How to make your hybrid workforce PCI compliant

The world of hybrid work is here. With ‘smart working’ and flexibility top priorities for many organisations, distributed workforces – comprised of employees working in-office, at home or a combination of both – are here to stay. Indeed, Gartner reports that 75% of hybrid workers say their expectations for working flexibly have increased, and that four out of ten employees are at risk of leaving an organisation if it insists they return to an in-person office.

While the true future of work remains uncertain, there are very few expectations that things will return to exactly as they were before the pandemic. This is especially true in the contact centre industry, where the boom in remote working has spurred a huge shift in operations, moving from legacy on-premise-based contact centres, to cloud-powered customer service – empowering contact centre agents to work from anywhere.

But with this hybrid workforce – as with a predominantly remote one – areas arise for concern, primarily over the security and compliance risks for digital and over-the-phone payments. As a result, there has never been a more appropriate time for contact centres to prioritise secure payment applications and ensure that their enterprise (including remote agents) are PCI (Payment Card Industry) compliant and their customers’ credit card data is always secure.

CONTENTS

IPI Exceptional Customer Contact

The compliance challenges of homeworking agents

Securing sensitive data is one of the biggest challenges for contact centres with a hybrid workforce. Ensuring agents can take payments securely has always been a priority for contact centres, but remote workers have a significantly increased risk profile.

Firstly, remote workers are operating outside of a secure corporate environment, making processing payment card data vulnerable to additional threats. While agents are using company-approved devices, factors such as the presence of unauthorised personnel can make securing systems located in home-working environments difficult. Even workers themselves are concerned, with SentryBay finding that 49% of employees feel insecure about the security of remote working. Working from home can also mean many distractions for agents, as they juggle work and home life.

In addition, PCI DSS controls are harder to implement remotely, as it is more difficult for supervisors to monitor performance and compliance. Whilst technology like Workforce Management systems make it easier, when it comes to secure payments, remote working means there is one less layer of security.

Finally, as customers become more digital-first and accustomed to an omnichannel customer experience, with PayPal and BigCommerce finding that 84.5% of consumers make at least one purchase a month on their mobile devices, remote agents also need to take secure payments across multiple platforms, from SMS to webchat.

Compliance regulations glossary

GDPR – Introduced in 2018, the General Data Protection Regulation is an EU law with mandatory rules for how organisations and companies can use personal data in a lawful and responsible way. In the UK, it was implemented under the 2018 Data Protection Act.

FCA – The Financial Conduct Authority is the financial regulatory conduct body in the UK for around 51,000 financial services firms and financial markets, operating independently of the Government.

PCI DSS - Payment Card Industry Data Security Standard focuses specifically on the protection of payment card and cardholder data, with prescriptive regulations on how this information can be secured. PCI DSS is mandated by credit card companies to help ensure the security of credit card transactions in the payments industry. The 12 PCI DSS requirements are:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for employees and contractors

The PCI industry has never been so busy – but the rules remain the same

The past year has seen a huge increase in the number of customers paying for items online or over the phone. According to McKinsey, e-commerce in the UK grew five times faster in 2020 than before the pandemic.

Along with changing consumer habits, compliance frameworks have also evolved. The introduction of GDPR in 2018 has seen a massive change in data protection concerns for business as well as more serious punishments for companies that fail to take it seriously. Likewise, PCI regulations are constantly adapting to protect consumers and businesses, with the latest version, 4.0, imminent.

The likes of GDPR, FCA and PCI DSS are implemented to keep both consumers and organisations safe, and the pandemic hasn't hindered the operations of the Information Commissioner's Office (ICO) and other compliance bodies. The ICO issued a record £42m in fines during 2020/21, a 1580% increase on the previous year, according to RPC.

Cybercriminals haven't slowed down their activities either, and are taking advantage of the increase in online use and decrease in security for remote workers. One study found that 47% of individuals have fallen for a phishing scam while working at home.

Being able to take payments securely from anywhere has never been more important and protecting customers and customer service agents should be a priority now more than ever.

IPI's best practices on how to ensure your hybrid workers are PCI compliant

In a hybrid working environment, fulfilling secure payments is an obstacle-filled course. Below, are IPI's best practices on how to ensure your hybrid contact centre is doing everything it can so that agents and customers alike remain compliant and secure:

Pause and Resume

Pause and resume or 'stop-start' recording technology aims to prevent sensitive authentication data and other confidential information from entering the call recording environment which is one of the CDEs (Cardholder Data Environment). Consistently a popular way to address some of the compliance regulations, pause and resume works by manually or automatically stopping the recording of a call at the very moment the customer provides their confidential card or bank details.

The main benefits of such technology within a hybrid working environment include a very low set-up cost and the speed of implementation, particularly in a cloud-based environment. IPI's own Pauseable, for example, is a cost-effective, proven mechanism for removing sensitive card data from the call recording. Pauseable allows voice and screen recordings to be automatically "paused" and then "resumed" based on predefined cues. When a recording is paused, the speech is automatically muted with tones periodically injected into the audio stream, preserving the same identity and call length as the original call, protecting call and quality integrity. It also requires no interaction from the agent to initiate the process so they can focus 100% of their attention on the customer experience.

The PCI controls that pause and resume address are mainly concerned with card detail storage, ensuring that liability is removed. However, do keep in mind that agents are still exposed to sensitive card information, and in a homeworking environment with the unauthorised personnel and less secure networks, it's important to ensure that measures are taken to ensure security. Automation is the perfect solution here.

IPI Customer Case Study - Boden

Global high-end fashion retailer, Boden, has been an IPI customer for over ten years. With the vast majority of customer purchases made by telephone, its contact centre is at the crux of its customer service, with calls peaking at 1000 calls a day in 2021 alone. As a telephony and contact centre expert, IPI has guided and supported Boden through many changing landscapes, including the pandemic's instigation of new technological adoption.

Boden quickly recognised the need to enhance its contact centre solutions to fit the world of evolving technology as well as meet its wider IT and transformation plans. IPI recommended a move to Genesys Cloud, as well as the implementation of Pauseable to satisfy stringent PCI requirements. With Pauseable's automatic pause and resume features, Boden felt assured that it would both satisfy compliance requirements, whilst also provide a seamless experience to its end customers.

As an established Genesys partner and with the experience of over a decade working with Boden, IPI was able to oversee the deployment, managing the complexities of a multi-geography contact centre environment and moving to new a system with minimal disruption.

For Boden, Pauseable has satisfied compliance requirements without negatively impacting the customer experience. Financial transactions can be handled safely and securely without any manual involvement from the agent, allowing the agent to focus wholly on the experience being delivered to the end customer.

DTMF Suppression

Regarded as the compliance gold standard, Dual-Tone Multi-Frequency (DTMF) Suppression helps organisations obtain PCI compliance whilst continuing to take payments over the phone and record calls – wherever agents are based.

DTMF works by generating a series of audio signals when a caller inputs numbers onto their phone keypad, each key producing two tones of a specific frequency. Suppressing the tones by replacing them or converting the two pitches into a single flat tone, means the code cannot be deciphered – by anyone. In addition, card details on the agent's screen will be masked as well as the DTMF tones being neutralised

In a home working environment, this CDE is eliminated and no payment details ever enter the home network, going only to the Payment Service Provider, reducing the risk of hacking or payment information being stolen. Customers can input sensitive card details into their phone without any concerns that the cardholder data will be exposed. DTMF suppression is also available as part of our IPI Cloud PCI offering.

Automated IVR Payment

Automated voice assistants, from Siri to Alexa, are part of our everyday lives. So interactive voice response (IVR) technology that allows us to interact using speech recognition or natural language, automated phone system is no hardship.

With automated IVR payments, card data is shielded from agents by directing callers through an automated payment application, and with tools like IPI's Cloud PCI solution, even homeworking agents can accept secure payments. IPI Cloud PCI is a two-tiered solution for handling payments over the phone that greatly assists PCI compliance, even in a hybrid environment. On the first tier is Pauseable. To completely rid the infrastructure of all CDEs, IPI also offers customers a cloud-based DTMF suppression solution (more on this below!).

But keep in mind that IVR payments can be quite disruptive to the customer journey, with the possibility of customers being disconnected and no guarantee they'll be reconnected to the same agent as before. What's more, if on premise, this approach requires very robust PCI controls.

Omnichannel

With omnichannel purchasing more popular than ever, being able to take payment over multiple channels – from social media to email to SMS – is crucial.

Achieved via the same integration as DTMF, a CDE is once again removed as, when a customer inputs their details via webchat or on an online browser, the details are blocked from the agent's view. For example, a secure payment link is sent via an SMS, email or WhatsApp to a customer which then opens a secure form in which card details can be entered.

Also available through the IPI Cloud PCI, an omnichannel offering not only gives customers more choice and allows them to pay at their own convenience, but it also removes a lot of the risks associated with agents taking payments from their home office and significantly reduces (as much as 90%) the PCI compliance controls needed. There's also an extra layer of security added through the omnichannel approach as many customers will be using devices with biometric capabilities.

Give your agents the power to add value to the business

With omnichannel purchasing more popular than ever, being able to take payment over multiple channels – from social media to email to SMS – is crucial.

Achieved via the same integration as DTMF, a CDE is once again removed as, when a customer inputs their details via webchat or on an online browser, the details are blocked from the agent's view. For example, a secure payment link is sent via an SMS, email or WhatsApp to a customer which then opens a secure form in which card details can be entered.

Also available through the IPI Cloud PCI, an omnichannel offering not only gives customers more choice and allows them to pay at their own convenience, but it also removes a lot of the risks associated with agents taking payments from their home office and significantly reduces (as much as 90%) the PCI compliance controls needed. There's also an extra layer of security added through the omnichannel approach as many customers will be using devices with biometric capabilities.

IPI
Exceptional
Customer
Contact

TAKE THE NEXT STEP

IP Integration Ltd
Integration House
Turnhams Green
Business Park
Pincents Lane
Reading, Berkshire
RG31 4UH

☎ 0118 918 4600

✉ enquiries@ipintegration.com

https://ipintegration.com