

# Don't Risk a PCI Compliance Breach in Your Contact Center: Automate and (Almost) Forget It!

Any business that wants to process, store, or transmit credit card data needs to comply with the Payment Card Industry Data Security Standard (PCI-DSS) — often referred to as PCI. PCI-DSS is a collaboration between credit card associations that sets industry-wide, global security requirements. It's a method to minimize exposure, vulnerability, and liability for both you and your customers under a mandatory compliance program.

Failure to meet PCI compliance standards could result in expensive data breaches, fines from credit card companies and banks, audits, loss of customers, lawsuits, and a tarnished brand image.

Verint® facilitates PCI compliance with secure systems and applications that address the following key mandates:

- Recording a card payment interaction without capturing Card Verification Value (CVV) data.
- Protecting stored cardholder data.
- Encrypting cardholder data at rest and in transit whether in short- or long-term storage.
- Providing the ability to restrict access to cardholder data.
- Identifying and authenticating access to system components.

## How Verint Solutions Support PCI Compliance

- **Capture Interactions with Verint Recording Solutions** — Interactions with your customers are increasingly subject to recording for a variety of reasons: to ensure good customer experience; to gain insight into what customers are communicating about your products and services; to protect an organization from liability; and to uphold regulations, such as PCI.

- **Pause and Resume Recordings with Verint Desktop and Process Analytics** — Based on actions taken by an agent, Verint Desktop and Process Analytics™ can automatically trigger the pause and resume functionality within the Verint recording infrastructure to prevent the capture of both audio and desktop screen recordings. This includes not just the CVV information mandated by PCI-DSS, but all cardholder data – relieving you of the responsibility to protect it.
- **Encrypt Files for Safe Storage with Verint Encryption Management** — Some organizations prefer to avoid capturing CVV information, but record the rest of the cardholder data. To keep this information safe from exposure, Verint Encryption Management™ uses the highest AES 256-bit standards of end-to-end encryption to encrypt data at rest and in transit, and meets FIPS 140-2 compliance. This helps ensure that, even if subject to a breach, the data remains encrypted and safe from exposure.

The security features of Verint's solutions can also allow you to limit access to only those individuals with specific authorization to view the data within the audio and desktop screen playbacks, such as legal counsel or auditors.

**VERINT.**



# Executive Perspective

## Benefits of Verint's Approach to PCI Compliance

By leveraging Verint solutions to avoid capture of sensitive information, and encrypt and protect stored information, your organization can:

1. Reduce human error from manual processing.
2. Avoid high costs and fines of non-compliance.
3. Protect profits by avoiding loss of customers from damaged brand image.
4. Reduce PCI compliance audits.

Here are a few examples of customer PCI success stories.

### PlumChoice

Using Verint Desktop and Process Analytics in tandem with Verint Quality Management™ (which includes call recording capabilities), PlumChoice was able to achieve PCI compliance. A context-driven desktop trigger pauses the call and screen recording, and another trigger resumes recording once the collection of payment data is complete.

### Fortune 500 Property and Casualty Insurer

This insurer uses Verint Desktop and Process Analytics extensively to not only achieve PCI compliance but also adhere to state-specific requirements. Desktop triggers automatically pause call recording when sensitive payment card data is collected.

Additionally, the company uses the solution's pop-up alerts to prompt agents to recite specific language during customer calls, helping ensure compliance with state insurance requirements. The solution also enables the insurer to tag customer calls for easy search and retrieval.

## Automate PCI compliance and make it one less thing you have to worry about

Verint has 25 years of experience supporting heavily regulated industries, including banking, healthcare, and telecommunications, as well as federal entities. Click here to learn how Verint helps organizations meet regulatory standards, minimize organizational risk, and reduce financial penalties.

## The Customer Engagement Company™

### Americas

info@verint.com

1-800-4VERINT

### Europe, Middle East & Africa

info.emea@verint.com

+44(0) 1932 839500

### Asia Pacific

info.apac@verint.com

+(852) 2797 5678



verint.com



twitter.com/verint



facebook.com/verint



blog.verint.com

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Not all functionality is available in all configurations. Please contact Verint for current product features and specifications. All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners. © 2019 Verint Systems Inc. All Rights Reserved Worldwide. 05.2019

# VERINT®