

THE ROLE OF TECHNOLOGY IN MEETING SECURITY AND DATA PRIVACY NEEDS

**PCI and other requirements demand
contact center and IT attention.**

By **Lori Bocklund**, Strategic Contact Inc.



Lori Bocklund
Strategic Contact

Contact centers and their IT departments have plenty of demands on their all too limited time, resources and money. Compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) for handling credit and debit cards often sits in a precarious position. While not every center handles payment cards, consumer protection principles apply to other data, such as Protected Health Information (PHI) and Personally Identifiable Information (PII). Chances are your center needs to be cautious—and compliant—with data management.

It's on Our "To Do" List

Big companies often have the resources—and the greater focus on risk management—to make security and data privacy a priority. For many centers, the data security planning project can get relegated to the corner with things like business continuity/disaster recovery planning. Everyone knows you should have up-to-date plans, but until something happens, it just doesn't seem that compelling. And with no auditor knocking on the door, it's easy to feel comfortable flying under the radar.

As data breaches of major retailers hit the headlines, we have to come to grips with the fact that the threat is very real. The contact center technology vendors pitching products and offering white papers further highlight the risks and demand informed engagement in how to mitigate those risks. It's time to bump security and privacy to the top of your list. And if you have tackled these issues in the past, it may be a good time to review what you've put in place and make sure that you're "compliant."

Getting to Know PCI

The PCI DSS is a set of technical and operational requirements that applies to anyone who "stores, processes and/or transmits" cardholder data. DSS is managed by the PCI Security Standards Council (SSC), working with credit/debit card issuers (American Express, MasterCard, Visa, etc.), to create a common set of guidelines, tools and ways to assess compliance. The PCI SSC provides valuable resources to educate IT and contact center leaders, as do the payment card companies.

HIPAA or other privacy standards have different (but similar) requirements. All such standards are grounded in *best practices* like encrypting data in storage and across networks, securing networks and systems, maintaining an information security policy, monitoring and testing, and strong access control and login rules in today's environment.

The PCI SSC provides guidelines and resources to help corporations become compliant; some focus specifically on what the contact center needs to do. For example, their guidelines for call recording define what a company can store and display. Two key messages for the center: You can't store Sensitive Authentication Data (SAD) (the card's security code that is typically three or four digits), and you have to encrypt the name, expiration date and account number. Those requirements apply to voice as well as data, creating a challenge for call recordings.

Depending on volume of transactions with the various payment card companies, the PCI standard calls for a self-assessment or assessment by qualified third parties. It also defines who must perform network scans and how often. The payment card companies are the enforcers, and there can be penalties for non-compliance, highlighting the need to not take that "we'll do it later" approach.

The standard continues to evolve in response to requirements, changes and learnings on a three-year development lifecycle. This approach enables gradual transition, evolution and compliance, and also emphasizes the need for this to be an ongoing responsibility in your center and company. Version 3.0 became effective on January 1, 2014 (issued November 2013); Version 2.0 ends December 31, 2014.

Call Recordings Are the Target of Security in the Contact Center

As you pursue security and compliance, you'll want to examine all possibilities, but not let technology drive what you do. Every technology plan should consider the value and cost tradeoffs, and the impact on contact handling and the customer experience.

The implications of PCI for the contact center are significant. It impacts:

- What you can record and, therefore, your use of call recording and quality monitoring systems for capture and playback.
- What you can store, including in a Customer Relationship Management (CRM) application or a Customer Information System (CIS).
- What form you can store and transmit voice and data (encrypt it!).
- What you can display and to whom, including the desktop CRM or CIS, and playback.
- Password management and access to information across the corporation, not just in the center.

Agents may have a “need to know” for credit card numbers to do their jobs (as they do PII or PHI). If they are allowed to hear and capture that information, you must have the right tools and processes to manage and protect it. Some prefer to not expose agents to the information and not deal with spoken numbers; technology options make that possible.

Agents versus systems taking private information highlights the need to define requirements and select the best approach for the customer and the center, considering costs and benefits, risks and mitigations, training, resource use, efficiency, etc. Table 1 highlights the main options and some advantages and considerations for each. There is no one “right” way. I am a fan of the solution that automatically stops/starts recording based on integration with your CRM or CIS if you can tackle the integration requirements.

Unfortunately, the general nature of the PCI DSS, along with market hype and myths, leads to different interpretations by contact center leaders, IT, security teams, legal, etc. The chosen approach can impact handle times, facilities layouts, customer experiences and technology complexity. In the end, any of those can impact costs—for a project, or for ongoing operations. So it's important to engage a crossfunctional team to explore the options to reach the best solution for the company, IT and the center. This is why the PCI SSC resources are so valuable as an educational tool. Armed with knowledge, work with your call recording/QM vendors, but also consider others such as specialty third-party solutions focused on compliance, and vendors with IVR-based solutions for integrated information capture.

Other Issues to Consider

Here are some other common issues we see clients tackling for data privacy and security—whether credit cards, SSN, health information or other sensitive data.

Non-phone media, and in particular, written communication like chat and email, should not request protected data. Tell customers not to include account numbers or other sensitive information on these channels, which are generally unencrypted. While the unknowing might like to try a transaction tied to their personal information via chat, they should be guided to use secure self-service or call to speak to an agent.

Technologies like Voice over Internet Protocol (**VoIP**) and now Session Initiation Protocol Recording (**SIPREC**) don't change the requirements. Encryption across the network is critical, and IT should consider the recording options a vendor offers and what is happening with the data packets. Some approaches duplicate packets; where and how they are transmitted and

The Role of Technology in Meeting Security and Data Privacy Needs

TABLE 1: Options and Tradeoffs for Call Recordings

| OPTION | ADVANTAGES | CONSIDERATIONS |
|---|---|--|
| Option to avoid recording | | |
| <ul style="list-style-type: none"> Don't record calls ▶ Don't buy QM ▶ Turn it off if you have it | <ul style="list-style-type: none"> ▶ Nothing to implement ▶ No cost (if already have, lose investment/benefits) ▶ Nothing to audit | <ul style="list-style-type: none"> ▶ Most already have a QM system ▶ Not an option if need recordings for liability ▶ Not an option if want to do speech analytics ▶ Still need to conduct QM; do so via live observations—but accept the compromises: <ul style="list-style-type: none"> - Unlikely to conduct QM at busiest times - Lack recordings for feedback, coaching, training |
| Option that only addresses part of the requirements | | |
| Encrypt call recordings and their transport | ▶ Fairly simple and low cost | <ul style="list-style-type: none"> ▶ A prerequisite—you must encrypt—BUT ▶ Not enough to be compliant! (You still can't store Sensitive Authentication Data) |
| Options that seek to avoid recording sensitive information | | |
| Manual Pause—agents pause recordings when taking sensitive information | <ul style="list-style-type: none"> ▶ Easy to implement ▶ Low cost | <ul style="list-style-type: none"> ▶ Not compliant! <ul style="list-style-type: none"> - Removal (or avoidance) of recording sensitive data must be automatic - Agents will forget and accidentally record sensitive information |
| Integrate with CRM/CIS—to automate the pause in recording when cursor in applicable field | ▶ Automates the stop/start | <ul style="list-style-type: none"> ▶ More complex and costly integration ▶ Carefully train agents to ensure synchronized timing between words and data entry |
| Use desktop analytics—to automate the pause in recording when cursor in applicable field | <ul style="list-style-type: none"> ▶ Automates the stop/start ▶ Less IT time demands than CRM/CIS integration | <ul style="list-style-type: none"> ▶ Requires investment in desktop analytics (and if going to purchase, consider other uses as well for process and systems optimization) ▶ Carefully train agents to ensure synchronized timing between words and data entry |
| Speech Recognition to trigger recording mute/pause | ▶ Automates the stop/start | <ul style="list-style-type: none"> ▶ More complex and costly ▶ Accuracy could be a challenge |
| Options that seek to avoid recording, and agent hearing, sensitive information | | |
| <ul style="list-style-type: none"> Transfer to IVR for data input ▶ Agent typically on hold while caller is in IVR and caller returns to agent when finished inputting data | <ul style="list-style-type: none"> ▶ Agent not hearing or capturing the sensitive information ▶ Easier to exclude from call recordings | <ul style="list-style-type: none"> ▶ More complex and costly for application and integration <ul style="list-style-type: none"> - Potential network costs if remote/hosted IVR ▶ Can increase handle time (not generally freeing up agent while customer in IVR) ▶ Can negatively impact customer experience (transfer and IVR entry are both typically dissatisfiers) ▶ Risk customer hangs up and lose sale or doesn't complete the transaction on that call ▶ Need an answer to the “what if” of the caller not willing to enter data into the IVR |
| <ul style="list-style-type: none"> Use IVR or other capture device with agent on phone (and block touch tones/DTMF) ▶ Agent asks caller to enter number | <ul style="list-style-type: none"> ▶ Provides call continuity while not exposing agent to spoken data ▶ Easier to exclude from call recordings | <ul style="list-style-type: none"> ▶ Need a trigger for capturing the touch tone—manual or automated—and has same considerations as other triggers (reliance on human or system) ▶ Some of the same risks as transfer to IVR—handle time, customer experience, hang up, etc. ▶ Need integration to enter data into system from capture device |
| Options that seek to remove sensitive information from recordings | | |
| Speech Analytics to identify and remove sensitive information | <ul style="list-style-type: none"> ▶ Automates the removal of sensitive data from recordings ▶ Can apply to existing recordings as well as new recordings | <ul style="list-style-type: none"> ▶ Must be done when recording (real-time) or immediately after recording ▶ More complex and costly ▶ Accuracy could be a challenge |

stored is part of the data security scope.


Masking data is an important element of security. We've all entered passwords where the field shows asterisks. The same sort of screening can be done with display or entry of private data so the agent isn't seeing more than needed, and to reduce the chance of capturing such data in illicit ways (e.g., on a smartphone or piece of paper). Present only the digits required for validation (e.g., last four of card or SSN), and mask the entry. For those that don't yet do real-time credit card validation, greater security may drive this requirement; without it, you risk many rejections when the batch run occurs. And finally, PCI may make those that allow use of electronic "Notepads" (or paper) for initial data capture change their rules and desktops.

PCI has implications for **physical space** in the center, and on the other end of the spectrum, guidelines for using home agents and remote agents. It's important to note PCI does not prohibit the use of home agents, but it does have something to say about who can be around agents handling protected information, whether they are in a corporate facility or their home. The bottom line is people with unrelated roles should not be near those taking this information (in earshot of, walking by or seeing). For some centers, a heightened focus on data privacy and security will be the catalyst for finally becoming paperless and perhaps enforcing policies about no personal phones on the desktop (with some clear added value in removing a potential agent distraction!).

Speaking of home agents, consider any resources interacting with customers **outside the center** walls as you think about your recording processes and technology. Any option should contemplate the end-to-end call flow, including transfers. For example, if you sometimes transfer to a store or other location (even partner companies), assess whether the call is still in your system and being recorded, or is released. **Home agents**, remote offices and offices that pitch in occasionally, such as a bank branch, need to be reviewed. Use encrypted VPN for voice and data and use remote recording capabilities. Compliance with recording and data masking requirements are paramount, but policies, monitoring and reinforcement are all critical as well.

Finally, some see **outsourcing** or **cloud-based solutions** as the cure-all for PCI (or other data protection) compliance: Let's make it someone else's problem! That is an option, but you better make sure that they are—and remain—compliant. Choose your partners carefully, and put an ongoing audit process in place to ensure that you are safe.

Get Started—and Keep Going

The market offers a variety of good solutions to address the main concern for centers—recordings—but each company must plan carefully, evaluate options, and find the best approach for that environment. Look for vendors that “get it” with well-designed solutions and a willingness to help you become compliant by effectively leveraging their products and supporting the necessary integration. And while technology plays a key role in addressing data privacy and security needs, this is not just a technology thing. Address process compliance and physical space needs along with the technology. And keep in mind that it is not just a one-time project; compliance is an ongoing top priority to maintain and reinforce. 

Lori Bocklund is Founder and President of Strategic Contact.

✉ lori@strategiccontact.com

☎ (503) 579-8560



VALUABLE RESOURCES FROM PCI SSC

Visit www.pcisecuritystandards.org to learn more about the PCI DSS, including information specific to the contact center. The following documents should be of particular interest to contact center and IT leaders supporting those centers:

- PCI DSS v3.0
- Getting Started with PCI Data Security Standard
- Payment Card Industry Security Standards Overview
- Protecting Telephone-based Payment Card Data
- PCI DSS Data Storage Do's and Don'ts
- Ten Common Myths of PCI DSS
- Information Supplement: PCI DSS Cloud Computing Guidelines

About Contact Center Pipeline

Contact Center Pipeline is a monthly instructional journal focused on driving business success through effective contact center direction and decisions. Each issue contains informative articles, case studies, best practices, research and coverage of trends that impact the customer experience. Our writers and contributors are well-known industry experts with a unique understanding of how to optimize resources and maximize the value the organization provides to its customers.

To learn more, visit: www.contactcenterpipeline.com



Online Resource

This issue is available online at: [ContactCenterPipeline.com](http://www.contactcenterpipeline.com)

<http://www.contactcenterpipeline.com/CcpViewIndex.aspx?PubType=2>