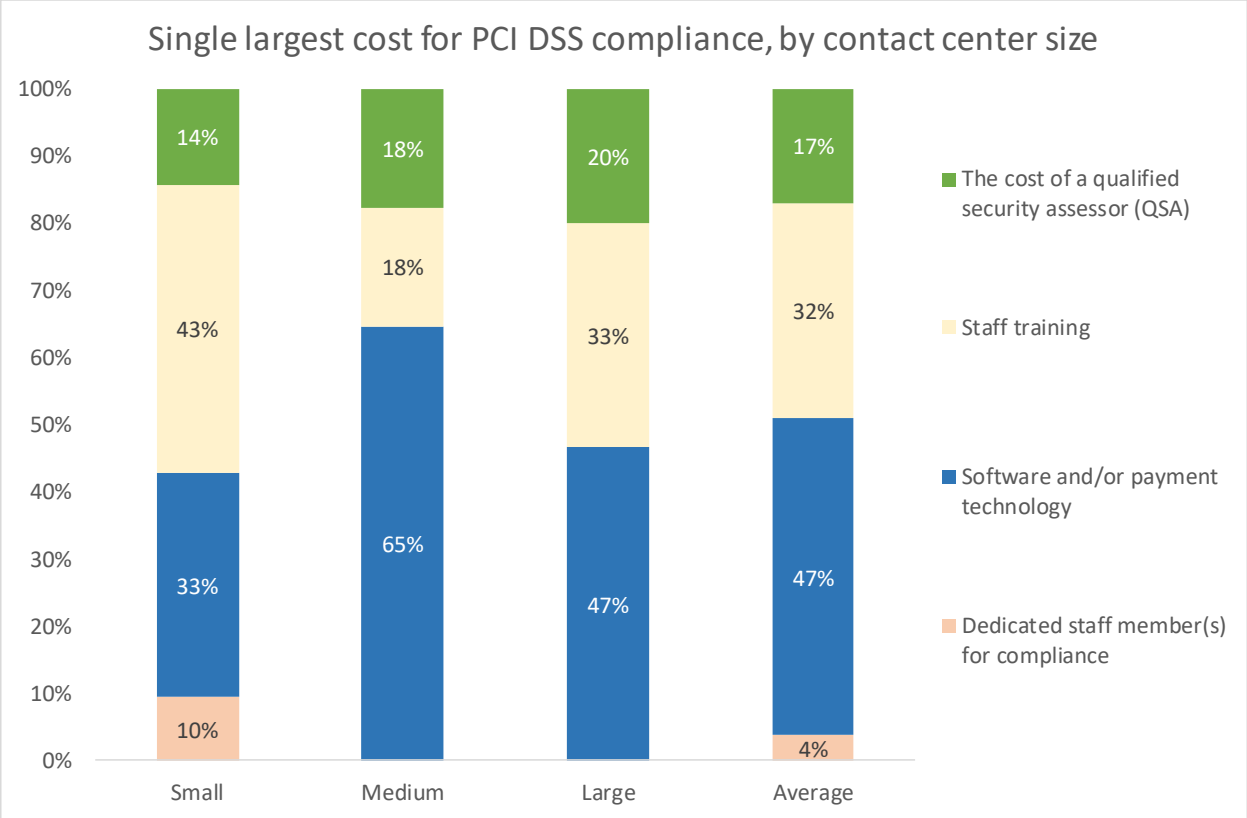
Figure 4: Effect of cost of compliance on card payments, by contact center size



47% 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 medium-sized operations.

In the smallest contact centers, the cost of training staff in card fraud prevention techniques and processes is said to be the largest cost in 43% of cases, with around 1 in 5 medium and large operations noting that the cost of a qualified security assessor (QSA) was considerable.

Figure 5: Single largest cost for PCI DSS compliance, by contact center size



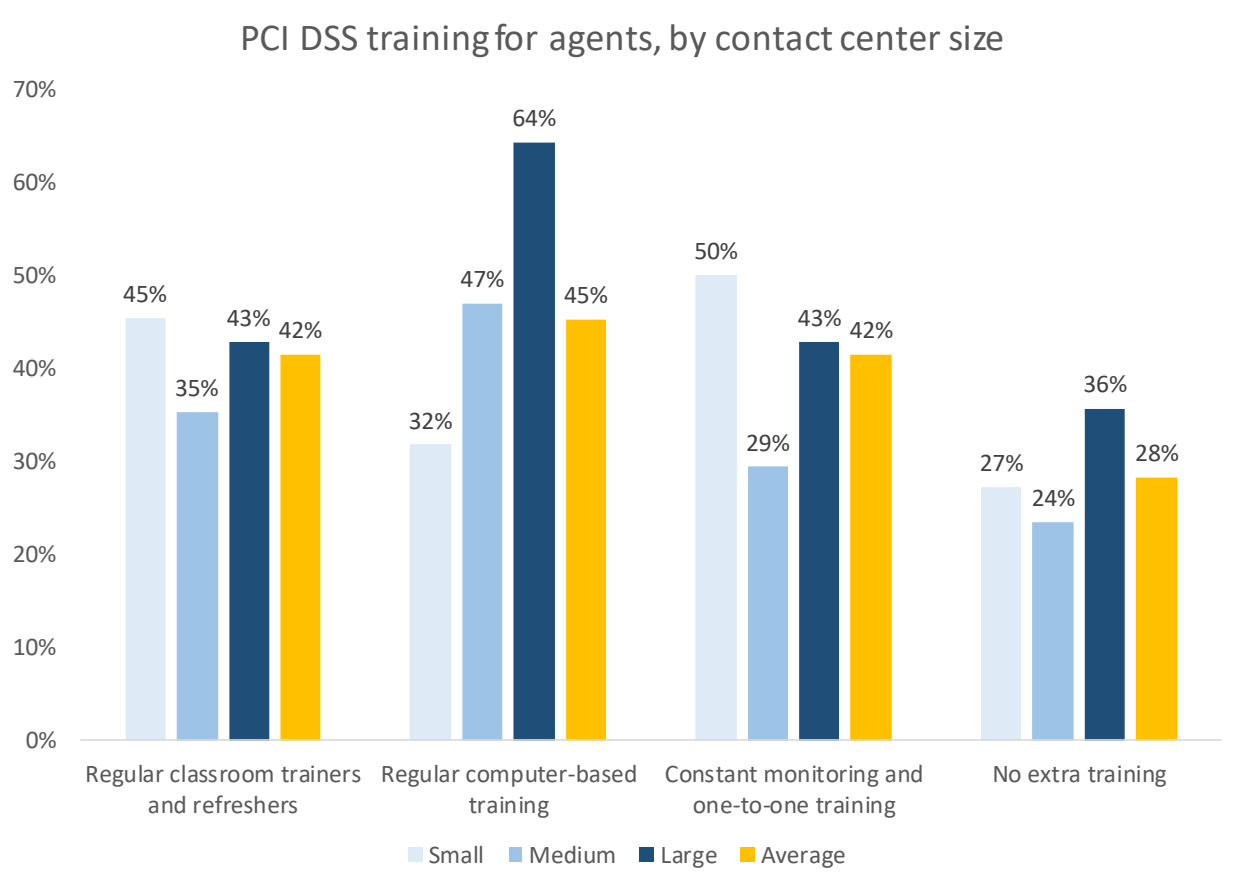
The cost of staff training is a major drain on resources for contact centers (especially smaller ones), and the following chart shows that small operations are providing individual levels of training similar to those that larger contact centers are giving to their agents.

Agents in small operations are more likely to be receiving constant monitoring and one-to-one training, a level of support which may be unsustainable and unaffordable in large-scale contact centers.

Larger contact centers are much more likely to be using regular computer-based training in order to educate agents about card fraud reduction practices, as this is likely to be scalable and require less personal support from managers and security specialists.

Somewhat less than half of contact centers from all size bands provide regular classroom training and refresher courses. 36% of large operations do not provide any additional PCI DSS or card fraud reduction training for agents whatsoever, perhaps preferring to outsource card payments altogether.

Figure 6: PCI DSS training for agents, by contact center size



ABOUT CONTACTBABEL

ContactBabel is the contact center 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 analyzing the contact center 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 center strategies and talk to the right prospects. We have shown the UK government how the global contact center industry will develop and change. We help contact centers 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 center industry, perhaps we can help you.

Email: info@contactbabel.com

Website: www.contactbabel.com

Telephone: +44 (0)191 271 5269

To download the full "2019-20 US Contact Center Decision-Makers' Guide", free of charge, please visit www.contactbabel.com