At a Glance – PCI DSS Compliance for SMEs

As the central hub for customer engagement, customer services, customer support or any team serving as the frontline interface for any customer interaction needs to processes and store a wide variety of personally identifiable information (PII) including payment card data, addresses, birth dates, bank account details, social security numbers, medical information and much more. As a result, businesses fall under the scope of compliance for the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is an industry standard designed to help protect consumers' payment card information. It is a set of requirements that organizations must follow in order to accept, process and transmit cardholder data as securely and safely as possible, in an effort to prevent fraud and reduce data breaches.

With its numerous sub-requirements and potentially hundreds of controls, the PCI DSS is one of the most complex industry-wide standards. And, like most data security regulations and legislation, the PCI DSS is constantly evolving to address the latest threats. As such, it can be costly and complicated for SMEs to stay on top of the latest updates and best practices for achieving and remaining PCI DSS compliant.

Who Needs to be PCI DSS Compliant?

In short, any merchant that accepts payments must be compliant with the PCI DSS, regardless of merchant level. This includes companies that accept payments and perform card-not-present (CNP) transactions over the phone, through digital channels such as online forms and web chat, or even through the mail.

Failure to comply with PCI DSS can be very costly to an organization. If a data breach occurs and the merchant is found to be non-compliant, the payment card brands can impose financial penalties on the merchant's acquiring bank. The bank then typically passes those costs along to the merchant - which can range from $5,000 to $500,000 per month. For repeat offenses, the payment card brands can even revoke the rights of the merchant to process card-based payment transactions.

Protecting Telephone-Based Card Payments

When it comes to protecting telephone-based card payments the PCI SSC has offered specific guidance that makes several points clear:

- Sensitive authentication data should never be stored or make its way onto call recordings.
- Pause-and-resume call recording systems **MAY** run the risk of accidentally capturing card data. To mitigate risk, additional controls must be implemented. These solutions also keep the agent in scope for PCI DSS compliance.
- Merchants **should avoid** solutions that leave agent environments in PCI DSS scope unless there is an unavoidable business requirement to do so.
- Recordings **will not capture card data** if DTMF masking is implemented prior to the data reaching recording systems. These solutions remove the agent from PCI DSS scope entirely

Keep Cardholder Data Out of Your Network Entirely

DTMF masking solutions are the most effective method to significantly reduce the number of applicable controls for PCI DSS descoping purposes by removing the agent, the call recording, and the entire network, while enhancing the customer experience.

Semafone's Cardprotect Voice+ solution, built specifically for SMEs, allow customers to make credit card payments

PCI DSS Requirements at a Glance

While there are twelve distinct requirements outlined in the PCI DSS, each addressing a different area of security, at its core the framework is about protecting card holder data and ensuring that sensitive card details are never stored.

Goal:	PCI DSS Requirement:
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	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.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel – and ensure that all personnel are aware of it.

over the phone by entering their PAN using the keypad, all while staying on the line with the customer service representative for the entirety of the call. Not only is it a cost-effective way to enable PCI DSS compliant payments with quick deployment times and powerful integrations, it also provides a more streamlined and frictionless customer experience. Doing so can help descope your business entirely for PCI DSS compliance, and can reduce the associated costs and headaches.