Oreka Security
&
PCI Compliance

OrecX
Open Source Recording

Contents

OrecX
Open Source Recording

Oreka Security and Compliance

Oreka offers multiple levels of security:

- **Secure Access To Recordings** - Access to recordings is end-to-end secured (both at rest and in transit) and restricted to logged in users.
- **Media Encryption** - OrkAudio may be configured to encrypt files using the Blowfish 256 encryption algorithm. Files can thus be played back only through the web portal.
- **OWASP Level 2 Compliance** – At the request of a large European Bank, Oreka's security was tested by third party penetration testing company, both manual testing (a real hacker trying to get in) and automated penetration testing - secure Oreka against Cross-Site Request Forgery attacks (CSRF), Session Fixation attacks, Cross-Site Scripting attacks (XSS), Horizontal and Vertical Brute force attacks and much more. Oreka met requirements set forth by the bank.
- **Tamper proof hashing** of media files. A mathematical hash of every audio file is computed at recording completion and stored in the database. This makes it easy to check whether a given file has been altered compared to when it was recorded.
- **Secure access to the web portal** via SSL (https access).
- **Download/Export privilege** can be revoked for classes of users so it's possible to have these users only be able to replay via the web portal.
- **Authentication Rules** for user login access such as locking user temporarily or permanently after a given number of unsuccessful login attempts, and password rules for ensuring a minimum level of complexity in passwords.
- **PCI Compliance** - Recording of both Screen and Audio can be paused via API or web user interface e.g. while credit card numbers are being received over the phone and entered into the information system by CSRs. This is the most effective way of respecting PCI compliance. Credit card numbers do not need to be protected since they are simply not recorded (link for more detail on PCI Compliance: http://files.orecx.com/docs/orecx-pci-compliance.pdf
- **Searchable Audit Trail** of all important actions that happen in the system.
- **Passwords** are stored with state of the art bcrypt hashing algorithm - staying safe if a database ever gets compromised.

OrecX
Open Source Recording

Payment Card Industry - Data Security Standard (PCI-DSS)

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.

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 PCIDSS 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 & Call Recording

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.

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.

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.

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.

ORECX Call recording & PCI

Oreka TR, a software product from OrecX LLC that includes call and screen recording and Quality Monitoring for Call Centers gives you all the tools necessary to achieve full PCI compliance.

ORECX call recording 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.

While OrecX LLC provides full technical support in reaching PCI compliance, PCI compliance depends on properly using configuration settings and/or API commands as well as making sure that the underlying infrastructure on which Oreka TR is running is also PCI compliant and is the sole responsibility of the Oreka TR customer or integrator.

OrecX PCI Option overview

Security features that can be used in order to achieve PCI compliance are listed below.

- Secure access to the recordings, i.e. access by simple URL can be prohibited in general and allowed only for valid users who are logged into the web portal.
- Media Encryption: OrkAudio may be configured to encrypt files using the Blowfish 256 encryption algorithm. Files can thus be played back only through the web portal
- Secure access to the web portal via SSL (https access).
- Download/Export privilege can be revoked for classes of users so it's possible to have these users only be able to replay via the web portal.
- Authentication Rules for user login access such as locking user after a given number of unsuccessful login attempts, and password rules for ensuring a minimum level of difficulty in passwords.
- Recording of both Screen and Audio can be paused via API or web user interface e.g. while credit card numbers are being received over the phone and entered into the information system by CSRs. This is the most effective way of respecting PCI compliance. Credit card numbers do not need to be protected since they are simply not recorded. We also strongly recommend automated pausing/resuming via API, which typically represents some integration work with the CRM software (e.g. pause recording when entering Credit Card number field on the CRM screen, resume when leaving it).

OrecX
Open Source Recording

OrecX & Specific PCI requirements

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).

ORECX & Requirement 4 – 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). ORECX supports Blowfish 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)

7 and 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.

ORECX & Requirement 7 – The ORECX 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.

Requirement 8 & 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.

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

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

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.

ORECX & 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 ORECX 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)

Requirement 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.

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, etc.

OrecX
Open Source Recording

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.

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 PCIDSS. In addition to the standards, there are many other actions you can take to help prevent breaches of sensitive card and personal information.

- 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.
- 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.
- 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).
- Ensure that proper user authentication is implemented for staff, agents and administrators (requirement 3.2).
- 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).
- 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.
- Make clear that unauthorized disclosure of sensitive personal information is grounds for termination.
- 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.
- If you are working with outsourcers, remember that PCI-DSS is an international requirement. The outsourcer must also be compliant.
- Understand the data security precautions taken by outsourcers.
- Do not allow thumb drives or any other portable storage devices into your contact center.
- 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
- Make sure you maintain strict processes that prevent agents from jotting down card numbers for later entry into the customer data base.

- Contact center agents should be discouraged from revealing their occupation on social networking sites. You don't want them to become unsuspecting targets.
- 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.
- 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.
- 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.
- Restrict access to QA recording and CRM data containing payment card data based on the user's log-in account and corporate role.
- Ensure that stored recordings are not played back over a speaker phone if payment card information is included.
- If you are considering a new interaction recording system, look into the approach adopted by ORECX. ORECX provides encryption at no extra cost. For companies that prefer a more flexible approach, ORECX's Oreka SC 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.

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:

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)
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)
Ensuring remote agents and supervisors use a two-factor authentication process. (Requirement 8.3)
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)
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) PCI Compliance & Call Recording o r e c x . c o m s a l e s @ o r e c x . c o m Page 9
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.
If not using an enterprise VoIP-based telephone solution, require agents to use analogue telephone lines when talking with customers.
At-home agents should not use consumer VoIP telephone systems (such as Vonage) because their communications may not be encrypted. (Requirement 4.2)
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.
Ensuring that at-home agent and supervisor PCs have personal firewalls installed and operational. (Requirement 1.4)
Ensure that at-home agent and supervisor PCs have the latest approved security patches installed.
Require agents and supervisors to use only company-supplied systems. (Requirement 12.3)
Monitor at-home agents more often than in-house agents. (Requirement 12.3)
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)

OrecX
Open Source Recording

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

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.

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.

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 mis-marking 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.

OrecX
Open Source Recording

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.
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.

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.
In this paper we highlighted some sound practices to help assure data security. We also noted that the widespread practice of recording voice 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 OrecX solution provides this option.