2012

DMG CONSULTING LLC

Payment Card Industry Data Security Standards (PCI-DSS) Guide for Contact Center Managers

January 2012

Reprinted for

OAISYS®
The Right Choice for Call Recording

Table of Contents

Executive Summary

Credit and debit cards, which are referred to as payment cards, are the most common form of debt payment. According to the U.S. Federal Reserve Bank of Boston, more than 50% of all transactions are made with payment cards, and 63% of payment card transactions involve a retailer or other consumer-related organization. 73% of U.S. households have at least one payment card, and the average is three. (1)

National, state and local governments require companies to safeguard consumer information, including the information on payment cards. In response, the largest payment card brands established the Payment Card Security Council and the Payment Card Industry Data Security Standard (PCI-DSS). This standard is a set of voluntary requirements and provides common benchmarks for payment card issuers, processors and merchants with regard to payment card data security. PCI-DSS is an international standard accepted in markets throughout North America, Latin America, Europe, the Middle East, and Asia. It covers areas such as data center security, protection of data during transmission, and standard operating procedures. While the standard is widely accepted by the credit card companies, there is still significant confusion in many companies that handle credit card payments about what PCI compliance means and exactly how it applies to them.

The purpose of this guide is to explain PCI-DSS and its impact on contact centers. This document clarifies the circumstances when organizations are required to adhere to these guidelines, and provides the accepted approaches used by contact centers to be in compliance.

What is PCI-DSS?

The Payment Card Industry Data Security Standard was developed through the combined efforts of five of the largest payment card brands: American Express, Visa, MasterCard, Discover and JCB International. It was established to provide guidance to merchants and payment card processors about securing personal customer data located on cards and on the cards' magnetic strip. PCI-DSS version 1.1 was released in 2006 and has since been enhanced a number of times. The Payment Card Security Council released the current standard, Version 2, in October 2010.

PCI-DSS is comprised of 12 broad requirements that set a baseline against which to measure and grade a vendor's data security practices, and provides mechanisms for members of the Payment Card Industry to self-regulate and self-police. The PCI-DSS does not dictate how a company must provide security.

The following requirements make up the current PCI-DSS:

Build and Maintain a Secure Network

- *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
- *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- *Requirement 3:* Protect stored cardholder data
- *Requirement 4:* Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- *Requirement 5:* Use and regularly update anti-virus software
- *Requirement 6:* Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- *Requirement 7:* Restrict access to cardholder data by business need-to-know
- *Requirement 8:* Assign a unique ID to each person with computer access
- *Requirement 9:* Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- *Requirement 10:* Track and monitor all access to network resources and cardholder data
- *Requirement 11:* Regularly test security systems and processes

Maintain an Information Security Policy

- *Requirement 12:* Maintain a policy that addresses information security

Each requirement above has more specific sub-requirements. Detailed information about the standards is available at www.pcisecuritystandards.org.

Below are a few common questions about PCI-DSS:

Who must comply?

Any business that accepts (merchant) or processes (processor) payment cards issued through the brands Visa, MasterCard, American Express, Discover and JCB International needs to be PCI compliant.

What information do the standards cover?

PCI-DSS covers the security of payment card information (such as account number, personal identification number (PIN), and Card Validation Value (CVV) or code) through the entire transaction network. The standard requires merchants and payment card processors to ensure that customer data are secured at the point of sale, while being transmitted throughout the company's network, and while being transmitted between merchants and processors. The data security standards also cover when and how payment card information is stored.

PCI-DSS specifically targets information stored on payment cards (embossed onto the card, printed on the card, or recorded on the magnetic stripe). The data may include, but is not limited to:

- Owner's name
- Account number
- Card Validation Value (or code)
- Personal Verification Value (PVV) or Personal Identification Number (PIN)
- Expiration date

PCI-DSS is not concerned with other non-public information such as social security number, driver's license number, card owner's address, etc., unless the information is stored on the payment card's magnetic strip.

Who maintains and modifies the requirements?

To develop and regulate the PCI-DSS, American Express, Visa, MasterCard, Discover and JCB International organized the PCI Security Standards Council. (These five card processing companies are referred to as "the brands" throughout this paper.) To avoid antitrust concerns, the Council has no enforcement powers; this remains the responsibility of the individual brands. The Council provides the umbrella structure, sets

policies, establishes common auditing and scanning procedures, and certifies assessors and scanners. It is up to each of the five card brands to interpret and enforce the standards.

The PCI Security Council uses a five-step, 24-month lifecycle process to maintain and update the security standard. The five steps include:

- Marketing implementation
- Gathering feedback from members
- Reviewing the feedback and revising the standards accordingly
- Releasing a final draft for final review
- Eliciting feedback from members and releasing a final revision

Who is responsible for enforcing compliance?

It is up to each of the five brands to interpret and enforce the standards. Each brand has implemented programs and established different levels of compliance. Part of what causes confusion in the market is that each brand has slightly different definitions and guidelines. The brands categorize merchants and processors based on the number of transactions they process each year, referred to as "levels." Figure 1 below presents the levels for the five card brands.

Figure 1: Card Company Annual Transaction Levels

Company	Level 1	Level 2	Level 3	Level 4
Visa [2]	6 million+	Between 1 and 6 million	Between 20,000 and 1 million	Less than 20,000
MasterCard [3]	6 million+	Between 1 and 6 million	Between 20,000 and 1 million	Less than 20,000
American Express [4]	2.5 million+	Between 50,000 and 2.5 million	Less than 50,000	N/A
Discover [5]	6 million+	Between 1 and 6 million	Between 20,000 and 1 million	Less than 20,000
JCB International [6]	More than 1 million	Less than 1 million	N/A	N/A

To assist companies in assessing their data security so that they can find potential data breaches, the Council certifies two "classes" of companies or individuals. A Qualified Standards Assessor (QSA) is a company or individual whose task it is to measure a

merchant or card processor's data security policies, procedures and technology against the requirements documented in the PCI-DSS regulations. They are also responsible for reporting to the Council and the appropriate brand how well the merchant or card processor complies with PCI-DSS standards.

An Approved Scanning Vendor (ASV) is a company or individual who is responsible for electronically scanning a corporation's network, including their interfaces to all associated merchants and card processors, to identify potential security breaches. ASVs then report the outcomes to the Council, company and brand.

The brands have different scanning and assessment requirements for each level. Figure 2 lists the assessment and scanning requirement for each level as defined by the brands.

Figure 2: PCI-DSS Scanning and Assessment Requirement Guidelines

Company	Level 1	Level 2	Level 3	Level 4
Visa [7]	Annually: Assessment by a Qualified Standards Assessor Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-assessment using the PCI Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-assessment using the PCI Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-assessment using the PCI Self-Assessment Questionnaire (Recommended) Quarterly: Network scans by an Approved Scanning Vendor (Recommended)
MasterCard [8]	Annually: Assessment by a Qualified Standards Assessor Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-Assessment Questionnaire (Recommended) Quarterly: Network scans by an Approved Scanning Vendor (Recommended)
American Express [9]	Annually: Assessment by a Qualified Standards Assessor	Quarterly: Network scans by an Approved Scanning Vendor	Quarterly: Network scans by an Approved Scanning Vendor	N/A

Figure 2: PCI-DSS Scanning and Assessment Requirement Guidelines

Company	Level 1	Level 2	Level 3	Level 4
	Quarterly: Network scans by an Approved Scanning Vendor		(Recommended)	
Discover [10]	Annually: Assessment by a Qualified Standards Assessor Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-assessment using the PCI Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-assessment using the PCI Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	Annually: Self-assessment using the PCI Self-Assessment Questionnaire (Recommended) Quarterly: Network scans by an Approved Scanning Vendor (Recommended)
JCB International [11]	Annually: Assessment by a Qualified Standards Assessor Quarterly: Network scans by an Approved Scanning Vendor	Annual: Self-assessment using the PCI Self-Assessment Questionnaire Quarterly: Network scans by an Approved Scanning Vendor	N/A	N/A

Level 1 processors and merchants must be audited by third-party QSAs annually, and must have their corporate networks scanned quarterly by third-party ASVs. Level 2 and 3 vendors must have their corporate network scanned by ASVs every quarter, but can self-certify their security processes annually. Level 4 vendors can self-certify and self-scan. While it is not required for Level 4 merchants to self-certify and self-scan, the brands strongly recommended that they do so. Furthermore, Discover, Visa and MasterCard data security procedures also allow Level 3 card processors to require their Level 4 merchants to prove the same level of PCI-DSS compliance as Level 3 merchants.

Each brand has a separate enforcement organization that evaluates the scans and assessments for the Council and determines if a merchant or card processor is PCI

compliant. Each brand sets the time frame for scans and assessments. They write the individual policies and procedures into the contractual agreements between processors and merchants and the branding company. Brands can fine their members and require additional security actions if a merchant is found to be in violation of the standards. Information on the brands' policies and procedures can be found through the organizations listed below:

- Visa (US) Card Information Security Program (www.visa.com/cisp)
- Visa (Canada) Account Information Security Program (www.visa.ca/en/merchant/fraud-prevention/account-information-security/index.jsp)
- Visa (Europe) Account Information Security Program (www.visaeurope.com/aboutvisa/security/ais)
- Visa (Asia) Account Information Security Program (www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml)
- MasterCard Site Data Protection program (www.mastercard.com/us/SDP)
- American Express Data Security Operating Policy (www.americanexpress.com/datasecurity)
- JCB International Data Security Program (www.jcb-global.com/english/jdsp)
- Discover (http://www.discovernetwork.com/fraudsecurity/disc.html)

Violation Notification Requirements

If a merchant or payment card processor is found to be in violation or discovers a security breach, they must alert the brand immediately. Each brand has a different process to report and repair a security breach. While these plans are unique to each brand, they are similar in terms of:

- Limiting the exposure
- Conducting a thorough investigation of the cause and determining the extent of the compromise
- Providing a complete accounting to the brand's security program of what was affected

Is PCI-DSS a Law?

The Payment Card Industry Data Security Standard is not mandated by any national government. However, data protection requirements spelled out in laws such as the Gramm-Leach-Bliley Act (US) [12], the Data Protection Act of 1998 (UK), EU Directive 95/46/EC, and the Personal Information Protection Law (Japan) require companies to guarantee the security of all non-public and personal customer information that they accept, transmit and store. Only one US state, Nevada [13], has enacted PCI-DSS into law in its entirety. Other states, like Minnesota [14], have written parts of the standards into law. While not mentioning PCI-DSS specifically, most states have passed laws mandating protection of customers' personal data by merchants and payment card processors. (For example, see Massachusetts's Standards for the Protection of Personal Information of the Residents of the Commonwealth [15].) Finally, almost all states require state agencies that accept payment cards to be PCI compliant.

The Implications of PCI-DSS for Contact Centers

In March 2011, the Payment Card Security Council published a document called "Protecting Telephone-based Payment Card Data." This document, which is called an information supplement, was intended to address concerns and questions related to how PCI-DSS affects contact center operations and, specifically, how recordings need to be handled. Unfortunately, the document is similar to other ones put out by this organization in that it is both broad and vague. It attempts to provide some general guidelines for handling secure customer credit and debit card information (credit and payment card numbers and the CVV) in call and screen recordings.

Contact Center Responsibilities:

All businesses that accept or process payment cards issued through the brands Visa, MasterCard, American Express, Discover and JCB International have to be PCI compliant.

The PCI-DSS guidelines are intended to be implemented by merchants and other retail businesses to ensure that payment card data is secure while stored and transmitted between the point of sale and the brands. Businesses and the brands are responsible for ensuring that all data transmission systems, network segments and data storage solutions comply with the Data Security Standard; this includes any wired, wireless, private and public networks. Security starts at the point where payment card information is received by the business, whether from a Web-based ordering system, swiped into a

point-of-sale device, or given to a contact center agent over the telephone; it ends with the brands.

Contact center applications cannot be PCI compliant, but they can help their users adhere to the requirements. (Only solutions that accept and process payment cards – card readers and online payment card validation solutions – can be PCI compliant). Call and screen recording solutions, customer relationship management (CRM) applications, billing systems, and Voice over Internet Protocol (VoIP) phone systems, etc., cannot be PCI-DSS compliant.

PCI-DSS does not require contact centers to use PA-DSS-certified solutions. That said, contact centers that process large volumes of payment card transactions need to be PCI-DSS compliant. They should work closely with their recording, quality assurance and CRM application providers to ensure they meet appropriate security protocols and operate within a secure network so that they comply with PCI-DSS requirements. More importantly, contact centers and IT departments must use the solutions correctly, employing all security features.

Vendor Methods of Adhering to PCI-DSS

PCI-DSS has taken on a life of its own. Many contact centers have adopted PCI-DSS as their security standard, though this was never intended to be its purpose. The purpose of PCI-DSS was to minimize (as it can never be eliminated) the risk of private payment card information getting into the wrong hands. To achieve this goal, organizations must limit access to recordings that contain private payment card data – specifically, the card number and the CVV. Organizations have gone to the next level to try to prevent this information from being recorded. (If it's not recorded it cannot be heard during a playback.) And now, organizations are trying to prevent their agents from hearing this information at all.

PCI-DSS states that unless it is necessary for legal or regulatory reasons or to meet the operational needs of the business, payment card information should not be saved and stored. Moreover, the CVV must never be captured and stored. The industry challenge is how to best adhere to these guidelines. Contact centers need technology to assist them in meeting these requirements.

Companies depend upon their vendor to deliver functionality that addresses these needs. Many approaches have been introduced to help companies meet PCI-DSS requirements. These include the following:

1. Recordings are encrypted from point of capture, and codes are used to decrypt to conversation.
2. A manual pause/resume capability is provided for agents – in other words, when a customer shares information that is considered sensitive, the agent manually hits a button (hardware or software-based) that pauses the recording. The agent then hits it again to resume recording.
3. Fully automated recording pause/resume functionality is being delivered in two ways today:
   a. An API is used to integrate the recording solution to the servicing (CRM) application. When an agent accesses the area of the servicing application that is considered sensitive, the recording is automatically paused. When the agent leaves the sensitive area, the recording automatically resumes. IT resources from either the vendor, enterprise or both are required to implement this solution.
   b. Desktop analytics is used instead of an API. It works in exactly the same way, except that these applications do not require changes at the code level, so they may not require IT resources to build the integration.
4. Speech analytics is used to identify sensitive information in captured recordings. The sensitive data is then deleted and the recording is stored without it.
5. Speech analytics is used to identify sensitive information in real time, and pauses the recording when necessary.
6. An IVR is used to capture all credit card information. (The agent would transfer the customer into the IVR.)
7. Detailed audit trail reports show all access to recordings.

Since companies that process payment cards need to adhere to multiple security requirements, they need to find vendors that can meet their needs based on their interpretation of the standards. The PCI-DSS functionality available from recording vendors has matured significantly during the past 12 months, but the offerings vary greatly. There are also some stand-alone vendors that are delivering functionality to help them adhere to PCI-DSS.

What Are The Most Applicable Standards for Contact Centers?

While all 12 requirements may have some relevancy to contact centers and their systems, the most significant requirements are:

- *Requirement 3:* Protect stored cardholder data
- *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- *Requirement 12:* Maintain a policy that addresses information security

In addition, there are some sub-requirements that also apply to contact centers. These include:

Requirement 3 obliges businesses that store payment card data to ensure that their storage solution is highly secure. Companies need to:

- Store payment card data only when absolutely necessary, and have a disposal procedure in place
- Display only as much of the card number as necessary, such as the last four digits of the number for verification purposes
- Ensure that customer information is stored as encrypted data using strong cryptography protocols
- Allow access to the personal identification number and the CVV within the record only on a need-to-know basis, and prevent users from being able to search for the code by encrypting it

Requirement 4 targets the transmission of payment card data across networks. It requires companies to:

- Use strong encryption protocols such as Secure Socket Layer and Transport Layer Security (SSL/TLS) or Internet Protocol Security (IPSEC) to provide secure transmission of data over the network
- Never send payment card information over an unencrypted medium such as chat, SMS/text or email

Requirement 12 targets how PCI-DSS is communicated and monitored. It requires companies to:

- Establish, publish, maintain and disseminate a security policy that:
  - Addresses all PCI-DSS requirements
  - Includes an annual process that identifies threats and vulnerabilities and results in a formal risk assessment
  - Includes annual reviews and updates when the environment changes

- Develop daily operational security procedures that are consistent with PCI-DSS requirements
- Develop usage policies for critical employee-facing technology to define proper use of these technologies for all employees and contractors
- Ensure that the information security policies and procedures clearly define the responsibilities of all employees and contractors
- Assign specific security responsibilities to an individual or team
- Implement a formal security awareness program so that all employees are conscious of the importance of payment card security
- Screen potential employees prior to hiring to minimize the risk of attacks from internal sources

How Should Contact Centers Protect Cardholder Information?

Contact center executives and leaders need to find the right balance between complying with all state and federal recording requirements, the PCI-DSS, and their own internal quality assurance guidelines. DMG suggests that managers do the following:

- Include all security policies in their organization's standard operating procedures (Requirement 12.1)
- Make sure that all employees and contractors are properly trained and knowledgeable about all security policies and procedures (Requirement 12.6)
- Require agents and supervisors to use only company-supplied systems (Requirement 9.1)
- Ensure that agents and supervisors do not share user IDs and passwords (Requirement 8.1)
- Segment contact center operations so that a limited number of agents 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 last four digits of the card number (Requirement 3.1)
- Ensure that stored recordings are not played back over a speaker phone if payment card information is included (Requirement 4.2)
- Prevent payment card information from being transferred using chat, email, SMS, or other non-encrypted communication channels (Requirement 4.2)

The following data security safeguards may require collaboration between corporate IT departments and quality assurance (QA)/recording and CRM vendors. DMG suggests that managers do the following:

- Maintain all database servers on which payment card information is stored in secure data centers with restricted physical access (Requirement 9.1)
- Ensure the data within the QA/recording and CRM solutions are encrypted using strong encryption protocols (Requirement 3.4)
- Ensure that the card validation code (referred to as CAV2, CVC2, CVV2, or CID) is not recorded or stored
- Restrict access to QA/recording and CRM data containing payment card data based on the user's log-in account and corporate role; for example, provide screen recording playback interfaces where the payment card information is displayed only to managers and compliance officers during legal discovery, and have it blacked out (masked) for all other supervisors and QA specialists (Requirement 8.5)
- Prevent all screen and voice recordings that include payment card data from being sent to individuals without first being encrypted (Requirement 4.2 and Requirement 9.7)
- Limit the amount of time that card information is kept on the QA/recording server and CRM solution databases (both voice and screen recordings); it may be necessary for corporate legal and QA departments to work out a compromise regarding what is needed to adhere to the PCI-DSS and regulatory compliance requirements (Requirement 3.1)
- Make sure that the QA/recording solution provides a process that agents can use to prevent card information from being recorded, as needed (such as when verifying account information) (Requirement 3.1)
- Develop agent desktop applications that can mask card information once it has been entered and verified (Requirement 7.1)
- Ensure that the network segment that carries screen and voice recording is encrypted (Requirement 4.1)
- Make sure that the VoIP voice stream is encrypted within the corporate network using strong encryption protocols (Requirement 4.1)

PCI and At-Home Agents and Supervisors

At-home agents and supervisors pose additional risks to PCI compliance because there is no definitive way to certify that at-home employees are working in a fully secure area and are not capturing and sharing payment card information. In addition, many remote agents and supervisors send and receive data over the unsecured Internet. Some even utilize unencrypted VoIP telephone systems for their home-office phones. When dealing with at-home agents, contact center managers should work with their IT departments to ensure that:

- Each agent and supervisor is using a virtual private network (VPN) with strong encryption protocols such as SSL/TLS (Requirements 4.1 and 4.2)
- Voice traffic is transmitted over a VPN into the corporate network (Requirement 4.2)
- At-home agents and supervisors use a two-factor authentication process (Requirement 8.3)
- Agent and supervisor PCs have personal firewalls installed and operational (Requirement 1.4) and have the latest version of the corporate virus protection software and definition files (Requirement 6.1)
- When using at-home or remote agents, ensure that agents' screens and voice conversations can be recorded remotely (Requirement 12.2)

In addition to the technical issues listed above, contact center managers need to develop a list of security-oriented best practices for at-home agents and supervisors. At-home agent best practices may include:

- Ensure that at-home agents and supervisors encrypt their wireless networks using strong encryption protocol; please note that Wireless Equivalency Protection (WEP) protocol is no longer permissible for any new wireless implementations and will not be allowed for any wireless implementation after June 30, 2010 (Requirement 4.1)
- Require agents to enter payment card information as it is given to them, and then mask the information once they verify its accuracy (Requirement 3.3)
- 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)

- If not using an enterprise VoIP-based telephone solution, require agents to use analog telephone lines when talking with customers; at-home agents should not use consumer VoIP telephone systems (such as Vonage) because they may not be encrypted (Requirement 4.2)

Final Thoughts

Any company accepting or processing American Express, Visa, Discover, MasterCard or JCB International brand credit and debit cards must be PCI-DSS compliant. It is the responsibility of merchants, payment card processors and other retail businesses that accept these cards to implement and maintain PCI-DSS compliance. Quality assurance/liability recording solutions, CRM applications and VoIP-based telephone systems cannot be PCI-DSS compliant, but can provide functionality to help a company comply with PCI-DSS regulations. Contact centers are one of the few points in the corporate infrastructure where payment cards are both viewed by humans (while being confirmed or entered) and stored. Contact center managers and executives need to work with their IT department and third-party application vendors to ensure that payment card information is secure from the time it is acquired, through database storage, until it is finally discarded.

While no one wants to think about data theft, it does happen, often resulting in significant financial cost and loss of consumer confidence in a company. The Payment Card Industry Data Security Standard offers companies a wide range of options to help keep their customers' credit and debit card information secure. At the front end of the process, contact centers play an important role in PCI-DSS. This document lets you know what you need to do and how to do it. If you have any questions, please contact deborah.navarra@dmgconsult.com or (516) 628-1098.

Endnotes

1. http://www.bos.frb.org/economic/cprc/presentations/2010/Schuh050610.pdf
2. http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp and http://www.visaeurope.com/aboutvisa/security/ais/main.jsp
3. http://www.mastercard.com/us/sdp/index.html
4. http://www.americanexpress.com/datasecurity/
5. http://www.discovernetwork.com/fraudsecurity/disc.html
6. http://www.jcb-global.com/english/jdsp/index.html
7. http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp and http://www.visaeurope.com/aboutvisa/security/ais/main.jsp
8. http://www.mastercard.com/us/sdp/index.html
9. http://www.americanexpress.com/datasecurity/
10. http://www.discovernetwork.com/fraudsecurity/disc.html
11. http://www.jcb-global.com/english/jdsp/index.html
12. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106
13. http://www.leg.state.nv.us/Statutes/75th2009/Stats200916.html#CHz355_zSBz227
14. https://www.revisor.mn.gov/bin/bldbill.php?bill=S1574.2.html&session=ls85
15. http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

About OAISYS

OAISYS® is a leading developer of call recording and contact center management solutions for a wide range of organizations, from small- to medium-sized businesses to multi-site large enterprises. OAISYS voice documentation and interaction management solutions help companies within a variety of industries—including healthcare, automotive dealerships, financial services, and the public sector—attract and retain customers by digitally capturing phone-based interactions for simple retrieval, playback and management. Compatible with leading business communications system providers, including Avaya, Mitel, ShoreTel and Toshiba, as well as SIP-based communications services, the OAISYS Tracer and Talkument® applications help companies improve risk management, quality assurance, customer retention, dispute resolution, regulatory compliance requirements and other critical business concerns. OAISYS is headquartered in Tempe, Ariz. OAISYS Ltd. is located in Cambridge, England.

More information about OAISYS can be found at www.oaisys.com.

About DMG Consulting

DMG Consulting is the leading provider of contact center and analytics research, market analysis and consulting services. DMG's mission is to help end users build world-class, differentiated contact centers and assist vendors in developing high-value solutions for the market. DMG devotes more than 10,000 hours annually to researching various segments of the contact center market, including vendors, solutions, technologies, best practices, and the benefits and ROI for end users. DMG is an independent firm that provides information and consulting services to contact center management, the financial and investment community, and vendors in the market.

More information about DMG Consulting can be found at www.dmgconsult.com.