Complying with PCI DSS

cirriusimpact
Hosted Contact Center

Table of Contents

Complying with the New PCI DSS Rulings

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by the PCI Security Standards Council to facilitate the broad adoption of consistent data security measures worldwide. The PCI DSS is a multifaceted security standard which includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

NICE Systems provides a set of solutions for call recording which includes strong access control tools, multi-tiered security design, and end-to-end multimedia encryption that facilitates PCI DSS compliance in a compliant environment. Refer to Appendix A for information about how NICE Perform® assists organizations to comply with PCI DSS requirements.

Recently, the PCI DSS Council clarified their intentions regarding recording audio data which includes card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by the payment brands).

They issued two subsequent clarifications to highlight when recording this type of sensitive data is permitted and forbidden.

The Council's latest ruling states:

"PCI SSC FAQ's are designed to provide merchants, assessors, acquirers and other Council stakeholders with clear and timely guidance on PCI standards. They are a critical two way communication channel from which the PCI SSC draws valuable market feedback and insight, and is able to share this with the industry. On January 22 2010, as part of the online FAQ feedback and submission process, the regular review of FAQ language, and inquiries from Participating Organizations the SSC sought to clarify its position on call center audio recordings. The updates to the FAQ language were intended to eliminate any inconsistencies in implementations of audio recordings in call center environments by providing a higher level of specificity in FAQ guidance. The Council's position remains that if you can digitally query sensitive authentication data (SAD) contained within audio recordings - if SAD is easily accessible - then it must not be stored. As a result of additional market feedback, on February 17, 2010 the SSC modified the new language to further clarify its position on audio recordings.

***Question**: Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of PCI DSS?*

This response is intended to provide clarification for call centers that record cardholder data in audio recordings, and applies only to the storage of card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by the payment brands).

It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted.

*It is therefore prohibited to use any form of digital audio recording (using formats such as wav, mp3 etc) for storing CAV2, CVC2, CVV2 or CID codes after authorization if that data **can be queried**; recognizing that multiple tools exist that potentially could query a variety of digital recordings.*

Where technology exists to prevent recording of these data elements, such technology should be enabled.

***If these recordings cannot be data mined**, storage of CAV2, CVC2, CVV2 or CID codes after authorization **may be permissible** as long as appropriate validation has been performed. This includes the physical and logical protections defined in PCI DSS that must still be applied to these call recording formats.*

This requirement does not supersede local or regional laws that may govern the retention of audio recordings"

For more details, refer to following link on the FAQ web page of the PCI DSS:
http://selfservice.talisma.com/display/2/articleDirect/index.aspx?aid=5362.

Knowledgebase Article #5362 - Are audio-voice recordings containing cardholder data and-or sensitive authentication data included in the scope of the PCI DSS)

The changes between the two versions of this clarification highlight the PCI DSS Council's intention to allow recording card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by payment brands) as long as this sensitive information cannot be queried or data mined with tools available on the market.

NICE solution architecture prevents external tools from data mining or querying sensitive information from recorded interactions in the following manner:

- The recorded interactions are saved in the NICE capturing units (the Loggers) in a raw fashion in an unformatted disk partition. There are no tools available in the market to read this information from the Logger partitions except for the NICE Logger solution itself.
- The recorded interactions are long term archived on an industrial storage solution in a NICE designed file format (NMF) so that other commercially available tools will not be able analyze and data mine them.
- When encryption is deployed, it is used as an additional means of security to block unauthorized users and tools from using, querying and data mining the recorded interactions.
- NICE applications do not tag the sensitive information inside the recorded interaction nor populate the system databases with that information neither presenting it to the system users.
- When NICE Interaction Analytics capabilities which include the transcription engine are deployed, the relevant information is masked out of the transcription, so that other available tools cannot data mine the interaction transcriptions.

For additional precautions, NICE offers solutions **to prevent recording this sensitive information during the call** and ensure that it is not recorded.

Audio and DTMF Tone Data

The NICE audio recording solution will be enhanced in the next NICE Perform release to pause and resume audio recording when callers provide sensitive information.

The NICE pause/resume recording capability enables pausing and resuming a NICE Logger's recording channels. The pause/resume functionality is performed in two ways:

- Manually – agent-initiate tray icon application installed on the agent's computer with a single-click user interface
- Automated – through an API for third-party integrations- the interface is suitable for integration with IVR, third-party applications or homegrown applications (CRM application, transaction processing applications, etc.)

The *Pause* function is invoked whenever the audio on that channel should not be recorded. The Logger's channel will remain paused until another external trigger resumes recording or until the next interaction on that channel takes place.

Agent Screen Data

NICE's recommendation is to prevent recording sensitive screen information as part of the NICE screen recording solution by blocking the recording of the specific application or web page used for inserting this data.

NICE provides a tool to define a list of applications or web pages that will not be recorded per agent. When playing back the recording, all screen information will be re-played except for the applications that were pre-set not to be recorded. Those applications appear as a black screen in their original location on the agent's desktop.

Another option to block sensitive information from being recorded is masking sensitive information by the payment or CRM application. An example of this type of implementation would be displaying only asterisks on the agent's screen in the CRM system while entering the CVV. This ensures that the information is masked on the recording level as well and not stored in the NICE solution.

In addition to these two options, NICE will present additional enhancements to the next NICE Perform release such as the capability to stop and resume screen recording based on different triggers like Desktop Analytics, third-party integrations and manual agent command via a tray application.

Appendix A

The following table provides information about how the NICE Perform system assists organizations to comply with the requirements of the PCI DSS.

Payment Card Industry (PCI) Data Security Standard	
Build and Maintain a Secure Network	
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	■ The NICE Perform solution architecture supports a multi-tiered security design allowing the segregation of data and functional elements into access control zones. Access between zones is controllable by a network firewall to ensure that only authorized components communicate across zone boundaries. ■ NICE provides a detailed list of services and ports necessary for the NICE Perform solution to operate. Most default settings of port numbers can be changed by the system administrator. ■ The NICE Perform solution supports Fully Qualified Domain Names (FQDN) and NAT/PAT networking environments to provide IP masquerading. ■ The communication of the applications and client side components with the NICE Perform Applications Server is secured and encrypted
Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters.	■ Customers are advised to change default system passwords during system installation. ■ NICE Perform features strong authentication and user password encryption. It also supports user authentication and single sign-on with Active Directory. ■ SQL Server default 'sa' login is not used. NICE Perform applications can be configured to employ Windows (NT) Authentication for SQL Server secure access. ■ NICE-provided servers are shipped pre-hardened using procedures consistent with industry-accepted system hardening standards. ■ NICE publishes a comprehensive hardening guide for all NICE Perform software components. Customer specific hardening procedures can be staged and certified by NICE Global Services. ■ All NICE Perform server-based components run as Windows services to provide enhanced security and data protection. They can be safely associated with Windows domains for better control and compliance with customer IT policies.
Protect Cardholder Data	
Requirement 3: Protect stored cardholder data.	■ Strong encryption of stored audio and screen recordings is provided using AES symmetric encryption with either 128 or 256 bit key lengths. Recordings are encrypted using cipher-block chaining (CBC) mode at their point of creation. They remain encrypted wherever they are stored, including data backups and archives. ■ Encryption keys are maintained in a secure Microsoft SQL Server 2005 database and only transmitted over SSL connections between authenticated entities. ■ Encryption keys are created dynamically, as required, and do not rely on user supplied values. ■ Non-encrypted audio files are stored in NMF format, a native NICE file format that is not compatible with generally available payback utilities such as Microsoft Windows Media Player. Specific user permission rights must be assigned to allow exporting files to other file formats.
Requirement 4: Encrypt cardholder data transmission across open, public networks.	■ All network transmission of audio and screen recordings are in encrypted format. When they need to be replayed, they are only decrypted just before use on the local device. ■ Encryption keys are only transmitted over SSL connections between authenticated entities.

Maintain a Vulnerability Management Program	
Requirement 5: Use and regularly update anti-virus software.	■ NICE Perform is certified to be compatible with anti-virus software from leading third-party providers including Symantec, McAfee and Trend Micro. Other anti-virus systems can be certified on an as-needed basis by NICE Global Services.
Requirement 6: Develop and maintain secure systems and applications.	■ NICE executes an expedited process for certifying Microsoft's critical and important security patches. Proactive security patch and service pack certification is based on the NICE Security Certification Policy. NICE customers and partners are regularly notified about certification status through the NICE extranet Web portal. ■ NICE developed procedures to ensure that current security settings and configurations are not changed when NICE Perform is updated. ■ NICE develops software applications based on industry best practices. Information security is incorporated throughout the software development life cycle inspired by Microsoft's Trustworthy Computing Security Development Lifecycle model.
Implement Strong Access Control Measures	
Requirement 7: Restrict access to cardholder data by business need-to-know.	■ NICE Perform uses a profile-based user administration methodology to control user access. A profile consists of a set of privileges that define system functions and resources to which access is permitted. Changes to access profiles are dynamic; the change takes effect as soon as it is saved. ■ Access permissions can be defined down to the individual database field level. ■ New users are added through a wizard-driven process ensuring that an access profile is assigned to them.
Requirement 8: Assign a unique ID to each person with computer access.	■ Every user with access to the system is assigned a unique user ID. ■ All users are required to input a unique user ID and valid password before gaining access to NICE Perform. ■ User passwords are hashed and stored using an industry standard 256 bit SHA. Clear passwords are never transmitted over a network. ■ Strong password management capabilities. ■ Users are automatically required to repeat the login process after 15 minutes (user configurable) of inactivity. ■ User authentication is performed using industry standard Challenge Handshake Authentication Protocol (CHAP) to prevent gaining access by recording a user's authentication exchange and replaying it. ■ Optional support for Microsoft Active Directory is provided to allow for user authentication and single sign-on based on the user's Windows credentials and for consistent user administration and password management policies in the organization.
Requirement 9: Restrict physical access to cardholder data.	■ Users must have specific access profile rights in order to export audio and screen recordings to other media and formats. ■ NICE capture devices utilize 'unformatted' disk storage devices that are not compatible with standard file share

Disclaimer

www.cirriusimpact.com • info@cirriusimpact.com • 1.866.411.0123

cirriusimpact
Hosted Contact Center