

The Most Flexible, Cost Effective PCI DSS Compliant Call Recording Solution Available Today

On October 28, 2010, the Payment Card Industry Standards Council announced tightened restrictions to recording and storage of sensitive data. PCI Data Security Standard version 2.0 went effective on January 1, 2011. Organizations that do not take action to ensure compliance with these new requirements could face costly fines.

Challenge with Most Call Recording Systems in Use Today

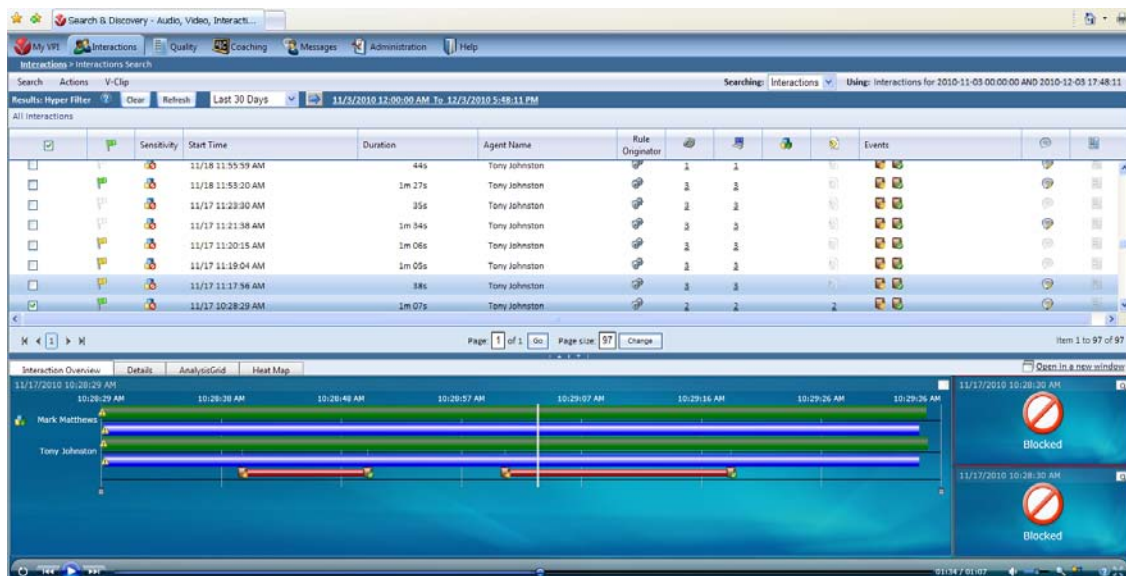
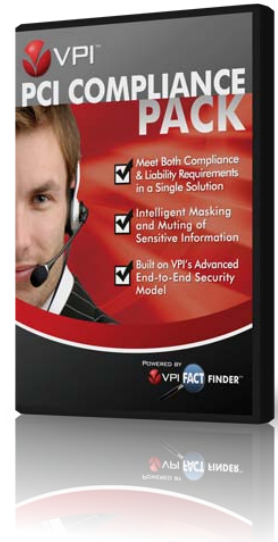
In order to comply with the new PCI Data Security Standard, many organizations will be forced to either abandon call recording or delete all call recordings that may contain verbal receipts -- because the process of listening to the contents of potentially hundreds of thousands of call recordings would be cost prohibitive and labor intensive. Unfortunately, the many calls that do not contain sensitive data will also be deleted - calls that should be retained for quality assurance (QA) purposes, training and liability management.

The VPI Solution Advantage

VPI, a PCI Security Alliance member, supports PCI DSS guidelines by employing advanced desktop screen analytics monitoring and PCI compliant call recording technology. The VPI recording system automatically identifies calls containing sensitive card holder information. Organizations are then provided with four options to help effectively balance their PCI requirements with liability, quality management and other regulatory requirements that require or strongly recommend that calls be recorded in their entirety. These include the Telemarketing Sales Rule, FSA (Financial Services Authority) Rules, BASEL I, Sarbanes-Oxley Act, Gramm-Leach Bliley Financial Services Modernization Act, Truth in Lending Act (TILA) and Fair Debt Collections Practices Act (FDCPA) Acts.

Option 1 - Roles-based Muting of Audio and Masking of Screen Video upon Call Playback

For organizations that have a justifiable need to record calls in their entirety, and that also require call playback for quality and training purposes, VPI offers a solution that allows selective access to recordings for playback that blocks sensitive information. The solution uses VPI's Fact Finder technology to identify and tag sections of call recordings where the sensitive events and data occur -- these segments are then masked and muted during playback. Agents, supervisors and QA analysts without full access rights are permitted to playback non-sensitive portions of the voice and screen recording - everything that led up to and following the sensitive transaction including after-call wrap time. Only authorized users, such as compliance officers or senior managers, would have access to those recordings in their entirety.



The VPI recording solution has the ability to mute out the audio and mask out the screen video during segments of the call containing sensitive data (marked in red) upon playback

Option 2 - Roles-based Access to Recorded Files Containing Sensitive Information

For organizations that are permitted to record entire calls (i.e. companies that perform, facilitate, or support credit card issuing services), the VPI solution has the ability to only allow access to call recordings containing sensitive payment card data based on the user's log-in account and corporate role. For example, only compliance officers and senior executives would have access to those recorded files during legal discovery. All other system users would not be able to access the recorded calls that are classified as sensitive.

Option 3 - Delete all call recordings with sensitive information but retain valuable non-sensitive interaction data for reporting and analysis

Data about what happened during the interaction often provides more business value than the actual recording itself. Instead of being deleted along with the sensitive audio and screen recordings, valuable data such as call date/time, call direction, total handle time, hold time, Customer ID, Agent ID, DNIS, sales or collections \$ amount, number of transfers, or even handle time of key processes within the call that led up to the successful transaction, is made available in interactive reports and analysis of key business issues and opportunities.

Option 4 - Permanent Muting/Masking during Segments Containing Sensitive Information

For organizations that do not have a justifiable need to review or keep entire recordings for liability and other regulatory reasons, VPI is creating a solution to permanently mask and mute sensitive audio and screen video, in compliance with the most stringent of the PCI requirements. In this case, the audio and video of segments containing sensitive card holder information will be deleted prior to storage of recordings, never becoming available to any system users, regardless of user authorization privileges. *VPI expects to make this feature generally available in 2011.*

Maximum Security to Ensure Compliance with PCI DSS Requirements

To further ensure maximum security and compliance with PCI DSS requirements, VPI also provides:

Encrypted Transmission of All Data across Open Networks

The intent of strong cryptography is that the encryption be based on an industry-tested and accepted algorithm. VPI supports AES 256 data and file encryption with strong cryptography as well as secure protocols including Secure Socket Layer, Transport Layer Security (SSL/TLS) or Internet Protocol Security (IPSEC) to provide secure transmission of recorded voice and screen recordings and associated data over the network. *(PCI DSS Requirement 4.1)*

Restricted Access to Card Holder Data by Business Need-to-know

The VPI system supports a granular definition of access rights for large number of user types which allows for greater control over system user Roles and Privileges, such as the ability to search for and playback media files which contain sensitive data as identified by the VPI Fact Finder desktop analytics tool. *(PCI DSS Requirement 7)*

Assignment of Unique IDs to Each Person with Computer Access

The system requires user authentication with a unique User ID and password to permit access. It tracks all user data-access activities within the system by User ID, date, activity type and ID of each recording accessed - displaying who has logged into the system, searched for calls, played back or exported calls and when. The status and history of all activities can be reported on and monitored in heat maps that present audit log data in a visual, easy-to-analyze manner. *(PCI DSS Requirement 8)*

Detailed Audit Log Tracks and Monitors All Access to Network Resources and Card Holder Data

This is achieved by providing a detailed audit trail of all user activities - linking specific actions to specific users, thereby providing high degree of visibility and transparency - so that organizations can conduct full trace audits to determine who accessed any recording in the system and when - for playback, export, or any other critical events. *(PCI DSS Requirement 10.1)* The VPI system also provides an interface for reconstructing events - user actions can be searched, categorized, sorted, reported and viewed by user or activity type. They can be visualized in heat maps by category. *(PCI DSS Requirement 10.2)*



About VPI

VPI (Voice Print International, Inc.) is the world's premier developer and provider integrated call recording, quality management and workforce optimization solutions for contact centers, enterprises, government agencies and first responders. VPI's award-winning solutions help over 1,500 organizations worldwide improve workforce performance, build customer loyalty, minimize risk and ensure compliance. For more information, visit www.VPI-corp.com or call (800) 200-5430.



VPI™

Immediate Results. Unmatched Value.™

*Some features and applications mentioned may require a future release and are not available in the initial release. Future product releases and applications are subject to availability and cost. Specifications are subject to change without notice. Some features may require additional hardware and/or specific software. All products and services mentioned are the trademarks, service marks, registered marks or registered service marks of their respective owners.