PCI in contact centres still isn't solved

In today's increasingly connected, always on, 24/7 culture, we all rely on using credit and debit cards for payments at any time of the day or night. Whether buying goods online or paying bills over the phone, consumers assume that the company that they are dealing with will manage their card data securely. But how safe are their details?

In the quest to deliver a seamless and compelling customer experience, and maximise sales, as an industry, do we sometimes cut corners? Jason Roos, CEO of Cirrus discusses the legal requirements and some new ways that companies can balance compliance requirements and keeping consumer data secure, with the need to attract and retain fickle customers in a channel-hopping world.

Major card fraud losses

In the first half of 2019, losses due to unauthorised financial fraud on payment cards, remote banking and cheques rose two per cent, to £408.3 million, according to UK Finance (the collective voice for the UK banking and finance industry representing more than 250 firms across the industry).

The ICO reports that during the third quarter of 2019/20, there was a total of 2,795 data security incidents. As we know, information stolen through a data breach can be used for months - or even years - after the event.

While today we are all much more aware of financial scams, the Take Five to Stop Fraud is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud. Led by UK Finance and backed by the government, the campaign aims to help customers to confidently challenge any requests for their personal or financial information, or to transfer money to a fraudster's account, to help everyone stay safe from fraud. As a responsible contact centre, it's worth highlighting the campaign to your customers.

Lack of compliance is endemic

Card fraud is an issue that needs to be tackled industry-wide by everyone involved in making and taking payments. If a business suffers a data breach and is not PCI DSS compliant, they will incur fines for the data loss and could be liable for the costs of fraud incurred by customers.

However, for many contact centres, compliance means expense and disruptive changes to IT infrastructure. According to Verizon's 2019 Payment Security Report, (PSR) there has been a negative trend globally for companies reporting full compliance with PCI DSS. Since 2008, the percentage of organisations that achieve PCI DSS compliance has varied from a low of 11.1% in 2012 to a high of 55.4% in 2016 and more recently dipping well below 40% (36.7%) in 2018.

Making payments secure

When PCI DSS was introduced in 2004 it was expected that organisations would achieve effective and sustainable compliance within about five years. Today, less than half maintain programs that prevent PCI DSS security controls from falling out of place within months of meeting formal compliance requirements.

Depending on the merchant level based on the volume of card payments taken, contact centres can either selfcertify PCI compliance or use a Qualified Security Assessor 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 audit rather than one of the self-assessment questionnaires (SAQs) now available in current PCI DSS standards.

PCI DSS 3.0 - Self Assessment

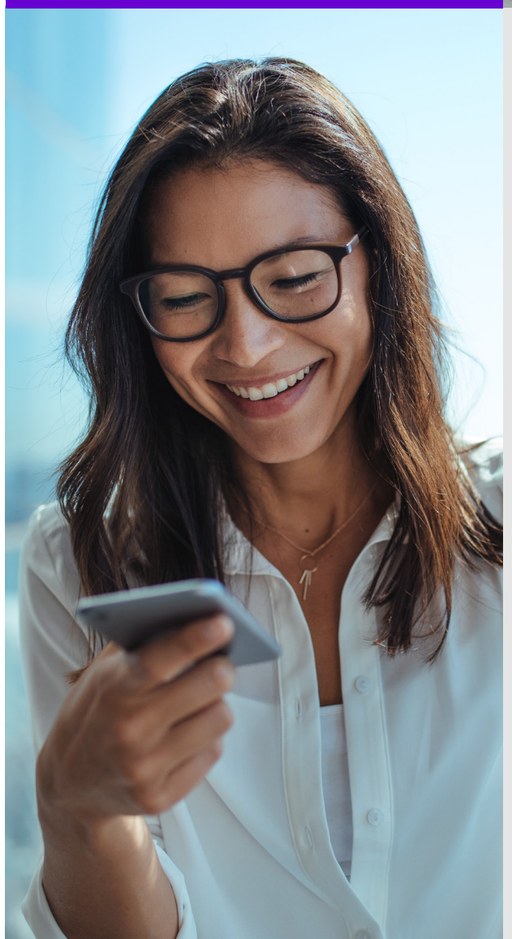
In the latest PCI DSS 3.0 standard, smaller and less at-risk companies do not have to complete the same list of requirements as a large multinational, as there are now a number of different types of SAQ. Many contact centres do not require a full audit and self-assessment questionnaires are becoming far more popular.

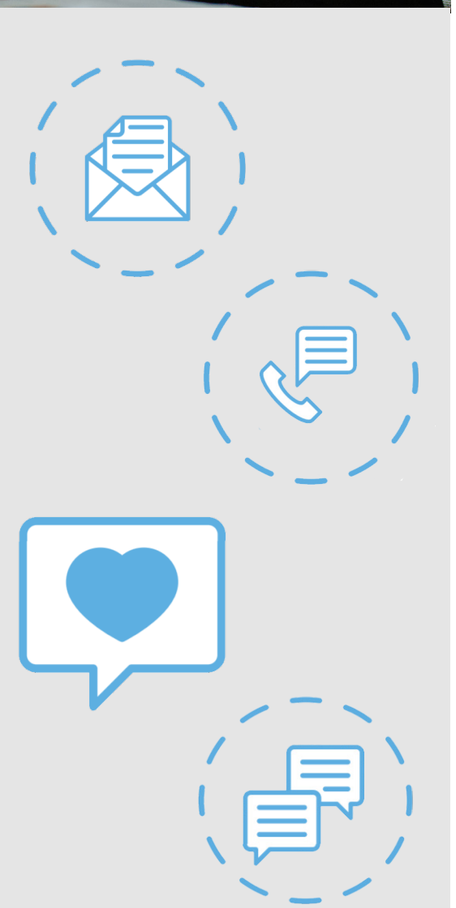
But the PCI problem still isn't solved

Being compliant with PCI DSS takes a lot of resource, however, if the business suffers a data breach, and is not PCI DSS compliant, they could incur fines for the data loss and be liable for the fraud costs incurred against these cards and those associated with replacing the accounts. As well as heavy fines, the company could suffer considerable reputational and brand damage, potentially losing even their most loyal customers.

New technologies like tokenisation and point to point encryption help to secure payments on the high street and online (including online banking), but telephone payments continue to pose additional challenges.

The need for many contact centres to record calls, for security and training purposes, makes protecting the data more difficult simply due to the number of people that may have access to the information. For example, customers entering card details in a web chat seems secure but actually poses a high risk. In a contact centre, quality assessors, team leaders and tech support people could all look up the history of chats and potentially pull out credit card details.





In order to comply with the standards, many contact centres de-scope by eliminating the customer card data that they hold in their systems. Not holding on to data in this way reduces the risk that their customers will be affected by fraud.

There are several ways to do this, but all have their own challenges:

• 'Stop-start' recording - preventing sensitive and confidential data from entering the call recording environment. This relies on the agent remembering to stop and start the recording.

• Clean rooms - where nothing can be written and no paperwork is allowed on desks. However, this is not a particularly pleasant working environment, resulting in a higher turnover of staff making it expensive to operate.

• Dedicated payment teams - also popular and probably provide the best customer experience, but the call often needs to be transferred and that in itself can create problems with extended wait times, lack of continuity, and dropped calls.

• Interactive Voice Response (IVR) Payments – removes the agent risk out of the loop entirely. However, the card data is still within the organisation's network, so although this approach reduces agent contact (and the risk of them writing down any details), it does not in itself ensure PCI compliance.

New ways to pay – More Secure and More Sales

In today's ultra-connected world there are new ways to pay that make it much easier for customers, while providing control for the contact centre. For example, the customer is sent a secure payment link, via any digital channel (such as web chat, WhatsApp, SMS, Facebook Messenger etc.), while they are on the phone or conversing with the contact centre agent or a bot using digital channels. The customer can enter their card details on a secure website page with confidence, often using biometric and other security elements within their own device. The agent or bot on the call doesn't see the card information, but sees a checklist of the steps completed.

Payments can now be taken within the call or chat, saving the customer the hassle of ringing a different number or visiting a website (with the risk of losing the sale). It's more convenient for the customer than entering card details over the phone using the keypad, and, help and advice can be given while on the phone or online.

Being compliant with PCI DSS means that companies are doing their best to keep customers' valuable information safe and secure and out of the hands of people who could use that data in a fraudulent way. At the end of the day the responsibility for compliance lies with the merchant - the key is to choose the right technology solution that fits the organisation and delivers the best possible customer experience. Achieving all of this will help develop loyal customers and boost sales.

Contact us to learn how we can help you address your PCI DSS requirements.

0333 014 0000
marketing@gamma.co.uk
www.gamma.co.uk