Compliance

Protect Sensitive Customer Data

Highlights

- Manage ChorusCX user authentication and authorization with Microsoft Active Directory
- Automatically pause recording to avoid collecting sensitive data in order to protect your customers and remain compliant
- Use SSL to securely connect to ChorusCX servers
- Monitor all system and user activity with automated audit logs and reports

ChorusCX Workforce Optimization (WFO) suite includes the call recording features and capabilities organizations need to improve service levels, enhance business processes and protect sensitive customer data while remaining compliant with federal, state and industry regulations

Protect Sensitive Customer Data

All companies conducting transactions over the phone require a reliable call recording solution that protects sensitive customer data and ensures compliance with various state, federal and regulatory requirements. ChorusCX delivers the solution.

Primarily used to safeguard credit card data, ChorusCX compliance tools help you adhere to the Payment Card Industry Data Security Standards (PCI DSS). Included in the many processes required of businesses to be PCI-certified is the requirement to secure the credit card number and the associated security codes (i.e. CAV2, CID, CVC2, CVV2) in call recordings. For some industries other regulations may apply, such as protecting Social Security Numbers (SSN) and/or Personal Health Information (PHI) in recordings to ensure compliance and eliminate potential theft of sensitive data.

Methods to Secure Data and Stay Compliant

Maintaining compliance with so many regulations may seem overwhelming, but with ChorusCX you can be assured sensitive data is secure.

eCapture

ChorusCX eCapture sends a command to pause recording just before sensitive information is collected and then sends a second command to resume recording after the data has been communicated. This method ensures sensitive data is not stored with recordings. Since nothing is recorded during the pause, sensitive information is not recorded and cannot be retrieved at any time in the future. This efficient method allows for retention, analysis and evaluation of recordings while maintaining compliance with PCI, HIPAA and other regulations.

ePause

ChorusCX ePause runs in the background, monitoring the open web page the recorded user is viewing. When it encounters a web page that is defined in the list of "pause" web pages, it pauses the recording. When it encounters a web page that is defined in the list of "resume" web pages, it resumes the paused recording.

Similar to eCapture, sensitive information is not recorded and therefore cannot be retrieved in the future. ChorusCX ePause is simple to configure and does not require any custom programming.

Compliance

Protect Sensitive Customer Data

Manage User Roles and Permissions

ChorusCX gives you complete control so you decide who can access recordings and reports, and perform evaluations. Its built-in programmable security and multiple permission layers let you decide the level of data each authorized user may access, and its flexibility allows you to set permissions at the group or individual level.

ChorusCX assigns each user a unique ID and validates the user's credentials using either Active Directory or ChorusCX security processes. Active directory ensures strong passwords with expiration dates. Access control permissions may be assigned to either the user or the group, and permit users to perform certain tasks available in ChorusCX, such as Playback and Save As. Permissions also include criteria that determine which recordings a user or group may access. Users automatically inherit their group's permissions, but unique permissions may also be assigned to the user.

Track User and System Activity

Whether you monitor for regulatory compliance, system activity or intrusion detection, ChorusCX makes compliance auditing easy by creating an audit log for every interaction. You can quickly see who accessed which record and what actions were taken.

The Audit Log Report details who accessed the system or recording, when they accessed it, and what they did. Fields available in the standard report include Date/Time, User ID, Event Type and Log Detail. Events may also be recorded to the Windows Application Event Log if needed. Events or activities that are specific to a particular recording may help you safeguard customer data and are easy to access in ChorusCX.

Architecture

Distributed Mode

ChorusCX distributed model allows the web service, database and recording applications to each reside on separate servers to ensure data security. The ChorusCX web interface does not interact directly with the database that contains the recording data. Instead, all database requests go through the DBAccess web service, further separating the user interface from the database layer. ChorusCX systems should be implemented and maintained in a physically secure location following industry standard best practices that meet PCI DSS standards. Firewalls and other appropriate security technologies should be used to protect the servers from intrusion and viruses per the PCI DSS standard. The ChorusCX web service should be configured with an SSL certificate so all recording transmissions are encrypted.

Recording Files Access

ChorusCX uses an encrypted file to store the location and access permission of all recordings; the database only has the recording filename. Users of the ChorusCX system cannot access a recording file directly or discover the location of the file.