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

- Protect personal identifiable information (PII)
- 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.outcomes can provide tremendous benefit to improve processes going forward.

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 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®

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

Automate Compliance and Make It One Less Thing You Have To Worry About

Even if you are already using one method to protect PII, AI can add even more security to your compliance strategy. The Verint PII Redaction Bot provides a new way to protect customers' personally identifiable information. Using Verint Da Vinci AI, the bot can automatically find instances of PII, like social security numbers, credit card numbers, and more from your interactions. It then hides this information in both the transcript and the audio playback for unauthorized users — adding a new layer of security to existing data protection strategies.

Benefits of Verint's Approach to PCI and PII 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.

IT Services Provider

Using Verint Desktop and Process Analytics in tandem with Verint Quality Management™ (which includes call recording capabilities), an IT Services Provider 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 to help ensure compliance for specific state insurance requirements with "pop-up" alerts, which prompt agents to recite precise language during customer calls. The solution also enables the insurer to tag customer calls for easy search and retrieval.

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

Learn more at
www.verint.com

Verint®. The CX Automation Company™

Americas
info@verint.com
+1 770 754 1900
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
x.com/verint
linkedin.com/company/verint
verint.com/blog

VERINT