PCI Redaction on Call Audio:

How ASR Technology Can Mitigate Risk

PCI Regulations: What Contact Centers Need to Know

PCI DSS Overview

In the early 2000s, as the theft of credit card information began to rise, companies realized that a change was required to protect their and their customers' data. Merchants and others entrusted with this important information needed to improve how they stored, processed, and transmitted credit card data. In response, stakeholders from across the industry developed the Payment Card Industry (PCI) Data Security Standard (DSS) in 2004. The PCI DSS established policy standards and procedures for securing sensitive data transactions and protecting cardholders against theft and misuse, covering areas such as:

- Network security
- Cardholder information storage protection
- Software security
- Access monitoring
- System monitoring to ensure security functionality and enforcement.

Today, PCI DSS compliance is mandatory for any organization that processes, stores and/or transmits cardholder information, including primary account number (PAN), cardholder name, and expiration date. Failure to achieve compliance exposes companies to a higher risk of fraud, theft, and liability. As the headlines too often demonstrate, data breaches can impact millions of customers and result in hefty lawsuits, major business disruption, and expensive incident discovery and response actions. Companies simply cannot afford to ignore the PCI DSS.

PCI Management & Concerns in Contact Centers

Because client calls frequently involve PCI data, PCI DSS compliance is a must have for the protection of Contact Centers and their clients. Until 2010, PCI DSS focused primarily on backend storage, but now Contact Centers must consider front end data collection as well. Current PCI DSS requirements are such that storing digital recordings of CVV is no longer in compliance, and organizations should proactively plan to prevent CVV from being recorded. Over time, such requirements may become stricter and even more expansive.

> For contact centers, the threat of PCI data being stolen or breached is serious.

As in any organization, the threat of a breach may come from outside the organization or internally from malicious and opportunistic employees or contractors. Protecting a contact center from these threats starts with a detailed PCI DSS compliance plan. When creating and auditing such plans, contact centers should consider the ways in which automated speech recognition (ASR) technologies can help mitigate key threats to PCI DSS compliance.

Mitigating PCI Risk When Migrating Stored Audio Data

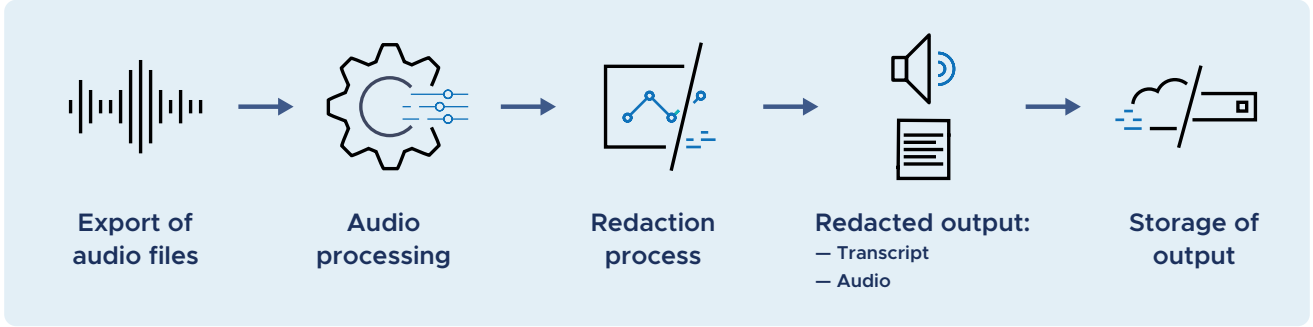
Risk is inherently involved in moving large amounts of data, and any PCI contained in the data increases that risk. Yet system migrations and technology upgrades necessitate the movement of large volumes of data. To reduce risk when preparing for a data migration, eliminating PCI is imperative, and Automatic Speech Recognition (ASR) technology can help. Where manually finding and removing PCI from stored audio data would be prohibitively costly and time-consuming, using ASR allows Contact Centers to clean millions of hours of recordings in days, not months. With an ASR solution, Contact Centers can efficiently detect and redact PCI and other sensitive data from stored files, with manual involvement required only for the ASR engine setup and implementation.

For PCI detection, many people expect PCI to only be found in certain strings of numbers. However, this is not always the case. Contact centers must take care to remove not only complete PCI numbers but PCI number fragments as well. For example, a caller will read out their credit card numbers in multiple segments and the agent will repeat back the digits they heard.

This can cause a fragmented string of numbers which makes it more difficult to find and redact. With so many possible scenarios, the best practice for reducing risk is to remove all numbers from recordings, minus the following exceptions that are generally safe to leave untouched:

- Individual numbers used as words (one question, two kids, etc.) not digits
- Ordinals (1st, 2nd, 3rd, 4th)
- Percentages (10%, 12.8%)
- Clock times (3:45 PM, 8 AM)
- Monetary amounts ($19.95, my $0.02)
- Numbers with 4 or less digits on each side of the decimal (I have 42.79 GB remaining on my data plan, etc.)

Following the automated cleaning of the audio files, employees can review metadata that identifies the file locations where data was scrubbed to assess the threat mitigation.



PCI-related questions to ask in your organization:

- Do we currently have PCI stored in our audio data? If so, how much?
- Do we follow the requirements of PCI DSS Compliance?
- Do we have a proactive plan in place?

Ongoing PCI Protection in Call Centers

Beyond concerns that arise during data migration and consolidation, the matter of ongoing PCI protection in new calls is also of crucial concern. Current methods used by Contact Centers include relying on data security and encryption, redacting information based on agent actions, and implementing real-time automated redaction.

Protection via Internal Security and Encryption: A High-Risk Practice

Rather than redacting PCI from the recordings, organizations often trust internal security measures to prevent theft or misuse of these new files. However, this requires extensive time, energy and vigilance from security and technology staff. Even then, with the powerful technology and increasing skill of modern cyber criminals, success is not guaranteed – and insider threats remain possible as well. For the most failsafe PCI protection and to ensure PCI DSS compliance, the gold standard is to avoid recording and storing PCI data in the first place. Remember, the less PCI data stored, the less risk the contact center faces.

Redaction Based on Agent Actions: Leaving Room for Human Error

Traditionally, many contact centers rely on agent actions to prevent PCI from being recorded. For example, they may ask agents to manually stop call recordings whenever sensitive data is being provided by a customer. Alternatively, agents may pass the call to an IVR system that will input the data as needed without recording the audio. Another method used by contact centers is to implement a desktop analytics system that automatically pauses the recording whenever an agent opens a specific page or moves the cursor into a PCI field on-screen.

These methods sound good in theory but in practice leave too much room for human error and malicious intent. For this reason, **PCI DSS does not approve of relying on manual interventions from staff to achieve compliance.** Agents can easily forget to pause a recording or only remember to do so after some information has already been recorded.

Likewise, they may forget to resume a recording after PCI has been given, in which case the contact center may miss out on audio that is valuable for analytics, compliance and quality control. Other times, callers may give information more quickly than an agent expected and the recording may not be paused in time. Finally, agents may abuse the ability to pause recordings and purposefully shield parts of their calls from QA or compliance review. In such cases, an organization increases risk for numerous compliance and legal issues.

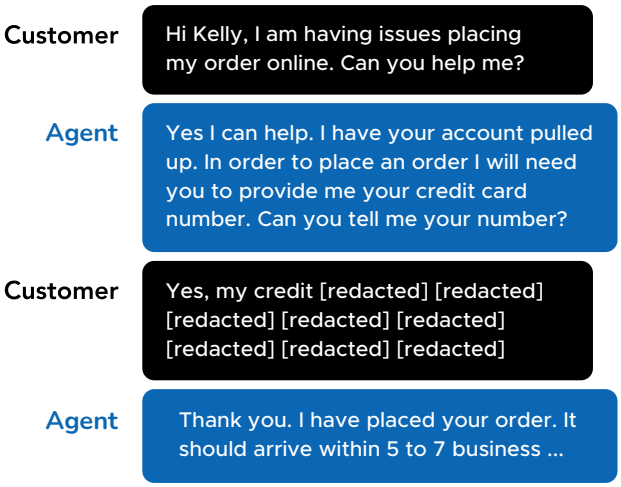
Automated Redaction: A Best Practice for PCI DSS Compliance

> Rather than leave the protection of PCI up to agents when the cost of mistakes is so high, automated PCI data detection and redaction provides a more robust and reliable solution. By using ASR technologies, Contact Centers can detect PCI data in real-time as it is spoken, while ensuring that the rest of the conversation is recorded for compliance and quality control purposes.

As PCI data is detected, these ASR solutions prevent the permanent recording of that information in audio files and corresponding transcripts. An ASR engine can also redact the numbers on screen so that agents cannot capture identifying numbers via screenshots. In transcripts where PCI data has been redacted, the dates and numbers will be replaced by a predetermined symbol; in the audio recording, the listener will hear silence.

By using ASR systems for PCI redaction, contact centers can more easily achieve PCI DSS compliance. They drastically decrease the chances of recording and storing PCI and therefore reduce business and legal risk in the event of a breach and prevent the need for costly corrective actions.

PCI redaction in call audio format



PCI redaction in the chat view

Why Trust QEval Speech for PCI Detection & Redaction?

QEval Speech Technologies offers a fast, highly-accurate ASR solution that supports real-time and post-call PCI redaction to protect Contact Centers and their customers. QEval Speech's ASR engine can clean existing files as well as recognize and prevent the recording of numbers and months in new calls to reduce the likelihood of PCI being stored in audio or transcript files. This includes preventing CVV and PIN capture per PCI DSS requirements as well as preventing the recording of other identifying information, including PAN, service code and expiration date. By default, QEval Speech's redaction feature is configured to redact all numbers, except for low-risk numbers such as ordinal numbers, percentages, times, prices, and short decimals – all of which QEval Speech's ASR engine can recognize by the context words around the numbers such as “dollars'' or “percent”.

By using QEval Speech for PCI detection and redaction, Contact Centers can create recordings that not only meet but exceed PCI DSS requirements while also ensuring that other information needed for QA and analytics isn’t lost in the redaction process.

Scalable to call centers of any size and configurable to any IT infrastructure setup, QEval Speech's ASR engine offers maximum efficiency and ease of deployment to deliver PCI redaction. To learn more about QEval Speech's affordable and reliable ASR solutions for PCI protection,
Visit www.qevalpro.com or call +1 936-559-2258

Lightning Fast
Industry leading time to results

Highly Accurate
Customizable to any business or industry

Open and Flexible
Easy integration for any technology stack

Safe and Secure
Automatic redaction of sensitive information

Speech Engine
Large Vocabulary Continuous Speech Recognition (LVCSR)

Languages Supported
All North American languages (English, Spanish, and French)