Call Recording and PCI Compliance

CallCopy and the Payment Card Industry Data Security Standard

Whitepaper
March 2011

CallCopy®

Contents

1. Introduction 1
2. Payment Card Industry (PCI) 2
3. PCI's Impact on Call Recording 4
4. Data Storage Guidelines 11
5. Recommendations 13
About CallCopy 15
Next Steps 15

No part of this document may be transmitted or distributed, or copied, photocopied, scanned, reproduced, translated, microfilmed, or otherwise duplicated on any medium without written consent of CallCopy. If written consent is given, the same confidential, proprietary, and copyright notices must be affixed to any permitted copies as were affixed to the original. The information contained in this document does not constitute legal advice, and should not be considered a replacement for sound legal counsel. CallCopy shall be in no way liable for any use or misuse of the information presented herein.

1

Introduction

We could fill volumes with the reasons that the Payment Card Industry (PCI) Data Security Standard (DSS) is important. It has been well-documented that identity theft is pervasive in today's economy, and consumers need to be protected. For example, the Privacy Rights Clearinghouse's Chronology of Data Breaches reports that more than a half billion sensitive records were breached between 2005 and mid-2010, leaving many consumers vulnerable to identity theft.[1]

The High Cost of Not Securing Payment Card Data

Organizations put themselves in financial peril if they fail to secure payment card data, resulting in monetary penalties and loss of business due to negative publicity. Consider these high profile cases of data theft:

- Between July 2005 and January 2007, a breach of systems at TJX Companies (the parent company of retailers T.J. Maxx, Marshalls and HomeGoods) exposed data from roughly 46 million credit cards. Resulting lawsuits have cost the company $10.28 million.[2]
- In August 2009, the ringleader of the TJX theft, Albert Gonzalez, was indicted in the largest identity theft case to date, after stealing data for at least 130 million credit and debit cards from credit card processor Heartland Payment Systems, retailers 7-Eleven and Hannaford Brothers and two other companies.[3] Heartland has since reached a $105 million settlement with MasterCard, Visa and American Express as a result of the breach.[4]

Putting Customer Data at Risk

A survey of 677 US and European-based organizations revealed their current data retention practices[1]:

- 81% store credit card number
- 73% store credit card expiration date
- 71% store credit card verification code
- 57% store customer data on the credit card magnetic strip
- 16% store other personal data

[1] Source: Forrester Research, The State of PCI Compliance, September 2007

Protecting Cardholder Data

The PCI DSS has become the gold standard for helping to alleviate vulnerabilities and protect cardholder data. In this whitepaper we will discuss PCI, how it affects recording applications and what you can do to help ensure your recording system operates in compliance with the PCI DSS.

While we have researched this topic extensively, we are not affiliated with the PCI Security Standards Council (SSC). The information presented in this whitepaper does not replace PCI SSC Security Standards or their supporting documents. Full details can be found on their website (www.pcisecuritystandards.org).

[1] http://www.privacyrights.org/500-million-records-breached
[2] http://www.databreaches.net/?p=5657 and http://www.databreaches.net/?p=7008
[3] http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/
[4] http://www.theregister.co.uk/2010/05/20/heartland_mastercard_settlement/

2

Payment Card Industry (PCI)

What is PCI?

The PCI Security Standards Council was founded by American Express, Discover Financial Services, JBC, MasterCard Worldwide and Visa International. The Council's stated mission is "to enhance payment account data security by driving education and awareness of the PCI Security Standards."[5]

> "PCI DSS represents the best available framework to guide better protection of cardholder data. It also presents an opportunity to leverage cardholder data security achieved through PCI DSS compliance for better protection of other sensitive business data – and to address compliance with other standards and regulations."
>
> **Aberdeen Group**
> IT Industry Analyst

Who Enforces PCI?

While the PCI Security Standards Council established and maintains the Data Security Standard (DSS), each card brand still manages its own compliance programs. If you have questions or concerns regarding your company's compliance status or the risks and penalties for falling out of compliance, we recommend you contact the payment brands you are contracted with.

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc.: www.visa.com/cisp
- Visa Europe: http://www.visaeurope.com/ais

Merchants and payment card service providers may be required to validate their compliance periodically. The PCI SSC approves several entities to assist in the validation of compliance with the PCI DSS. Qualified Security Assessors (QSA) assess compliance with the PCI DSS and Approved Scanning Vendors (ASV) validate adherence to the PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers. In addition, eligible organizations that are not required to submit a Report on Compliance (ROC) can instead complete a Self-Assessment Questionnaire (SAQ) as a validation tool.

States Adopting PCI Standards as Law

Several states have begun adopting PCI standards, either in part or whole, as part of their state laws. Many legal experts believe that other states will follow suit, and use these early adopters as

[5] www.pcisecuritystandards.org

models on which to base their own laws. States that have already introduced laws related to PCI compliance include:

- **Minnesota** In May 2007, Minnesota became the first state to pass a law that incorporates concepts from the PCI DSS. The state's Plastic Card Security Act (H.F. 1758) increases the liability for organizations that collect payment card data by prohibiting the retention of certain payment card data for more than 48 hours. In addition, it allows financial institutions to file lawsuits to recover costs associated with a payment card security breach.[6]
- **Nevada** Nevada was the first state to mandate full PCI compliance for businesses. Nevada Senate Bill 227, effective January 1, 2010, states "If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions...."
- **Washington** Similar to Minnesota's Plastic Card Security Act, Washington's law seeks to protect consumers from identity theft and fraud due to data breaches of credit card data by providing issuing banks a legal mechanism to collect the costs to reissue payment cards after a payment card security breach.[7]
- **Massachusetts** Massachusetts 201 CMR 17.00 (or Standards for the Protection of Personal Information of Residents in the Commonwealth) requires the protection of personal user information for state residents, including "financial account number, or credit or debit card number." This applies to any entity that stores or processes the personal information of Massachusetts residents.[8]

Learn More...

To learn more about the legal issues related to call recording, please download CallCopy's ***"This Call May Be Recorded..." Legal Issues Related to Call Recording*** whitepaper: www.callcopy.com/document-library/whitepapers/recording-laws

Who Does the PCI Data Security Standard Apply To?

The PCI DSS applies to all entities that store, process or transmit cardholder data. The deciding factor in determining the applicability of PCI DSS requirements is whether a primary account number (PAN) is stored, processed or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

If cardholder name, service code and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements except Requirements 3.3 and 3.4, which apply only to PAN.[9]

The PCI Data Security Standard

The PCI DSS is the global data security standard adopted by the payment card brands for any organization that processes, stores or transmits cardholder data. Table 1, "The PCI Data Security Standard," summarizes the goals and requirements of the PCI DSS.

[6] http://www.infolawgroup.com/2007/06/articles/privacy-law/minnesotas-plastic-card-security-act/
[7] http://www.infolawgroup.com/2010/03/articles/payment-card-breach-laws/faq-on-washington-states-pci-law/
[8] http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf
[9] PCI DSS v2.0

Goals	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

Table 1: The PCI Data Security Standard

3

PCI's Impact on Call Recording

What follows is an outline of the PCI DSS requirements that are most relevant to call recording systems, and best practices for maintaining compliance. The full PCI DSS version 2.0 is available at www.pcisecuritystandards.org.

In early 2010, as part of its regular review, the PCI DSS language was updated to eliminate inconsistencies and provide a higher level of clarity on the impact to call recording applications. Below is the language contained in the modification:

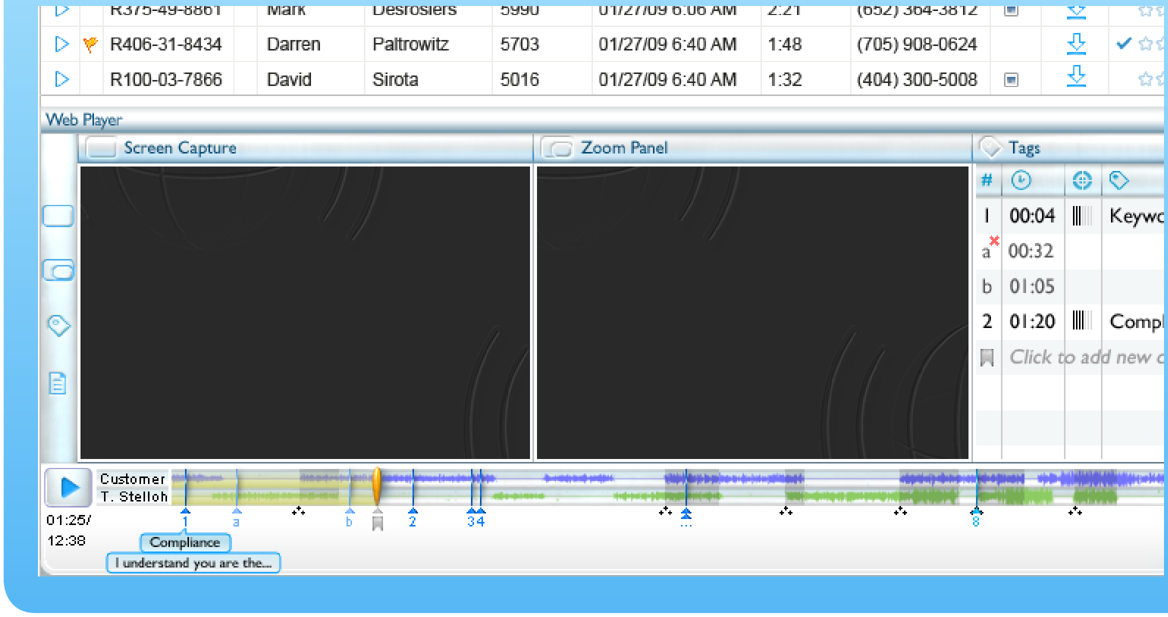
> *Question: Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of PCI DSS?*
>
> This response is intended to provide clarification for call centers that record cardholder data in audio recordings, and applies only to the storage of card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by the payment brands).
>
> It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted.
>
> It is therefore prohibited to use any form of digital audio recording (using formats such as .wav, .mp3, etc.) for storing CAV2, CVC2, CVV2 or CID codes after authorization if that data can be queried; recognizing that multiple tools exist that potentially could query a variety of digital recordings.
>
> Where technology exists to prevent recording of these data elements, such technology should be enabled.
>
> If these recordings cannot be data mined, storage of CAV2, CVC2, CVV2 or CID codes after authorization may be permissible as long as appropriate validation has been performed. This includes the physical and logical protections defined in PCI DSS that must still be applied to these call recording formats.
>
> This requirement does not supersede local or regional laws that may govern the retention of audio recordings.[10]

CallCopy's recommendation for addressing this requirement is to utilize automated blackout triggers based on activity in a desktop application or web form. In this scenario, a trigger to start a blackout would be sent when an agent clicks on the field to enter the security code, and it would end when the agent submits the account information. This method is still not infallible, as a customer may provide account information before the agent takes the action that starts the blackout. To address this, cc: Discover includes file-level disk encryption for audio and video files as an added layer of security. As a result, any sensitive information that is erroneously recorded cannot be decrypted without the required password/keyfile(s) or encryption keys.

[10] http://selfservice.talisma.com/display/2n/kb/article.aspx?aid=5362&n=1&s=

A Closer Look at Blackouts

Blackouts are a way to ensure that sensitive data is not stored in interactions. By detecting the point in time when sensitive data is being transmitted, the recording application should be able to pause both the audio and video recording, and resume recording after the transmission has been completed. This results in an interaction recording that includes a beginning and an end for QA and liability purposes, and a "blackout" portion in the middle. For PCI compliance purposes, the recording (both audio and video) is paused when the agent enters a field identified as containing sensitive data, and resumes when the credit card processing is completed.



R375-49-8861	Mark	Desrosiers	5990	01/27/09 6:06 AM	2:21	(652) 364-3812	
R406-31-8434	Darren	Paltrowitz	5703	01/27/09 6:40 AM	1:48	(705) 908-0624	✓
R100-03-7866	David	Sirota	5016	01/27/09 6:40 AM	1:32	(404) 300-5008	

#			
1	00:04	‖‖	Keywo
a	00:32		
b	01:05		
2	01:20	‖‖	Compl
	Click to add new c		

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

CallCopy SOLUTION

cc: Discover utilizes SSL encryption for all client-server communications, both in recording and playback mode. All data is encrypted prior to and during recording. This includes video being streamed from a workstation and any audio being transmitted from a remote server to the core file storage location.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings and elimination of unnecessary accounts.

CallCopy
SOLUTION

CallCopy has security settings which force password adherence to the PCI DSS. Passwords are required to include a length of at least seven characters and contain both numeric and alphabetic (both upper and lower case) characters. Additionally, users are required to change their password every 90 days and not re-use the four most recent passwords.

CallCopy
SOLUTION

Part of CallCopy's standard installation procedure is to reset/remove all default passwords.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

The best way to ensure that cardholder data is protected is to not store it in audio and screen recordings at all. However, being 100-percent certain that sensitive data is not stored is not always possible. Thus, it is imperative to take the steps necessary to encrypt all audio and video recordings and enforce policies and procedures to ensure their security.

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.

CallCopy
SOLUTION

cc: Discover supplies automatic record archiving and purging. Users can specify how long audio and video recordings are stored. When that time has expired, the system will securely erase the recordings. Users can be granted permission to override auto-archiving when needed, such as for legal proceedings and discovery or as part of a long-term root-cause analysis program.

3.2 Do not store sensitive authentication data after authorization (even if encrypted).

CallCopy
SOLUTION

CallCopy's blackout feature ensures that sensitive data is not stored. By utilizing start and stop triggers to define the beginning and end of a period within a call that contains sensitive information, the recording of both audio and video is effectively paused. Please refer to the *Blackouts: Avoid Recording Sensitive Authentication Data* section for additional information.

3.4 Render PAN 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

CallCopy
SOLUTION

cc: Discover includes on-the-fly file-level disk encryption for audio and video files, meaning that no stored data can be read (decrypted) without the required password/keyfile(s) or encryption keys.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Your call recording system should be on your network behind a firewall, and not on an open public network. If you offer access to the system by remote workers or third parties, such as a client accessing a system at an outsourcer facility, that access should be through a secured connection such as VPN, and not over the public Internet.

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

CallCopy SOLUTION

cc: Discover utilizes SSL encryption for all client-server communications, both in recording and playback mode.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Best Practices

If work-at-home agents are using wireless networks, ensure that they utilize strong encryption for authentication and transmission.

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

CallCopy SOLUTION

CallCopy's screen capture module records full-motion video of agents' desktop activity during all types of interactions, including chats, email and calls, and can be configured to extend recording beyond the end of the interaction. This tool can be utilized to verify that agents are performing in compliance with the PCI DSS.

CallCopy SOLUTION

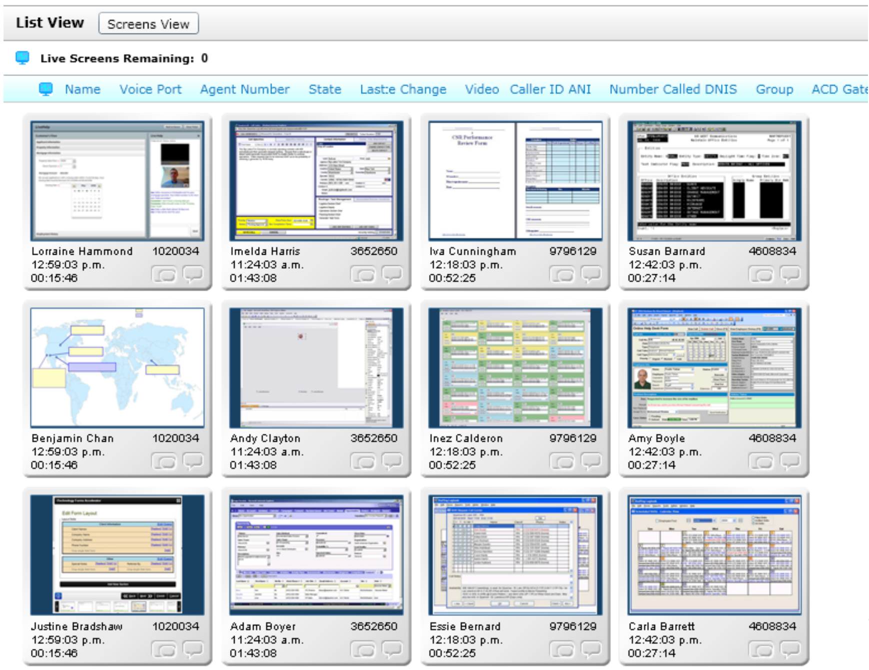
cc: Discover provides a real-time screen-monitoring interface, allowing supervisors to observe up to 12 agent screens at one time. Managers monitor agents in real-time, to ensure they are performing in compliance with the PCI DSS.

CallCopy SOLUTION

CallCopy's cc: Insight performance management platform provides an effective way for management to communicate with agents and send periodic reminders to reinforce organizational policies that align with the PCI DSS.

CallCopy SOLUTION

As previously discussed, blackouts are the best way to ensure that sensitive data is not stored in recordings; however, that is not always possible. cc: Discover provides file-level encryption, ensuring that any recordings that are exported and emailed do not contain any unprotected PANs.



Live Screens Remaining: 0

Lorraine Hammond 1020034
12:59:03 p.m.
00:15:46

Imelda Harris 3652650
11:24:03 a.m.
01:43:08

Iva Cunningham 9796129
12:18:03 p.m.
00:52:25

Susan Barnard 4608834
12:42:03 p.m.
00:27:14

Benjamin Chan 1020034
12:59:03 p.m.
00:15:46

Andy Clayton 3652650
11:24:03 a.m.
01:43:08

Inez Calderon 9796129
12:18:03 p.m.
00:52:25

Amy Boyle 4608834
12:42:03 p.m.
00:27:14

Justine Bradshaw 1020034
12:59:03 p.m.
00:15:46

Adam Boyer 3652650
11:24:03 a.m.
01:43:08

Essie Bernard 9796129
12:18:03 p.m.
00:52:25

Carla Barrett 4608834
12:42:03 p.m.
00:27:14

cc: Discover's real-time screen-monitoring interface

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

User permissions should be able to restrict what records each user can access, or deny any person from having access to the server. You can also use IP restrictions in your data network to further ensure the unauthorized employees cannot reach the server from their workstations.

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

CallCopy SOLUTION

CallCopy's robust security features include hierarchical role-based permissions. This provides the ability to set granular security controls, allowing only qualified users access to and export of audio and video recordings.

Requirement 8: Assign a unique ID to each person with computer access

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

CallCopy SOLUTION

CallCopy provides an unlimited number of user licenses for playback. This eliminates the need to share login IDs between users.

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components.

CallCopy SOLUTION

CallCopy's security and audit features ensure users can only access recordings that they are authorized to, based on role-based permissions. An extensive activity tracking system, supported by a database of all system activity, allows administrators to conduct full trace audits to determine who has accessed any recording in the system for playback, export or any other critical functions.

Requirement 9: Restrict physical access to cardholder data

The recording server should be in a locked computer room/data center at your facility to limit unauthorized physical access. For a hosted solution, check with your hosting provider to ensure access to the server is restricted. Having encryption for your stored files is also helpful in restricting physical access to the data.

9.7 Maintain strict control over the internal or external distribution of any kind of media.

CallCopy
SOLUTION

Role-based permissions allow internal access only to qualified individuals. File-level encryption ensures the protection of any recordings that are exported from the system. Encryption also ensures that if the server becomes physically compromised, the files are not retrievable from the hard disk.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Most PCI-compliant companies are likely to have something in place to monitor network activity. Your recorder should log user access and user activity within the system as it pertains to accessing recordings.

10.2 Implement automated audit trails for all system components.

CallCopy
SOLUTION

User security and audits provide an extensive activity tracking system, supported by a database of all system activity. Managers can conduct full trace audits to determine who has accessed any recording in the system for playback, export or any other critical functions.

Requirement 11: Regularly test security systems and processes

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

CallCopy
SOLUTION

As new features are added to cc: Discover and its various modules, part of CallCopy's software development process is to conduct regression testing to ensure new components do not have unwanted effects on existing modules.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

If your vendor has direct access to your recorder through modem, VPN or other means, you should ensure that vendor has a policy for information security.

12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.

CallCopy
SOLUTION

cc: Discover's agent coaching and training module (included with no additional licensing costs) allows training materials related to the importance of cardholder data security to be assigned out for reading. The completion of the reading assignment can be tracked within the system. Periodic reminders can be pushed out through cc: Insight to reinforce awareness.

4

Data Storage Guidelines

Guidelines for Cardholder Data Elements

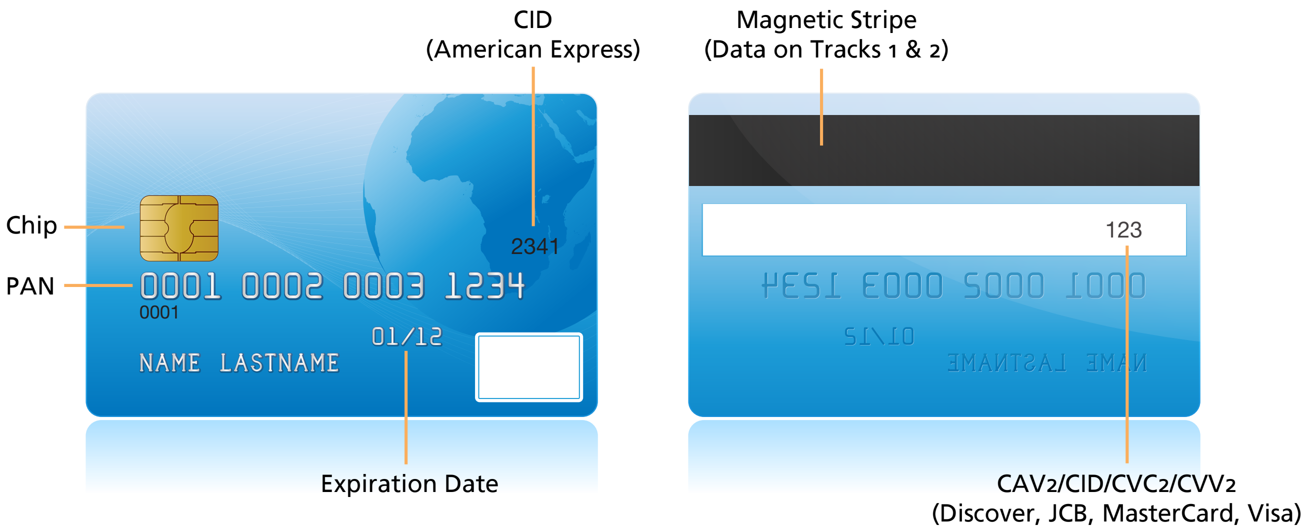
Table 2 outlines whether storage of individual data elements is permitted and whether it must be rendered unreadable.

Table 2: Storage Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot Store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot Store per Requirement 3.2
		PIN/PIN Block	No	Cannot Store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorization (even if encrypted).
[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Anatomy of a Payment Card



Card Validation Value or Code

Also known as Card Validation Code or Value, or Card Security Code, each payment card brand uses its own set of terms.

The first type of card validation value or code is magnetic stripe data. These are data elements that use a secure cryptographic process to protect data integrity on the stripe, and reveal any alteration or counterfeiting.

- **CAV:** Card Authentication Value (JCB)
- **CVC:** Card Validation Code (MasterCard)
- **CVV:** Card Verification Value (Visa and Discover)
- **CSC:** Card Security Code (American Express)

The second type of card validation value or code is printed security features. For Discover, JCB, MasterCard and Visa payment cards, this appears as the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the payment card face. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic.

- **CID:** Card Identification Number (American Express and Discover)
- **CAV2:** Card Authentication Value 2 (JCB)
- **CVC2:** Card Validation Code 2 (MasterCard)
- **CVV2:** Card Verification Value 2 (Visa)

5

Recommendations

The aspect of the PCI DSS that poses the greatest challenge to organizations that engage in interaction recording is the storage of sensitive cardholder data. For this reason, it is highly recommended that when implementing a recording solution, you chose one that offers automatic audio and video "blackouts" that will allow you to prevent the recording of such data, in accordance with the PCI DSS.

Blackouts: Avoid Recording Sensitive Authentication Data

CallCopy's cc: Discover workforce optimization solution includes the bcc: Security module, which allows users to prevent the recording of sensitive data through the use of a blackout feature. This feature allows start and stop triggers to define the beginning and end of a period within a call that contains sensitive data, effectively pausing the recording of both voice and screen. The blackout can be automatically triggered based on activity in a desktop application or web form. In this scenario, a trigger to start a blackout would be sent when an agent clicks on the field to enter the security code, and it would end when the agent submits the account information. CallCopy offers two methods for triggering blackouts based on third-party application integrations.

cc: Fusion

CallCopy's desktop analytics platform, cc: Fusion, facilitates the integration between cc: Discover and third-party applications by automatically detecting where fields exist in the interface. This allows triggers to be established based on agent activity (such as a mouse's movement to a payment card processing application), without the need for any custom application development.

API Integration

cc: Discover's product license includes access to our application programming interface (API) and software development kit (SDK). This allows you to integrate with any program that can communicate over TCP/IP. Messages are sent in a simple and descriptive XML format.

cc: Fusion vs. API Integration: Which is Right for You?

Both cc: Fusion and an API integration achieve the same end result. Your organizational infrastructure and available resources will determine which option is a better fit for you.

Use cc: Fusion if:

- You do not have development staff available to build the integration;
- You have legacy applications that are no longer supported by the vendor;
- You have multiple applications that you need to integrate with;
- You plan to change application vendors in the near future;
- You prefer a single point of contact for your integrations.

Build an API Integration if:

- You have available development resources that you can devote to building and managing the integration;
- You have a strong relationship with the provider of the application you are trying to integrate with, and can rely on them to support you during the development process.

Encryption

A recording system must provide encryption for your stored data as well as encryption for all client-server communications. This includes screen data being sent across your networks and audio/video playback.

Exported Records

Perhaps the most critical time to encrypt calls is when they are exported from the system. It is critical to secure your data, and this includes ensuring that calls are not allowed to be exported unless they are encrypted and password protected. cc: Discover includes the option of encrypting calls in the proprietary CallCopy Audio Video (.CAV) file format when they are exported. The .CAV format utilizes AES 256-bit encryption, and requires a password to play back the file in CallCopy's media player.

About CallCopy

CallCopy, a leading provider of innovative call recording and contact center solutions, is dedicated to ensuring the highest standards of customer and employee satisfaction. The award-winning, enterprise-proven cc: Discover suite delivers advanced call recording, screen capture, quality management, speech analytics, performance management, customer survey and workforce management capabilities to organizations of all sizes and industries across the globe.

CallCopy empowers these organizations to gather business intelligence, which is leveraged to maximize operational performance, reduce liability, achieve regulatory compliance and increase customer satisfaction.

For more information, visit www.callcopy.com.

Next Steps

CallCopy has taken great strides in delivering call and screen recording solutions that comply with the PCI DSS, which has lead to many of our customers passing PCI Compliance Audits. If you would like to learn more about how CallCopy's call recording and PCI compliance solutions can benefit your organization, please contact us:

- Toll-free: 888.922.5526 x1
- Direct/International: 614.340.3346
- email: info@callcopy.com