semafone
securing data · protecting reputations

New Guidance for Protecting Telephone-Based Payment Card Data

What You Need to Know

The influx of new technologies into the contact center over the last few years has meant an increase in the number of channels used for customer communication. While this has been great for consumers trying to connect with brands, it's also resulted in a more complex compliance landscape, especially when it comes to securing cardholder data.

Because of these developments, the Payment Card Industry Security Standards Council (PCI SSC) has updated the guidelines for protecting telephone-based payment card data for the first time since 2011. The new guidance clarifies a number of points relating to auditing, payment card data security and protection.

Most Important Points to Consider

1. **Avoid "scope creep": keep your softphones separate.**

The main market adoption of VoIP and softphones, which are often connected to the desktop environment processing payments, can result in the entire unintended networks and applications coming into "in scope" for PCI DSS and subject to its stringent controls. As a result of this "scope creep", it is strongly recommended that contact centers fully segment their data and telephony networks.

2. **Pause and resume means more checks than ever.**

Qualified Security Assessors (QSAs) now have clear guidelines regarding call recordings and the capture of sensitive card details. Both manual and automated "pause and resume" systems, where the recording is briefly stopped, are deemed to run the risk of accidentally capturing these details. If a contact center is using either of these solutions, QSAs can demand extensive evidence of the measures used to protect sensitive data and are empowered to conduct invasive auditing to ensure that additional controls, such as securely deleting card holder data and adding multi-factor authentication controls, have been put in place effectively.

3. **Third-party service providers are in scope if they provide more than a dial tone.**

Many organizations previously used third-party service providers to off-load compliance responsibilities and reduce their amount of applicable PCI controls. The new guidance specifies that any call service, from a "transfer" to a "call recording", that is provided by a third party, will bring that provider into scope for the PCI DSS. The only service that is exempt is a simple voice communications connection, or "dial tone".

semafone
securing data · protecting reputations

4. **Devices that control Session Initiation Protocol (SIP) Redirection are in PCI DSS scope.**

The new guidance recognizes that redirecting a call to a secured line, just for the payment process itself, exposes it to a potential risk of interception or diversion by hackers. As a result, all such devices, on or offsite, controlling redirection are vulnerable and fall into scope for PCI DSS and are therefore subject to the full range of controls.

5. **Organizations must ensure all DTMF tones, including any DTMF bleed, are not present in their environment.**

The guidance states, "It is important to ensure that all DTMF tones, including any initial small portions of 'DMTF bleed' that may be inadvertently allowed through a masking process, are not present in the environment." This means that QSAs will now check to ensure DTMF bleed doesn't occur when using DTMF masking solutions.

Remember, removing the card data from the contact center is the only secure solution.

The updated guidance recommends scope reduction techniques and technologies, including managed and unmanaged dual-tone multi-frequency (DTMF) masking solutions, such as Semafone's Cardprotect. These solutions entirely remove cardholder data and other personal information from the contact center environment. Callers enter their card numbers via their telephone keypad, remaining in full communication with the agent throughout. The DTMF key tones are masked with flat bleeps, so they cannot be identified by their sound. This prevents any sensitive card information from coming into contact with the agent, with call recording technology and with any other desktop applications. The card data is sent directly to the payment processor, bypassing the contact center completely. What's more, Cardprotect has built-in bleed removal features to ensure DTMF digits cannot be recovered, ensuring peace of mind and keeping merchants out of scope for PCI DSS.

Does your contact center comply with the new guidance? Contact Semafone now to find out more.

+1-888-736-2366 nasales@semafone.com semafone.com Twitter LinkedIn