CONTACTBABEL

The US Contact Center Decision-Makers' Guide 2016

The PCI DSS Compliance Chapter

Sponsored by

semafone®

securing data · protecting reputations

"The 2016 US Contact Center Decision-Makers' Guide (9th edition)" – EXTRACT

To download the full report, please visit: www.contactbabel.com/reports.cfm

The *"US Contact Center Decision-Makers' Guide (2016 - 9th edition)"* is the major annual report studying the performance, operations, technology and HR aspects of US contact center operations.

Taking a random sample of the industry, a detailed structured questionnaire was answered by 221 contact center managers and directors between March and June 2016. Analysis of the results was carried out in June 2016. The result is the 9th edition of the largest and most comprehensive study of all aspects of the US contact center industry.

This White Paper is taken from the "PCI DSS Compliance" chapter, sponsored by Semafone.

PCI DSS COMPLIANCE

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. The PCI SSC 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 banks whose merchants do not follow regulations (which the banks will pass on), or even deny the merchant the ability to take card payments at all.

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. While all of the requirements have some impact upon the workings of the contact center, it is generally considered that Requirements 3, 4 and 12 may have the greatest relevance.

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.

Many organizations, including those regulated by the government, are required to record phone conversations with customers, yet at the same time are prohibited by PCI DSS regulations from recording and storing payment card data. Organizations struggling to strike the right balance between these competing objectives should look to technology solutions that record the call without recording the payment card information. Using Dual Tone Multi Frequency (DTMF) masking technology, companies can have customers enter their card payment information using the telephone keypad, allowing the call to continue as normal, without capturing the payment card data on the call recording.

[1] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

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 centers, 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.

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: if the email or chat interaction is then 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 3.0 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 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 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 defense, go at least as far as the original requirement and not negatively impact upon other PCI DSS requirements.

PCI Security Standards Council
PARTICIPATING ORGANIZATION

semafone®
securing data · protecting reputations

Are Your Telephone Payments Watertight?

When you take payments over the phone you need to ensure sensitive card data can't leak from your telephony infrastructure into your IT environment. Many of today's solutions put a patch over the problem and inconvenience your agents.

Semafone's patented payment method builds a secure channel between your customer and the bank, bypassing your agent's desktop, the network and the company… taking the entire contact center out of scope from PCI DSS, protecting your customers from fraud and safeguarding your business from the reputational damage that results from a data breach.

secured by semafone

For more information go to www.semafone.com or call +1-888-736-2366

THE VIEW FROM THE CONTACT CENTER

Potential danger points within the contact center fall into three main areas: storage, agents and infrastructure. The storage element will revolve around the recording environment - both voice and screen - and the potential and opportunity for dishonest employees to access recordings 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 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

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:

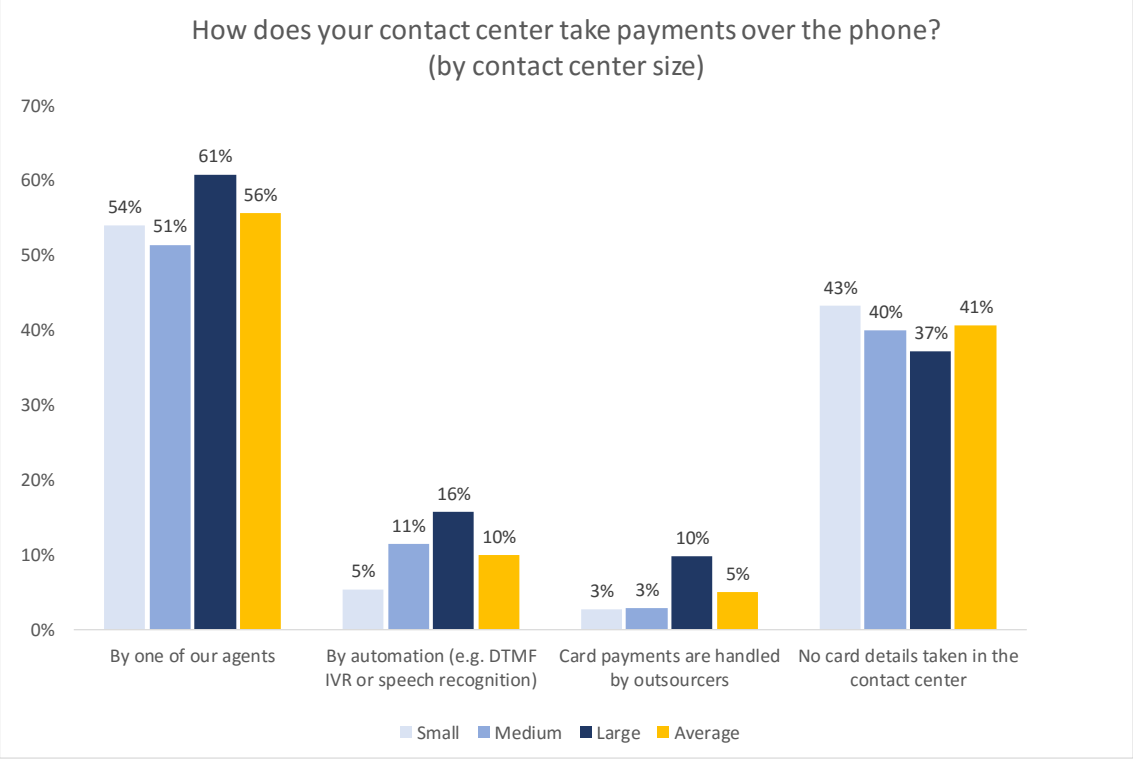
- make sure that contact center employees do not share passwords or user IDs with each other, in order to maintain a segmented and auditable security and access environment
- limit the number of employees given access to full card information. For example, restrict access to call recordings based on 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, analyzing 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 centers and limit physical access to servers which store payment card information
- do not record sensitive authentication data such as the card validation code in any circumstances if possible
- 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.

semafone securing data - protecting reputations Ensure card data remains segregated and remove personally identifiable information or Sensitive Authentication Data (SAD) before it hits the contact center infrastructure by using Dual Tone Multi Frequency (DTMF) masking technology solutions. Because payment card numbers are no longer spoken aloud, the call recording does not need to be paused. At the same time, the sensitive data is not captured on the call recording, so the entire contact centre is taken out of the scope of PCI DSS.

This year, 59% of respondents stated that their operations handle card payments from customers over the telephone. Payments are normally taken by agents, although large contact centers which are more likely to have high volumes of card payments are more likely to provide a fully-automated as well as a human payment option to their customer base, or use outsourced third parties to handle their card payments.

semafone securing data - protecting reputations Ensuring that card data and sensitive information are not recorded on calls and never hit the contact center infrastructure reduces the scope of the Cardholder Data Environment (CEE) and can take the contact center out of the scope of PCI DSS. This is by far the most cost effective solution for both security and compliance – reducing compliance costs by up to 85 percent by reducing the amount of technology required as well as the level of human effort involved in carrying out necessary checks and controls. Such solutions also improve productivity as agents can initiate wrap up tasks while callers input their information on the telephone keypad, adding to further contact center efficiencies.

Figure 2: How does your contact center take payments over the phone? (by contact center size) – multiple selections allowed



There are significant elements to consider around manually taking payment from cards: the time taken to take payment, the risk of fraud by agents, unauthorized access to call recordings, and compliance with the Payment Card Industry Data Security Standard[2], in order to reduce credit card fraud.

Some of the literature around PCI compliance and card handling mentions organizations which adopt a "trust-based approach" that relies on the honesty of their agents as well as their recruitment and agent management processes to avoid fraud. While incidences of agent fraud are rare, compliance with PCI DSS no longer makes this an acceptable option.

Businesses may consider that as well as achieving and maintaining PCI DSS compliance, they may benefit by reducing the DSS scope as well, which will limit the size of the compliance task and cost. A significant reduction in DSS scope can make maintenance easier, reduce the amount of patching and vulnerability scans, as well as reducing the areas of risk and potential attack. For many organizations, the cost and upheaval of large-scale PCI compliance projects, as well as the ongoing efforts of remaining compliant means that trying to move as much of the operation out of scope is a very attractive proposition that makes sense in terms of cost and resource.

Businesses attempt to reduce their DSS scope by limiting the number of places where card data is present by:

- removing redundant and obsolete storage facilities and applications
- replacing the full PAN with a truncated, encrypted and/or masked version
- move away from the need to encrypt by using tokenization
- outsourcing elements of card handling, storage and processing to PCI DSS compliant third parties, and reducing or eliminating the cardholder data environment as a result
- large organizations may define 'PCI security zones' and locate the system components that handle card data, and all systems connected to it, within those zones. Full isolation of the cardholder data environment may be prone to failure due to lack of clear guidelines around how this can be practically implemented and sustained.

[2] https://www.pcisecuritystandards.org/security_standards/

Securing the Contact Center – No One Can Hack Data You Don't Hold

When it comes to taking payments, debit and credit card transactions are the great equalizer. Whether you're a small mom-and-pop shop or a 5000-seat call center, if your business accepts card payments, you need to be aware of the regulations associated with the Payment Card Industry Data Security Standards (PCI DSS).

On the surface PCI DSS makes a lot of sense. By placing restrictions on how card data is handled you're potentially reducing both risk and card fraud. But when it comes to actually implementing the controls in your contact center to comply with PCI DSS, it's not always so cut and dry.

It's a common but false belief that telephone and mail-based sales will diminish as companies move their business from bricks and mortar to online. In reality, the reverse is actually true. As online business increases, call centers are transforming into multi-channel contact centers that have to expand to cater for the online customers who, mid-transaction, may decide to call a customer representative for help with a purchase. Because the numerous telephony and data networks—from call recording to CRM—used by contact centers are all linked together, businesses have a huge infrastructure that has to be controlled. Not to mention the fact that the card data is also being exposed to the agents themselves, requiring the physical contact center environment to be secured as well, often in a Draconian "clean room" process. Each of these areas require up to 327 PCI controls if they are in contact with card data, and that's where things start to get both challenging and expensive.

Attempting to identify and seal every possible point of entry in a technologically complex contact center is like trying to cut the heads off a hydra; for every one you remove, another two appear. If the ongoing business of security checks and remedies is becoming one of the principal activities of your IT team, you are going to have even more problems. The only way to become PCI DSS compliant without embroiling yourself in the vast myriad of demands and costs is to remove the credit or debit card data from your company's contact center altogether. After all, the bad guys can't hack data you don't hold.

One of the most effective ways to remove the card data from the contact center environment is through the innovative use of DTMP masking technology that allows your customer to enter their payment card details into their telephone handset without being transferred to an automated payment system or another part of the contact center. The payment details are then sent directly to the bank for verification without being seen or heard by the agent, or recorded on the corporate IT or telephony network.

This approach has a threefold advantage:

1. No card data is held on your systems, thereby removing these systems from the scope of PCI regulations and at the same time, the need for the many checks and controls.

2. The person taking the call does not hear or see any of the card details, the keypad tones are masked to flat tones which means call recording can continual as normal. This avoids any risk of fraud from your own staff and means that you don't have to subject them to strict security measures such as "clean rooms," in which mobile devices and even pens and paper are forbidden.

3. The fact that the voice call continues during the payment process means that your customer is far more likely to complete the transaction because they have a human on the end of the line to help them with any difficulties. This also greatly improves customer satisfaction as most customers hate talking to machines.

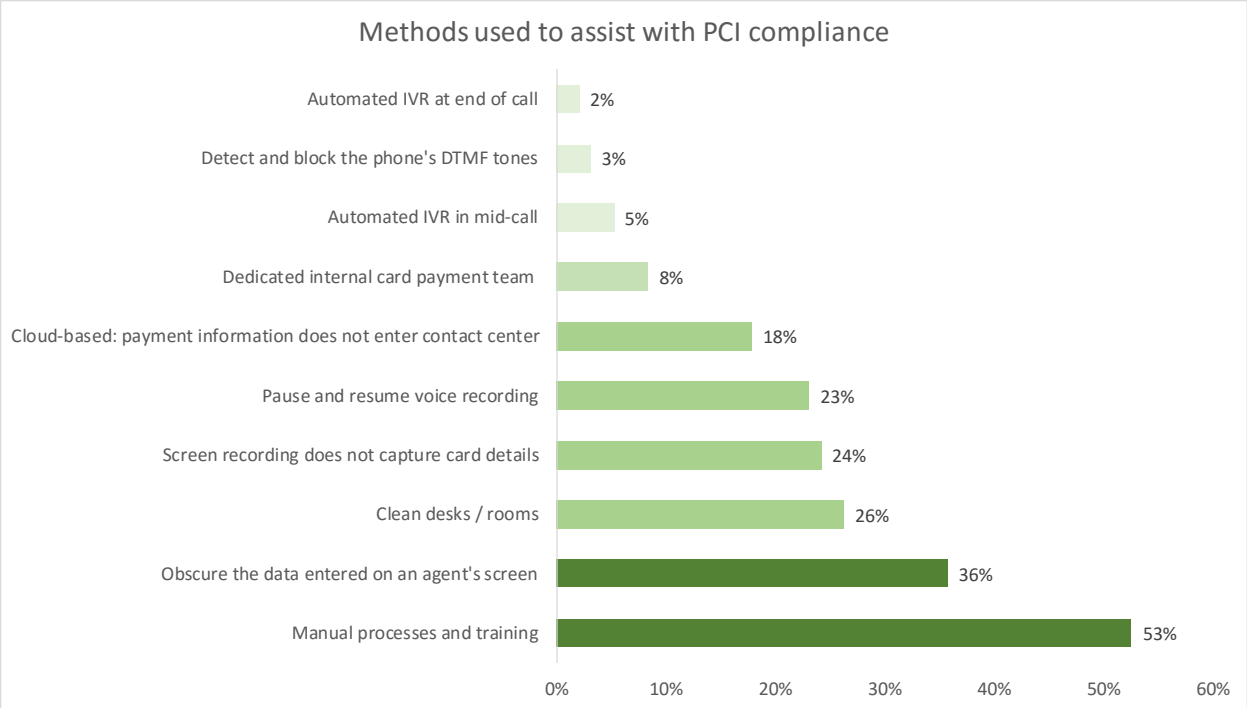
Many people still do not trust payments over the web, so there is an added opportunity to use voice for the last mile of an online purchase. A 'call me' button on the website not only offers a way to take a secure payment over the phone but also provides an excellent opportunity for an 'upsell', mitigating the risk of a lost sale and providing an opportunity for further revenue.

The number of customers paying over the phone continues to grow and with it the challenges of security. Fortunately, the continued popularity of the telephone has inspired technology solutions to reduce the costs and risks of managing this security, while making compliance easy. The customer's voice is still strong and can also be secure.

PCI DSS compliance is not simply about implementing a piece of technology, as compliance covers people and business processes, as well as systems. As PCI DSS is replaced and upgraded every few years (the current version is v.3.0), businesses have tended to implemented a patchwork of solutions and processes to reduce the danger of card fraud and maintain compliance.

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 center, and were asked to indicate which they used.

Figure 3: Methods used to assist with PCI compliance



The most widely used method was that of **agent training**: the biggest risk in any organization relating to data theft is its staff, 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.

'**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. PCI DSS compliance does not seem to permit manual pause and resume capability, as the guideline states that this process must be fully automated, with no manual intervention by staff. 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. There are also alternative options, such as muting the recording or playing a continuous audio tone to the recording system while payment details are being collected, rather than actually pausing the recording, 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. 36% of respondents **mask card details** on the agent's screen, to prevent copies being made.

Some organizations 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 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 was estimated that it takes around $3,000 per agent per year to create and maintain a clean room environment.

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) is more popular than **post-call IVR**, 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.

Only 3% 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 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.

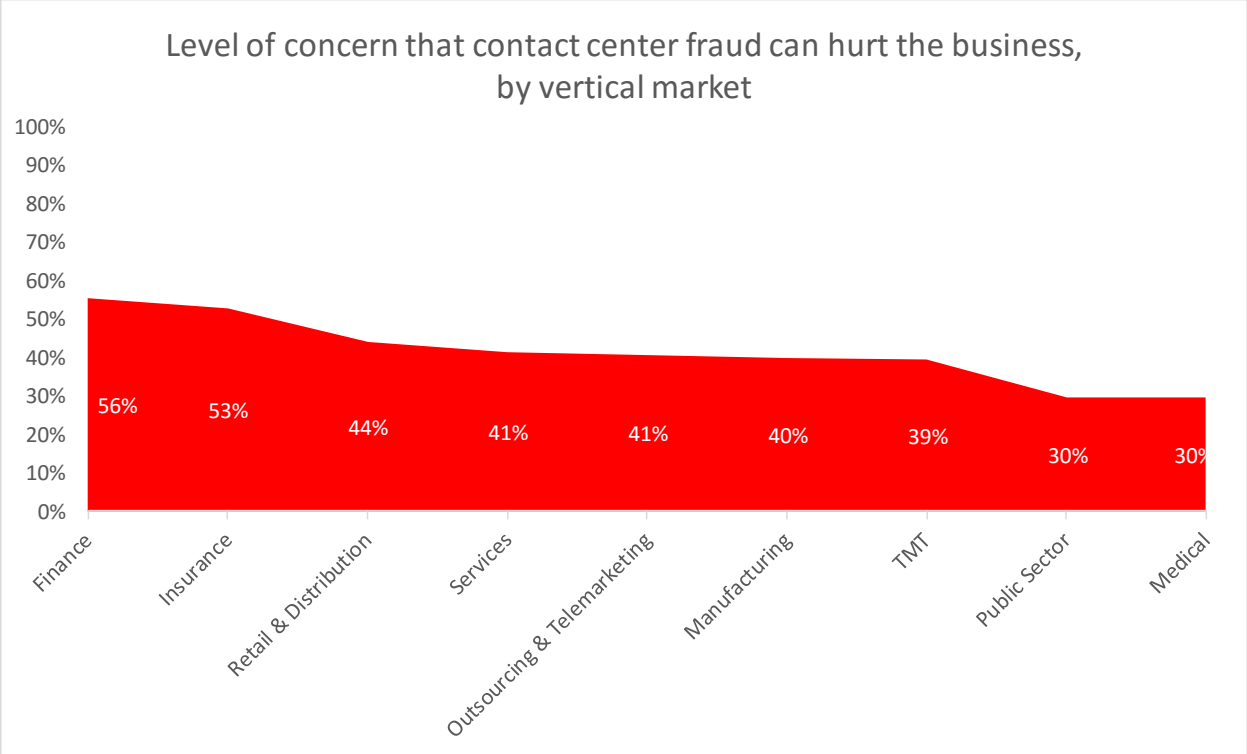
18% of respondents use **third-party cloud-based payment solutions**. Using a hosted or cloud-based solution to intercept card data at the network level means that no cardholder data is passed into the contact center environment, whether infrastructure, agents or storage. As such, this can be seen to 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 what is 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.

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 PCI DSS Compliance in the Contact Center", which is available from www.contactbabel.com/reports.cfm

The following chart shows the extent to which contact centers within each vertical market are concerned about the possibility of fraud within the operation. Respondents were asked to show their level of concern by giving a score between 1% and 100%, where "1%" was "Not at all concerned about fraud as we have the necessary measures in place", and "100%" was "Extremely concerned, and we know we need to improve this".

On average, contact centers tended to be more sanguine than concerned, although as might be expected the financial services sector seems to take things less for granted. While this may appear reassuring, the previous chart showed that the majority of contact centers had a patched-together and possibly even partial approach to PCI DSS compliance and fraud prevention, and these findings suggest that this low level of concern is more about complacency than reality.

Figure 4: Level of concern that contact center fraud can hurt the business, by vertical market



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 QSA audit rather than the self-assessment questionnaire. 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.

Service providers have two levels rather than four, with a cut-off point of 300,000 aggregated card transactions per year. Service providers also have to prove compliance, but to each card brand, rather than to an acquiring bank (which merchants have to do). The proof of compliance is a formal Attestation of Compliance (AOC) which is usually signed by the Financial Director, and states that all PCI requirements have been met. 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 organization might interpret a PCI requirement in an internal self-assessment. Merchants who are looking for a service provider should investigate the limit of the scope that any self-assessment is taken, for example a cloud-based solution provider only applying it to the segments of their platform that handle sensitive data. Merchants may feel that a holistic perspective of security is more appropriate, 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.

Businesses should be aware that proving compliance is not simply a matter of making sure all of the requirements are covered, but 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 program, 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 minimize?

Respondents from small operations are likely to choose unaudited self-assessment questionnaires (SAQs) to prove compliance, with almost a quarter having no PCI compliance program at all. Larger operations are likely to have a mixture of programs, using both internal and external resources, especially QSAs.

Figure 5: How in the contact center's PCI compliance program run?

PCI compliance program method	Small	Medium	Large	Average
SAQ, not externally audited	32%	44%	27%	33%
SAQ, externally audited	21%	33%	27%	26%
External QSA	13%	22%	40%	24%
Internal dedicated resource	26%	56%	37%	36%
No PCI compliance program	*24%*	*12%*	*14%*	*19%*

NB: totals may add up to more than 100% as multiple selections allowed

APPENDIX: 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

The full version of "The 2016 US Contact Center Decision-Makers' Guide (9th edition) is available free of charge from: www.contactbabel.com/reports.cfm