



A white paper from Mitel

IMPACT OF PCI DSS ON RECORDING SOLUTIONS

What is PCI DSS?

PCI DSS stands for Payment Card Industry Data Security Standard and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

(<http://www.pcisecuritystandards.org>). The standard was created to help organizations that process credit card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. A company processing, storing, or transmitting payment card data must be PCI DSS compliant.

Non-compliant companies who maintain a relationship with one or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined. All in-scope companies must validate their compliance annually. This validation can be conducted by auditors - i.e. persons who are PCI DSS Qualified Security Assessors (QSAs), however smaller companies have the option to use a self-certification questionnaire. Whether this questionnaire needs to be validated by a QSA depends on the requirements of the card brands in that merchant's region.

How are Mitel recording solutions affected by the PCI DSS standard?

Mitel recording solutions may unintentionally record and store communications containing credit card data (account numbers), if, for example, a customer reads out his credit card account number (also called Primary Account Number (PAN)) to the call center agent via the telephone. Even more sensitive is the so-called card validation code (CVC) also called card verification value (CVV), card security code (CSC) or Kartenprüfnummer (KPN)). This information must not be stored in any case according to the PCI standard.

When screen recording is used, the PAN and CVC may also be captured unintentionally and stored on the recorder.

The Solution

The primary goal shall be to avoid the recording of credit card data in the first place by muting audio and excluding credit card data input from screen recording.

In order to achieve this goal Mitel will provide detailed instructions on how to configure the audio and screen recording to avoid the capture of credit card information. In addition, templates for Standard Operating Procedures (SOP) for companies will be provided, detailing the procedures for muting audio.

As long as the system is configured correctly, and the users adhere to the SOPs the recording of credit card information will be reduced to recording due to human error. In order to reduce the potential security vulnerabilities even further, a couple of measures will be taken within the Mitel recording solution to avoid the misuse of such unintentionally and exception-based recorded credit card data. These measures comprise of:

- Encrypted storage of audio data (Industry standard AES encryption)
- Encryption of audio transmission to players
- Hardening of Mitel's recorders by means of port scanners and ongoing thorough security threat assessments
- Virus scanner (upon request)
- Firewall
- Deletion of unintentional recorded credit card information (with two-person integrity)
- Central logging of system and security events

Please note that despite some statements made by other players in the marketplace, encryption (even so-called end-to-end encryption) will not automatically make a recording solution PCI DSS compliant. As stated before, there is credit card information which must not be recorded at all (e.g. CVC), even encrypted.

Encryption will only help to reduce the leakage of unintentionally recorded credit card information.

PCI DSS compliance can only be testified for merchants' or service providers' existing installations dealing with cardholder data. Mitel provides solutions which are designed in a way that can be part of an overall system which meets the PCI requirements that lead to PCI DSS certification.

Appendix:

High level description of the 12 PCI DSS requirements and Mitel's comments

Requirement Number	Description	Mitel's Comment
1	Install and maintain firewall configuration to protect cardholder data.	Firewalls shall be configured according to Mitel's product documentation.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Mitel systems are deployed with specific accounts and passwords.
3	Protect stored cardholder data	The primary goal is not to record cardholder information in the first place. Exceptional cardholder data stored due to human error is encrypted.
4	Encrypt transmission of cardholder data across open, public networks	Mitel's programs use secure transmission mechanisms (https, sftp, ssl) for all communication across the network.
5	Use and regularly update anti-virus software	Virus scanners can be installed on Mitel recorders.
6	Develop and maintain secure systems and applications	<ul style="list-style-type: none"> • Mitel will include latest patches of third-party software in every new release • Mitel software will be checked with a static code analyzer • Mitel development executes regular code reviews • System security will be checked with security scanner for every new release • Mitel systems will be checked by independent security experts at regular intervals
7	Restrict access to cardholder data by business need-to-know	The primary goal is not to record cardholder information in the first place. Exceptional cardholder data stored due to human error can only be accessed following a two-person integrity mechanism.
8	Assign a unique ID to each person with computer access	Support of LDAP and two-person integrity login.
9	Restrict physical access to cardholder data	Physical access to the recorders can only be restricted by the company. E.g. by placing recorders in server rooms with restricted access. Archives of communication are encrypted i.e. unauthorized obtained archive media cannot be played back.
10	Track and monitor all access to network resources and cardholder data	Mitel systems provide a detailed audit trail.
11	Regularly test security systems and processes	At the company's discretion.
12	Maintain a policy that addresses information security for employees and contractors	At the company's discretion.



To find out more about Mitel's compliance recording and analytics solutions visit:
mitel.com/products/applications/contact-center/mitel-workforce-optimization

mitel.com

 **Mitel**
Powering connections

© Copyright 2020, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.