A SECURITY ASSESSOR'S GUIDE:

SECURING CONTACT CENTER PAYMENTS

PCIpal®

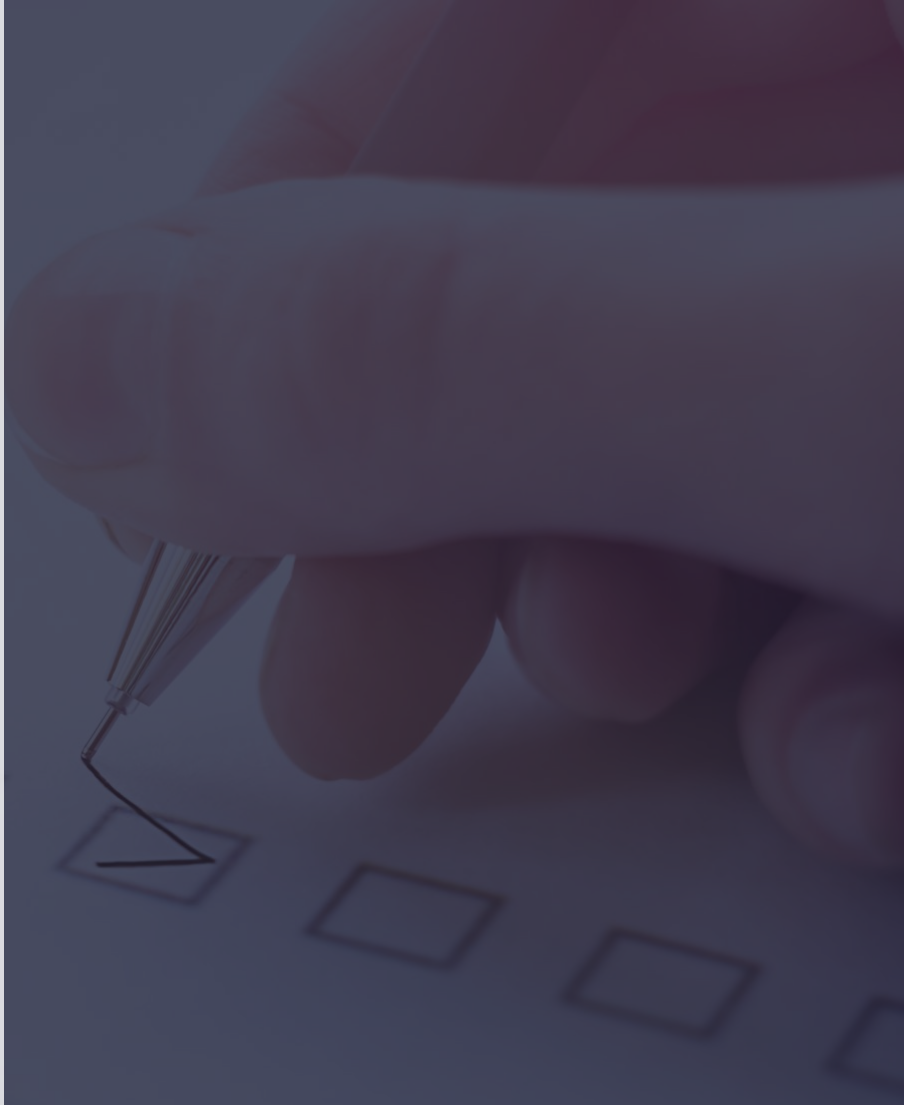
OVERVIEW

This guide serves to provide QSAs an outline of strategies and technologies available to meet payment compliance regulations within contact centers.

Keeping both personal and financial data secure is of increasing importance to companies. Be 'in the know' on the latest technologies and how they can optimize compliance within the business communication environment.

What you'll find in this eBook:

- **PCI DSS and its place in the contact center**
- **Compensating Controls and why they aren't enough**
- **DTMF Masking and its many benefits**
- **PCI Pal Solutions**



PCI DSS:

AND ITS PLACE IN THE CONTACT CENTER

What is PCI DSS?

Prior to 2004, each major credit card brand (Visa, Mastercard, JCB, American Express, and Discover) had its own sets of policies and standards that organizations were expected to implement to ensure a minimal level of security when it came to handling cardholder data. In order to mitigate the complexity of having multiple standards to adhere to, the credit card brands got together and in 2004 released the first version of the Payment Card Industry Data Security Standard (PCI DSS). Two years later, the PCI Security Standards Council (PCI SSC) was formed as a governing entity for the PCI DSS.

Why is the PCI DSS important?

The PCI DSS requirements are designed to combat card fraud by specifying minimum technical and administrative requirements for systems and staff handling credit card data. With data breaches on the increase, laws and regulations have come into effect as a way of strengthening data protection globally. The PCI DSS is a global standard, but it isn't a law. However, almost all data protection laws consider payment card data to be Personal Identifiable Information (PII). As such, non-compliance with the PCI DSS may also mean a breach of other legislation, and is therefore subject to scrutiny and potential fines. By ensuring your contact center is PCI DSS compliant, you are also protecting your business – both financially and legally.

How does it work?

The PCI DSS is a set of 12 requirements that apply to any organization that stores, processes, or transmits credit card details from the major card schemes. In short, if your company takes card payments then the PCI DSS applies, and you need to prove compliance against the standards. The twelve requirements as laid out by the PCI SSC are:

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

NEXT: COMPENSATING CONTROLS

COMPENSATING CONTROLS

AND WHY THEY AREN'T ENOUGH

What are Compensating Controls?

Compensating Controls are band-aid solutions to partially address or fix a greater concern within the contact center as it relates to compliance or sensitive data. Compensating controls have become a sore point with many assessors who are having to question if businesses are using them as loopholes instead of addressing the true problem. Developed as a quick-fix workaround, they are now outdated as data security standards and regulations have developed, and there is a push to implement comprehensive solutions such as descoping through DTMF masking.

Below we have highlighted some of the significant drawbacks of common compensating controls:

Pause / Resume Call Recording	Pause / Resume Screen Recording	Encrypted VoIP Telephony	Clean Room Environment
Broken Recordings	Technical Difficult	Expensive	Diminished Morale
Complaint Handling	Inaccurate	Technically difficult	Impractical
Agent Training	Inconsistent	Affects all calls	Difficult to maintain
Other Regulations	Agent Training		Customer Care Reduced

* PCI Pal and Verizon. (2018). *Keep Calm and Descope ....*

What do the numbers show?

Out of all the contact centers out there, 72% of them accept Card-Not-Present payments.* Extremely common, two-thirds of contact centers are using compensating controls. That means that over 60% of contact centers taking payment by phone are going through a more complicated and often more expensive process than necessary for results that still end in headaches.*

72% of contact centers take Card-Not Present Payments

Why aren't they enough?

Compensating controls solve a partial problem, but the data is still entering the environment. Therefore, the contact center is still within scope for PCI DSS and other regulations. For each partial solution, it's one more possible point of failure in a process.

Organizations are paying, with both time and money, for workaround solutions that have faults of their own and waterfall into other issues.

NEXT: DTMF MASKING

PCIpal®

DTMF MASKING

AND ITS MANY BENEFITS

What is DTMF Masking, and how is it useful?

DTMF (Dual-Tone Multi-Frequency) is the discordant two-tone signal or sound that is generated when you press a button on a telephone's touch keypad. In DTMF masking, the consumer enters their card number, expiration date, and security code using their telephone keypad, rather than speaking their payment card data. These tones are intercepted by the solution, removed, and replaced with a monotone comfort beep for the agents. The captured card data is then sent straight to the Payment Service Provider (PSP) for processing. This process means the data completely bypasses the contact center environment.

The use of DTMF masking technology for PCI compliance can eliminate data breaches at the contact center level. By preventing payment data from entering the environment in the first place, there is no data stored to breach. DTMF masking technology for PCI compliance removes any need for the agent to see, hear or store sensitive payment data. The best solutions allow the customer and agent to speak at all times during the payment process. The voice flow is therefore uninterrupted as the customer enters their details.

As DTMF masking technology removes spoken card data, there's no possibility of the contact center inadvertently recording sensitive financial information. The burden of sensitive data storage rests solely with the payment provider.

What are the benefits?

Improved customer experience – the customer is reassured that their data is handled securely. They are not diverted away from the agent to a 'payment line' solution to complete their transaction with no support.

Reduced PCI DSS scope – as no data is being stored, processed or transmitted within the contact center, the Cardholder Data Environment (CDE) is greatly reduced. This minimizes your risk of a data breach.

Improved agent experience – As the sensitive cardholder data is removed from your contact center, your agents are not exposed to demotivating compensating controls such as clean room environments and additional security checks. In addition, DTMF masking technology means the agent doesn't see or hear the sensitive cardholder data, reducing the company's internal threats from bad actors.

What Industry Thought Leaders Are Saying

This view is underlined and supported by the PCI SSC's guidelines on 'Protecting Telephone-Based Payment Card Data'. Verizon Security also highlights the benefits of DTMF masking as a step towards descoping the contact center in their white paper 'Keep Calm and Descope'.

NEXT: PCI PAL SOLUTIONS

pcipal®

PCI Pal Contact Center Solutions

Agent Assist

Our core solution, **Agent Assist**, utilizes DTMF (Dual Tone Multi-Frequency) masking and speech recognition technology to provide companies with a secure way of handling payments by phone without bringing their environments in scope of PCI DSS.

Digital

PCI Pal **Digital** enables your agents to provide secure payment options via digital engagement channels such as Webchat, Whatsapp, Social Media, Email, and SMS.

IVR

PCI Pal's **IVR** Payments solution empowers your customers to make payments 24/7 without speaking with an agent or accessing your website. Payments are handled within PCI Pal's secure cloud and are integrated with your IVR platform.

We are committed to continuing to provide the most updated resources to the payment security community. For additional resources or to get in touch with our team, connect with us through your channel of choice below:

- www.pcipal.com
- info@pcipal.com
- @pcipal
- linkedin.com/company/pci-pal

pCIpal®