PELORUS
ASSOCIATES

Call Recording Guide to PCI-DSS Compliance

How to Balance PCI, Liability, Quality Assurance and other Regulatory Requirements

Authored by Dick Bucci, Chief Analyst, Pelorus Associates

Compliments of VPI™

TABLE OF CONTENTS

Table of Contents

Introduction

Identity theft was the number one source of consumer complaints to the Federal Trade Commission (FTC) in 2007. Estimates by private market research firms peg the incidence of identity theft as high as 15 million consumers. The most common form of identity theft, according to the FTC, is the misuse of credit and debit card accounts. Approximately 3.4 million adults can expect to have their payment card data compromised every year. When credit card identities are stolen, it's not just the credit card companies that are left holding the bag – cardholders often face economic losses, lengthy legal battles and struggles to re-establish clean credit records. While for most consumers the impact is modest, according to the FTC one out of twenty victims suffer median out of pocket loses of $400 and spend 60 hours trying to clean up the mess that resulted.

Approximately 3.4 million adults can expect to have their payment card data compromised every year. One out of twenty victims suffer median out of pocket loses of $400 and spend 60 hours trying to clean up the mess that resulted.

- FTC

Cyber Crime

For today's high-tech thieves, software is a much more productive and arguably less risky way to take other people's money than dumpster-diving for card receipts or picking pockets. A class of software known generally as malware can unsuspectingly creep into data bases and extract hundreds of thousands of account identifiers. Malware is also spread by propagating a worm or virus or by making the malware available on a web site that exploits a security vulnerability. Common techniques include phishing, key and screen loggers, and SQL injection attacks. According to The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, a report published by the U.S. Department of Homeland Security in 2006, "Credible estimates of the direct financial losses due to "phishing" alone exceed a billion dollars per year."

The largest security breach to date was disclosed in January 2009. The case involved Heartland Payment Systems Inc. Heartland processes more than 100 million card transactions per month for 250,000 clients. On August 17, 2009 Albert Gonzalez, 28, of Miami Florida was charged by the Department of Justice with stealing data from 130 million debit and credit card holders. According to the indictment, Gonzales and international co-conspirators used an intricate hacking technique called an "SQL injection attack," which seeks to exploit a computer network by finding a way around firewalls to steal credit and debit card information. It turns out that Gonzales and his thugs were also responsible for the highly publicized intrusion of TJ Maxx card holders. Heartland expensed $144.2 million to consummate the settlement of claims.

Credible estimates of the direct financial losses due to "phishing" alone exceed a billion dollars per year."

- U.S. Department of Homeland Security

Contact Centers and Identity Theft

Contact centers can become unsuspecting targets of cyber criminals. Outbound telemarketing centers, inbound centers that engage in up-selling and/or cross -selling, service providers, and collection companies always take payment in the form of credit or debit cards. The card information is entered into a CRM or other sales automation software and recorded by voice and screen recorders. And there it resides - thousands and even millions of card records inviting remote criminals or even greedy employees to extract for personal gain or sell into a sophisticated secondary market.

Think it can't happen?

An investigative reporter from the BBC (British Broadcasting Company) posed as a fraudster seeking to buy credit card records from a fence in Delhi. The Indian conspirator offered to sell details on hundreds of plastic cards for $10 each. The video shows a buy being made and money changing hands. The reporters bought 50 cards as a "sample" with the hint that a larger buy would follow if the cards checked out. The names were later traced to a call center taking service calls for U.S.-based Symantec Corporation.

Also in India, local police in the city of Pune arrested 12 persons associated with a call center operated by outsourcer MphasiS for allegedly siphoning off $350,000 from the Citibank accounts of four US citizens. Some employees gained the confidence of customers and obtained their PIN numbers to commit fraud. They did this under the guise of helping the customers out of difficult situations.

In 2006, an employee at the HSBC Data Processing Center in Bangalore, India was arrested for allegedly passing personal customer information. As a result UK bank customers lost approximately USD$425,000. The incident cast a black eye on outsourcing work to India and may affect future projects being considered to India and other parts of Asia.

According to IT Business News, the HSBC incident was brought to notice by some of its customers in England who complained that money was transferred out of their accounts without their knowledge. The lessons from these incidents at HSBC have prompted several security and quality assurance policies aimed to protect customers' sensitive personal information. A dedicated team of compliance officers have been specially trained and deployed to ensure that breaches in security and access of customer information will be minimized.

According to press reports, Alaska Airlines and Horizon Air had to notify 1,500 of their customers that their credit cards may have been misused by a former call center employee. The former employee is alleged to have taken the card information provided from some of the airlines' customers to pay for reservation changes. Rather than process the payment on behalf of the airlines, the individual is alleged to have diverted the funds to a personal account.

In the first example, Symantec followed up with a thorough investigation of the underground economy. Among the findings from their 68-page report was that the BBC reporters grossly overpaid for customer card data. Quoting from the report, "Credit cards are also typically sold in bulk, with lot sizes from as few as 50 credit cards to as many as 2,000. Common bulk amounts and rates observed by Symantec during this reporting period were 50 credit cards for $40 ($0.80 each), 200 credit cards for $150 ($0.75 each), and 2,000 credit cards for $200 ($0.10 each)."

Payment Card Industry Response

In order to reduce fraud, the Payment Card Industry (PCI), which consists of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. established the PCI Security Standards Council in September 2006. The aim of the council was to establish a set of rules that merchants and service providers must comply with in order to accept payments through the credit and debit card apparatus set up by the card vendors. While the Council is managed by the card industry, membership is open to any organization that participates in the payment processing system, including merchants, processors, POS vendors, and financial institutions.

In 2006, an employee at the HSBC Data Processing Center in Bangalore, India was arrested for allegedly passing personal customer information. As a result UK bank customers lost approximately USD$425,000.

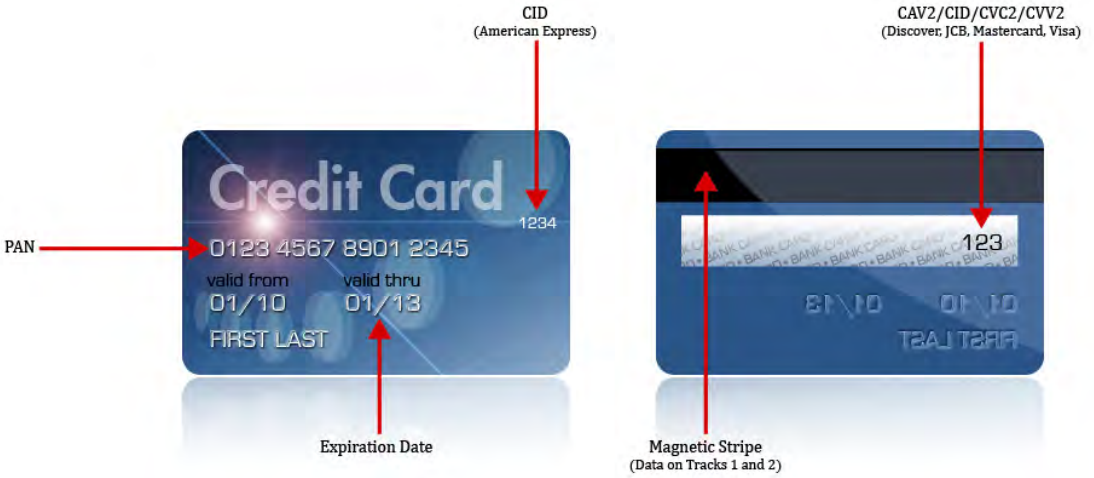
In order to reduce fraud, the Payment Card Industry (PCI), which consists of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. established the PCI Security Standards Council in September 2006.

The Council subsequently issued a Data Security Standard (PCI-DSS) which details security requirements for members, merchants and service providers that store, process or transmit cardholder data. The original PCI regulations specifically forbade storing primary account numbers (PAN), PIN numbers, service codes, expiration dates, and other specified identifiers unless they met PCI-DSS encryption standards. Payment processors, service providers and merchants that process more than 20,000 e-commerce transactions and over one million regular transactions are required to engage a PCI-approved Qualified Security Assessor (QSA) to conduct a review of their information security procedures and scan their Internet points of presence on a regular basis. However, no organization that accepts cards issued by the founding members of the council is exempt from compliance.

While the standard is primarily aimed at cardholder information in data bases, contact centers can easily become unsuspecting violators. This is because of the practice of collecting and entering card data into order entry systems and archiving private customer information in call and data recording systems. Initially, the PCI-DSS allowed the voice and data recording and storage of sensitive card information provided that certain safeguards were in place, such as encryption, firewalls, and need to-know authorizations. The precise levels of encryption are spelled out in the standard as are data categories that may be stored when properly encrypted.

PCI-DSS Requirements Impacting Call Recording – Do Not Record Validation Codes

On October 28, 2010 the Standards Security Council issued a clarification that states that it is a violation of the PCI-DSS to store card validation codes and the full contents of and track from the magnetic stripe located on the back of the card. This includes the cardholders name, the primary account number (PAN), and expiration date, and personal identification number (PIN) after authorization even if encrypted. Note: it is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.



The card validation value code is the three or four digit number that is usually imprinted next to the signature line on the back of the payment card. On American Express cards, the security code is on the face of the card.

The Card Verification Code (referred to as CAV2, CVC2, CVV2, or CID) must not be retained post authorization, cannot be stored in a standard digital audio or video format (e.g. wav, mp3, mpg, etc.), and a proper disposal procedure must be in place. If the recording solution cannot block the audio or video from being stored, the code must be deleted from the recording if it is initially recorded.

Payment processors, service providers and merchants that process more than 20,000 e-commerce transactions and over one million regular transactions are required to engage a PCI-approved Qualified Security Assessor (QSA) to conduct a review of their information security procedures and scan their Internet points of presence

On October 28, 2010 the Standards Security Council issued a clarification that states that it is a violation of the PCI-DSS to store card validation codes and the full contents of and track from the magnetic stripe located on the back of the card.

When it is absolutely necessary that your organization retain card verification codes, you will need to demonstrate to your QSA (Qualified Security Assessor) and your acquiring bank that:

> You perform, facilitate or support issuing services - it is allowable for these types of organizations to store sensitive authentication data only if they have a legitimate business need to store such data. It should be noted that all PCI-DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with PCI-DSS and specific payment brand requirements.

Telephone order takers require the validation code as well as the PAN (Primary Account Number) and expiration date in order to secure authorization from the card issuer. Without that number, cyber thieves cannot make eCommerce purchases or illegally transfer funds out of the cardholders' accounts. The standards committee made the change because of the availability of sophisticated malware that could penetrate encryption algorithms.

Telephone order takers require the validation code as well as the PAN (Primary Account Number) and expiration date in order to secure authorization from the card issuer. Without that number, cyber thieves cannot make eCommerce purchases or illegally transfer funds out of the cardholders' accounts.

The latest PCI-DSS standards require that PAN must be rendered unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

Other Important PCI-DSS Requirements that Impact Call Recording

Requirement 4 and Subsection 4.1 require that strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet protocol security (PISEC).

Requirement 7 and Subsection 7.1 require that access to computing resources and cardholder information only to those individuals whose job requires such access, e.g. for strong business reasons. Organizations should create a clear policy for data access control to define how, and to whom, access is granted.

Requirement 7 and Subsection 7.2 require organizations that accept payment cards to establish a mechanism for systems with multiple users that restricts access based on a user's need-to-know and is set to "deny all" unless specifically allowed.

Requirements 8 and Subsection 8.1 require organizations that accept payment cards to Assign a unique ID to each person with computer access before allowing them to access system components or cardholder data.

Subsection 8.3 requires a two-factor authentication for remote access to the network by employees, administrators and third parties.

Subsection 8.5 requires proper user authentication and password management for users and administrators on all system components.

Subsection 8.5.16 requires organizations that accept payment cards to authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

Requirements 10 and Subsection 10.1 require card acceptors to track and monitor all access to network resources and card holder data and establish a process for linking all access to system components to each individual user.

Requirement 10 and Subsection 10.2 require card acceptors to implement automated audit trails for all system components to reconstruct events such as user access to cardholder data, access to audit trails, use of authentication mechanisms, and the like.

If an important part of the agent's job is to accept and/or solicit sales, then the question becomes: how do we prevent recording and storing of sensitive authentication data and the full contents of any magnetic stripe track?

Available Alternatives

Alternative 1: Cease recording all sales and transaction calls.
Alternative 2: Train agents to disable the recording function when card data is required then restart after the transaction is completed.
Alternative 3: Require agents to delete the section of the recording that includes the authorization code.
Alternative 4: Third-party devices that require the caller to enter card details via their touchtone pad.
Alternative 5: Do nothing.
Alternative 6: Invest in call recording systems that automatically mask and mute sensitive card details.

Alternative 1 - Cease Recording

The notion of simply halting the practice of recording all calls and related data that may involve the capture of interactions containing sensitive information is certainly an approach that will be compliant. Thieves cannot steal information that was never stored. However, the trade-off is too severe. You must be able to manage call quality and there are laws and regulations that many centers, particularly outbound, need to comply with. Full-time recording is the only way to measure compliance.

Alternatives 2 and 3 - Agent-driven Compliance

At the final stage of taking credit card data, recorded agent could transfer the call to an unrecorded extension where a second agent takes aspects of the customer credit card data such as the CVV number for bank verification. Some recording systems allow the agent to manually pause and resume the recording via buttons on their screen or handset.

These approaches may work but it adds a burden to agents and is obviously error-prone. There may also be a question of whether relying on employee actions would pass muster with the payment card council which prefers solid, technology-based solutions.

Alternative 4 - Transfers to Third Party Devices

There are third party devices that can be bolted onto an existing recorder. This method works by requiring the caller to enter card details manually via the touchtone pad. The idea has merit, since little agent intervention is required and the system automatically masks card entries on the agent screen and blocks the DTMF tones from being recorded. Agents could also transfer calls to an IVR platform for taking such details as CVV for bank verification. The downsides are the paucity of choices, risk of user error, the unnatural interruption of call flow, the need to manage an adjunct device that's not part of an integrated solution, and an added cost per transaction.

You must be able to manage call quality and there are laws and regulations that many centers, particularly outbound, need to comply with. Full-time recording is the only way to measure compliance.

At the final stage of taking credit card data, recorded agent could transfer the call to an unrecorded extension where a second agent takes aspects of the customer credit card data such as the CVV number for bank verification.

Alternative 5 - Do Nothing

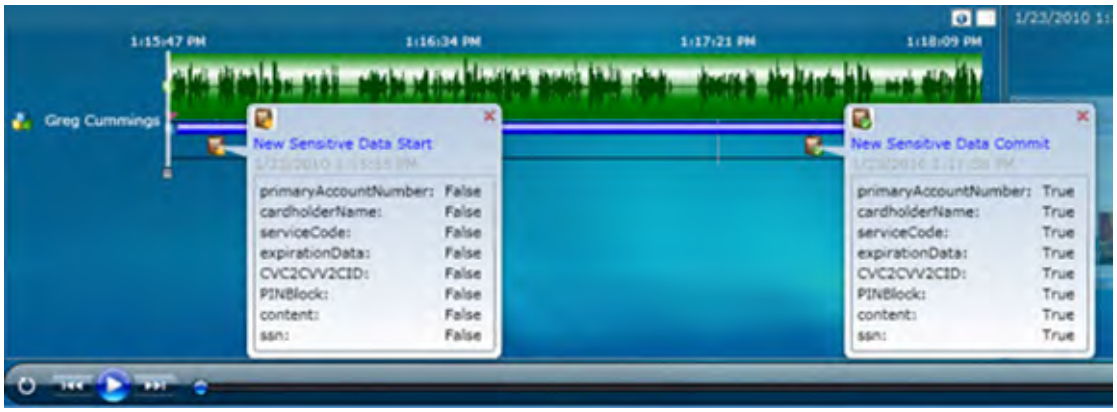
The 'do nothing" option appears to be the favored choice at this point. In the 2009 Data Breach Investigations Report conducted by the Verizon Business RISK Team researchers uncovered 90 confirmed breaches within their 2008 caseload encompassing an astounding 285 million compromised records and 81% of businesses were not Payment Card Industry (PCI) compliant. The most common form of data breach was compromised payment cards, with retail and financial services accounting for six out of ten of the security breaches.

A 2009 poll of United Kingdom call center managers found that more than 19 in 20 call centers do not delete or mask credit card details in their call recordings, which is a violation of the Payment Card Industry Data Security Standard. Of the 133 call center managers contacted for the survey, only 3 percent indicated compliance with the guidelines. Among the reasons for failing to abide by PCI-DSS, 61 percent said they were unaware of the standards, 18 percent were aware but said they couldn't comply for technical or budgetary reasons, 11 percent were aware but chose not to follow them, and 6 percent were aware and were working toward compliance.

A 2009 poll of United Kingdom call center managers found that more than 19 in 20 call centers do not delete or mask credit card details in their call recordings, which is a violation of the Payment Card Industry Data Security Standard.

Alternative 6 - Invest in Call Recording Systems that Automatically Mute and Mask Sensitive Card Details

A handful of leading call recording vendors have developed truly integrated solutions. With the VPI solution; for example, the recorder uses desktop analytics to monitor application screens in use by the agent during the interaction (to include CRM, sales automation or other applications) to automatically sense when the agent is entering screens or fields where sensitive information must be entered, without the need for a costly back-end integration to those systems.



The VPI Fact Finder desktop analytics application can detect when an agent enters a screen with sensitive information, when sensitive information is inputted, and when they leave a screen containing sensitive information.

A handful of leading call recording vendors have developed truly integrated solutions. With the VPI solution; for example, the recorder uses desktop analytics to monitor application screens in use by the agent during the interaction to automatically sense when the agent is entering screens or fields where sensitive information must be entered, without the need for a costly back-end integration to those systems.

The VPI Solution

The VPI recording system then automatically classifies calls containing sensitive card holder information and provides organizations with four options to help effectively balance their PCI requirements with liability, quality management and other regulatory requirements:

VPI's Four Options

Option 1 - 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

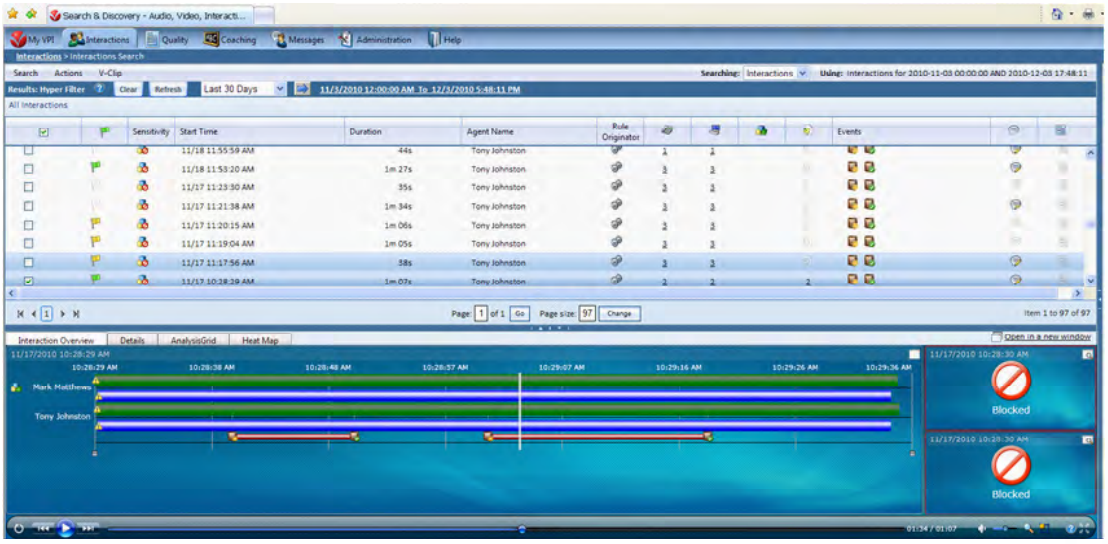
ID, DNIS, sales or collections $ amount, number of transfers, or even handle time of key processes within the call that led up to the successful transaction, is made available in interactive reports and analysis of key business issues and opportunities.

Option 2 - Roles-based access to recorded files containing sensitive information

For organizations that are permitted to record entire calls (companies that perform, facilitate, or support 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 (Requirement 3.2 and 8.5).

Option 3 - Roles-based muting/masking upon playback

For organizations required to record calls (e.g. those per 3.2), and who would also like to playback for quality and training purposes, VPI has a solution that allows access to recordings while controlling the access to sensitive information. The solution uses VPI's Fact Finder technology to tag the sensitive events and upon playback mutes the audio and masks the screen video during segments of the call containing sensitive data. Agents, supervisors and QA analysts without full access rights are able to playback the call while hearing and seeing 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 recorded files in their entirety. (Requirements 3.2, 7.1 and 7.2)



VPI solution has the ability to mute out the audio and mask out the screen video during segments of the call containing sensitive data upon playback

Option 4 - Permanent muting/masking during segments of the call containing sensitive info

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 that will comply 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 and unavailable to all system users regardless of user authorization privileges.

NOTE: VPI expects to make this feature generally available in 2011. Timeline for this feature is subject to change)

For organizations required to record calls for liability and regulatory requirements, and who would also like to playback for quality and training purposes, VPI has a solution that allows access to recordings while controlling the access to sensitive information.

VPI Response to Requirement 4 – Encrypt transmission of cardholder data across open networks

The intent of strong cryptography is that the encryption be based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm). VPI supports AES 256 data and file encryption using 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. (Requirement 4.1)

VPI supports AES 256 data and file encryption using 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

VPI Response to Requirement 7 – Restrict access to card holder data by business need-to- know

The VPI system is capable of supporting 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.

VPI Response to Requirement 8 – Assign a unique ID to each person with computer access

The VPI system has unique user system log-in with an audit trail showing who has logged into the system, searched for calls, played back or exported calls and when. The status of all activities can be also monitored in heat maps that present audit log data in a visual, easy-to-analyze manner.

VPI Response to Requirement 10 – Track and monitor all access to network resources and card holder data

This is achieved by providing an audit trail of all user activities – linking specific actions to specific users, thereby providing high degree of visibility and transparency. (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. (Requirement 10.2)

Consequences of Non-Compliance

Non-compliance risks revocation of card acceptance privileges and violation of state laws. Loss of card acceptance privileges could easily spell the death knell for retailers, service providers, and collection agencies. In fact, it is difficult to think of any type of business, nonprofit, or government revenue collection entity that does not rely on payment cards. The card issuers have the authority to revoke card privileges through their contracts.

Non-compliance risks revocation of card acceptance privileges and violation of state laws. Loss of card acceptance privileges could easily spell the death knell for retailers, service providers, and collection agencies. In fact, it is difficult to think of any type of business, nonprofit, or government revenue collection entity that does not rely on payment cards. contracts.

The other possibility is violation of state laws. As of this time, three states; Minnesota, Nevada, and Washington, have codified payment card industry data security standards. Quoting from the Washington state law, "A processor, business, or vendor will be considered compliant, if its payment card industry data security compliance was validated by an annual security assessment, and if this assessment took place no more than one year prior to the time of the breach." This requirement is not contingent on the volume of transactions.

The Nevada law requires that companies doing business in the state of Nevada that accept payment cards must be compliant with the Payment Card Industry Data Security Standard (PCI-DSS). The law also requires that companies retaining personal data, including Social Security numbers (SSNs), driver's license numbers or account numbers together with passwords must use encryption if they send the information outside of the company. The Nevada law is reported to be the only law that actually mandates PCI-DSS compliance. The language "doing business in the state of Nevada" is very broad and presumably could include companies not domiciled in the state. Other states are considering legislation that would codify PCI-DSS.

Advisable Best Practices

Obviously, if your business or organization accepts payment cards, it is in your best interest to become compliant with PCI-DSS. In addition to the standards, there are many other actions you can take to help prevent breaches of sensitive card and personal information.

1. Work with your information technology department before implementing contact center-specific solutions. Compliance is an organization-wide commitment. IT may have an overall security plan that contact centers must adopt. For example, individuals that require access to archived calls that may include card data must be specifically authorized to access this information.
2. Make sure your order entry, new customer applications, and any other customer data bases that your agents frequently access mask out credit, debit, and other sensitive information.
3. Limit the amount of time that card information is kept in the call recording server database (both voice and screen recordings). It may be necessary for corporate governance, legal and QA departments to work out a compromise between what is needed to adhere to the PCI-DSS and regulatory compliance requirements (requirement 3.1).
4. Ensure that proper user authentication is implemented for staff, agents and administrators (requirement 3.2).
5. Segment contact center operations so that a limited number of employees have access to payment card data. For example, payment card information can be entered by a sales agent, but a customer service representative may have access only to the masked PAN (requirements 8.1 and 8.5).
6. Be very careful about who you hire. If the agent will be accepting card payments or otherwise be privy to sensitive personal information, conduct a thorough background check before extending a payment offer.
7. Make clear that unauthorized disclosure of sensitive personal information is grounds for termination.
8. If an employee is terminated or resigns, immediately change the password to that individual's work station. Don't wait until the end of the work day.
9. If you are working with outsourcers, remember that PCI-DSS is an international requirement. The outsourcer must also be compliant.
10. Understand the data security precautions taken by outsourcers.
11. Do not allow thumb drives or any other portable storage devices into your contact center.
12. Agents or other employees should never open emails from unknown sources. This is a favored method by cyber criminals for installing key loggers and other malware.
13. Make sure you maintain strict processes that prevent agents from jotting down card numbers for later entry into the customer data base.
14. Contact center agents should be discouraged from revealing their occupation on social networking sites. You don't want them to become unsuspecting targets.
15. Ensure that agents and supervisors do not share user ID's and passwords. Each user must be uniquely identified by their own login credentials. This information should be encrypted when stored in any computer systems.
16. Review your CRM, sales automation, collections and order entry systems to assure that complete card numbers and the security code are not displayed. The security code should never be stored.
17. Find out how your current recording software handles PCI-DSS compliance. Some vendors do not have a solution. Others may require deleting entire interactions that involve card transactions, making it impossible to conduct quality evaluations on these calls or retrieve them for compliance or verification purposes.
18. Restrict access to QA recording and CRM data containing payment card data based on the user's log-in account and corporate role.
19. Ensure that stored recordings are not played back over a speaker phone if payment card information is included.
20. If you are considering a new interaction recording system, look into the approach adopted by VPI. VPI provides encryption at no extra cost. For companies that prefer a more flexible approach, VPI's VPI CAPTURE call recording software can automatically detect when an agent enters a screen where a credit card field is to be filled out and then mask both the voice and screen entries for the duration of the agent's activities while working in those screens. The security code can be permanently deleted from both, voice and screen recording. The system masks the sensitive information in voice and data recordings, which can only be accessed by authorized personnel.

If you are working with outsourcers, remember that PCI-DSS is an international requirement. The outsourcer must also be compliant.

Ensure that employees do not share user ID's and passwords. Each user must be uniquely identified by their own login credentials. This information should be encrypted when stored in any computer systems.

VPI supports AES 256 data and file encryption using 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.

Best Practices for Securing At-Home Agents

Contact center at-home agent programs are rapidly growing in number and size due to their attractive benefits of reducing operational costs, increasing performance and improving the customer experience. However, using at-home or remote workers carries with it a much greater security risk. When utilizing and recording at-home or remote workers, the following are additional advisable practices:

1. Be sure that the same level of firewall, corporate anti-virus protection, security patches, and definition files are extended to remote agents and supervisors' PCs. (Requirements 1.4, 5.1 and 6.1)
2. Remote workers should be forbidden from copying, moving, and storing cardholder data onto hard drives or moveable electronic media when accessing cardholder data. (Requirement 12.3.10)
3. Ensuring remote agents and supervisors use a two-factor authentication process. (Requirement 8.3)
4. Use strong network encryption protocols such as Secure Socket Layer and Transport Layer Security (SSL/TLS) or Internet Protocol Security (IPSEC) to provide secure transmission of the VoIP voice stream and data over the public network. (Requirement 4.1)
5. Ensure each at home agent and supervisor is using a VPN connection into the corporate network with strong encryption protocols such as SSL/TLS. (Requirement 4.1)
6. Require remote agents and supervisors to encrypt their wireless networks using strong cryptography (Requirement 2.1.1 and 4.1.1). As of June 30, 2010, the Wired Equivalent Privacy (WEP) protocol is no longer permissible for any new wireless implementations (Requirement 4.1). The use of WPA2 is recommended.
7. If not using an enterprise VoIP-based telephone solution, require agents to use analogue telephone lines when talking with customers.
8. At-home agents should not use consumer VoIP telephone systems (such as Vonage) because their communications may not be encrypted. (Requirement 4.2)
9. Ensure that payment card information is never sent over an unencrypted medium such as chat, SMS/text or email or other non-encrypted communication channels.
10. Ensuring that at-home agent and supervisor PCs have personal firewalls installed and operational. (Requirement 1.4)
11. Ensure that at-home agent and supervisor PCs have the latest approved security patches installed.
12. Require agents and supervisors to use only company-supplied systems. (Requirement 12.3)
13. Monitor at-home agents more often than in-house agents. (Requirement 12.3)
14. Annually review all security policies and procedures with all agents and require at-home agents. to acknowledge the security requirements as part of their daily sign-in process. (Requirement 12.6)

Dilemma for Contact Centers

PCI-DSS compliance is only one of a growing list of laws, regulations, and industry standards that contact centers need to consider. There are several regulations that require or strongly recommend that calls be recorded in their entirety.

- 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

Ensure that payment card information is never sent over an unencrypted medium such as chat, SMS/text or email or other non-encrypted communication channels.

Monitor at-home agents more often than in-house

PCI-DSS compliance is only one of a growing list of laws, regulations, and industry standards that contact centers need to consider. There are several regulations that require or strongly recommend that calls be recorded in their entirety.

Telemarketing Sales Rule

The Telemarketing Sales Rule requires a consumer's express verifiable authorization for use of bank account information to obtain payment through phone checks or demand drafts. This can be done via confirmation by a call recording of the consumer giving authorization or advance written authorization.

The recorded authorization and written confirmation must include the date and amount of the draft(s), the name on the account from which the funds will be paid, the number of draft payments authorized, if more than one, a telephone number answered during normal business hours tat the consumer can call with questions, and the date of the consumer's authorization. Many states require advance consent of the recorded party; the recorded confirmation must show that the consumer understands and acknowledges each term of the transaction and authorizes it.

The Telemarketing Sales Rule requires a consumer's express verifiable authorization for use of bank account information to obtain payment through phone checks or demand drafts. This can be done via confirmation by a call recording of the consumer giving authorization or advance written authorization.

FSA (Financial Services Authority) Rules

The United Kingdom Financial Services Authority (FSA) published rules in March of 2009 requiring firms to record telephone conversations and other electronic communications including email and instant messages relating to trading orders and the conclusion of transactions in the equity, bond, and derivatives markets. The rules were established as part of the FSA's efforts to combat market abuse, particularly insider dealing and to help deter and detect market manipulation and abuse in the United Kingdom. The FSA rules are in accordance with Markets in Financial Instruments Directive (MiFID) general record keeping standards. The rules require organizations to retain their recorded calls and communications 6 months. This is expected to be longer in future regulations (the initial recommendation was three years). The FSA must be able to access recorded calls readily.

Other regulated organizations involved in retail activities such as banking, insurance, loans or mortgages will still have the option to record calls or keep alternative records however recording is likely to become mandatory in the near future. Insurance companies complying with directives such as the Insurers Conduct of Business (ICOB) are already advised to introduce call recording. Companies will also find in 99% of cases the Financial Ombudsman Service will favor the client's word if the organization cannot provide a recorded transcript of relevant telephone calls.

The United Kingdom Financial Services Authority (FSA) published rules in March of 2009 requiring firms to record telephone conversations and other electronic communications including email and instant messages relating to trading orders and the conclusion of transactions in the equity, bond, and derivatives markets.

BASEL II

BASEL II recommendations and policies, developed by the BASEL committee consisting of representatives from all G-20 major economies as well as other major banking locales such as Hong Kong and Singapore, prescribes that banks and their outsourced contact centers implement Operational Risk Management practices. The BASEL committee defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. In order to protect from the official event types defined by BASEL II, including Internal Fraud (misappropriation of assets, tax evasion, intentional mismarking of positions, bribery), External Fraud (theft of information), Employment Practices and Workplace Safety (discrimination, workers compensation, employee health and safety), Clients, Products, & Business Practice- market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning), and Execution, Delivery, & Process Management (data entry errors, accounting errors), many banks require full-time call recording and long-term storage of their recorded interactions.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act extensive guidelines for the documentation of business processes and transactions, mandating that businesses create and maintain electronic records as part of their regular business processes. To help ensure compliance with Sarbanes-Oxley, many organizations currently record and store all their calls in their entirety. Maintaining an electronic record of telephone calls in the

same manner as emails helps to ensure compliance with Sarbanes-Oxley and simplifies the discovery and auditing processes, reducing the potential for abuse or mistakes.

Gramm-Leach-Bliley Financial Services Modernization Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. Under the Safeguards Rule, financial institutions must create and follow a written information security plan that details how they will protect the non-public information, such as account and identification numbers, of their current and former customers.

Call recording solutions make it easy to incorporate voice-based communications as part of an organization's GLBA compliance plan. In addition, companies that factor call recording into their electronic records plan have an added layer of security, knowing that every aspect of their business is compliant, rather than just their written documents and transactions.

Truth in Lending Act (TILA) & Fair Debt Collections Practices Act (FDCPA) Acts

Full-time call recording is also frequently mandated to ensure contact center employees are accurately disclosing information required by the Truth in Lending Act and complying with collection practices required by the Fair Debt Collections Practices Act.

Full-time call recording is frequently mandated to ensure contact center employees are accurately disclosing information required by the Truth in Lending Act and complying with collection practices required by the Fair Debt Collections Practices Act.

Barclaycard Guidance

Balancing the need for PCI compliance with other regulations, laws and risk management requirements with the quality management requirements can pose a dilemma. Barclaycard prepared a very informative white paper that, among other things, advises that:

Call centre managers will need to ensure that the PAN is masked when displayed (i.e. first 6 and last 4 digits). This is part of requirement 3.3 and may include:

- Restraint access to QA/recording and CRM data containing payment card data based on the user's log-in account and corporate role; for example, providing screen recording playback interfaces where the payment card information is displayed only to the managers and compliance officers during legal discovery, and have it blacked out (masked) for all other supervisors and QA specialists.
- Segmenting contact centre operations so that a limited number of agents have access to payment card data; for example, payment card information may be entered by a sales agent but a customer service representative will only have access to the masked PAN.

Readers are encouraged to read the entire paper for more suggestions.

Executive Summary

Identity theft is a massive problem in the United Sates and globally. In response, the payment card industry has established clear rules to help assure that critical financial and identification data is protected from menaces both outside and within the enterprise. The PCI-DSS requirements must be adhered to by every organization - regardless of size - that accepts payment cards. There are direct impacts on contact enters, which in the past have proved to be fertile grounds for extracting payment card details from unsuspecting customers.

In this paper we highlighted some sound practices to help assure data security. We also noted that the widespread practice of recording vice and data interactions may result in a breach of the data security standards and even a violation of certain state statues unless important precautions are taken. Choosing to

abandon interaction recording altogether or limit it to non-transactional calls is not an option. Besides the obvious need to assure consistent call quality there are many other laws And regulations where recording is a legal requirement or the only practical means of establishing compliance.

It is important that any call recording system purchased now can cope with both current and future changes in laws and industry standards and that the recording solution facilitate best practices. Suppliers must be able to prove that their products will help you assure compliance today and have the flexibility to adapt to future changes. The best solution is to avoid recording of the validation code altogether, after approval. The VPI solution provides this option.

About the Author

Dick Bucci is Principal of Pelorus Associates where he specializes in contact center technologies. He has authored ten in-depth reports on workforce optimization applications and over 30 white papers. As one of the industry's foremost thought leaders, his articles and observations have appeared in trade and business publications around the world. Dick has over 30 years of experience in the telecommunications industry.

About VPI

VPI is the world's premier provider of call recording, analytics and workforce optimization solutions for enterprises, contact centers, trading floors, government agencies, and first responders. For more than a decade, VPI has been providing proven technology and superior service to more than 1,500 customers in 50 countries. VPI's award-winning VPI EMPOWER software is an essential component for any organization that strives to enhance the customer experience, increase workforce performance, improve business efficiency and manage compliance. VPI EMPOWER leverages VPI Fact Finder™, a ground-breaking desktop screen analytics technology that automatically detects events and data directly from application screens being used by employees and tags them to appropriate points within recorded interactions. With VPI EMPOWER, organizations of all sizes now have the ability to rapidly identify the root cause of important trends and issues via targeted analysis and evaluation from anywhere – all from an intuitive, personalized Web-based portal interface. In addition, the secure solution leverages advanced file and data encryption, is built around the principles of open, service-oriented architecture, and is platform independent to integrate seamlessly into any existing and evolving infrastructure in just weeks, resulting in compound reduction of costs and a significant and rapid Return on Investment. For more information, call 1-800-200-5430 visit **www.VPI-corp.com/PCI**

References

- The FTC in 2009, annual report of the Federal Trade Commission (March, 2009)
- The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond: A Joint Report of the US Department of Homeland Security, SRI International Identity Theft Technology Council, the Anti-Phishing Working Group, and IronKey, Inc. (September, 2006)
- Symantec Report on the Underground Economy July 07 - June 08, Symantec Corp., (November 2008)
- Navigating PCI-DSS - Understanding the Intent of the Requirements, Version 2.0 Payment Card Industry (PCI) Data Security Standards, Payment Card Industry (PCI) (October, 2010)
- 2009 Data Breach Investigation Report, Verizon Business RISK Team
- Safe and Sound, Processing Telephone Payments Securely, BarclayCard (April, 2010)

It is important that any call recording system purchased now can cope with both current and future changes in laws and industry standards and that the recording solution facilitate best practices. Suppliers must be able to prove that their products will help you assure compliance today and have the flexibility to adapt to future changes.

Contact VPI at
Info@VPI-corp.com
1.800.200.5430
www.VPI-corp.com