

safe and sound

processing telephone payments securely

a white paper from Barclaycard
leading the way in secure payments

April 2010

Executive summary

The following information and guidance is intended to provide key payment security advice to new or existing merchants who trade over the telephone. This information highlights the key areas organisations with call centre operations need to address in order to process card payments securely, and how best to protect their business and their customers from the risks of fraud.

Barclaycard are developing a range of further guidance that will provide greater detail on this and other related issues, that will be made available during the course of 2010.

Audience

This information and guidance is aimed at Company Owners, Financial Directors, IT Directors and Call Centre Managers of businesses processing card payments over the telephone.

Purpose

To help make sure merchants are not exposing themselves and their customers to the risks of fraudulent activity when processing card payments over the telephone.

Why telephone card payment security is important

In face-to-face environments, Chip & PIN has been the main fraud reduction driver, whilst risk mitigating technologies such as Verified by Visa and MasterCard Secure Code have significantly helped in the e-commerce sector. Both face-to-face and e-commerce fraud rates have benefited from these initiatives but there remain a limited amount of solutions that can fight fraud in the Mail Order/ Telephone Order (MOTO) space, resulting in a shift of card fraud towards MOTO.

The Financial Services Authority has introduced UK legislation requiring some companies to record and store telephone conversations in a range of situations.

The Payment Card Industry Data Security Standard, however, stipulates that the CVV2 (Credit Card Validation Value, or three-digit security code) cannot be kept post-authorisation, and full Personal Account Numbers (PAN) cannot be kept without further protection measures.

As such there is a risk that organisations who take customer credit card details over the telephone may be recording the full cardholder details, and therefore be in contravention of the mandatory requirements of the Payment Card Industry Data Security Standard (PCI DSS).

Clarification of the PCI DSS Guidelines for Voice Recordings

The impact of PCI DSS has been far reaching and its goal to eradicate payment card data loss (malicious or otherwise) from the merchant environment is becoming a reality.

For all merchants, this requires appropriate measures to protect their cardholder environment and for those who process payments via their call centres, compliance within their voice network is required as well. This impacts on call recording management and storage and control of the agent/caller interface within the physical call centre space. Barclaycard produced this fact sheet in order to clarify the PCI DSS guidelines on voice recordings and to promote consistency in the merchants and QSA (Qualified Security Assessor) population.

Recap: the PCI DSS FAQ

[Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of PCI DSS? *FAQ 5362*](#)

This response is intended to provide clarification for call centres 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.

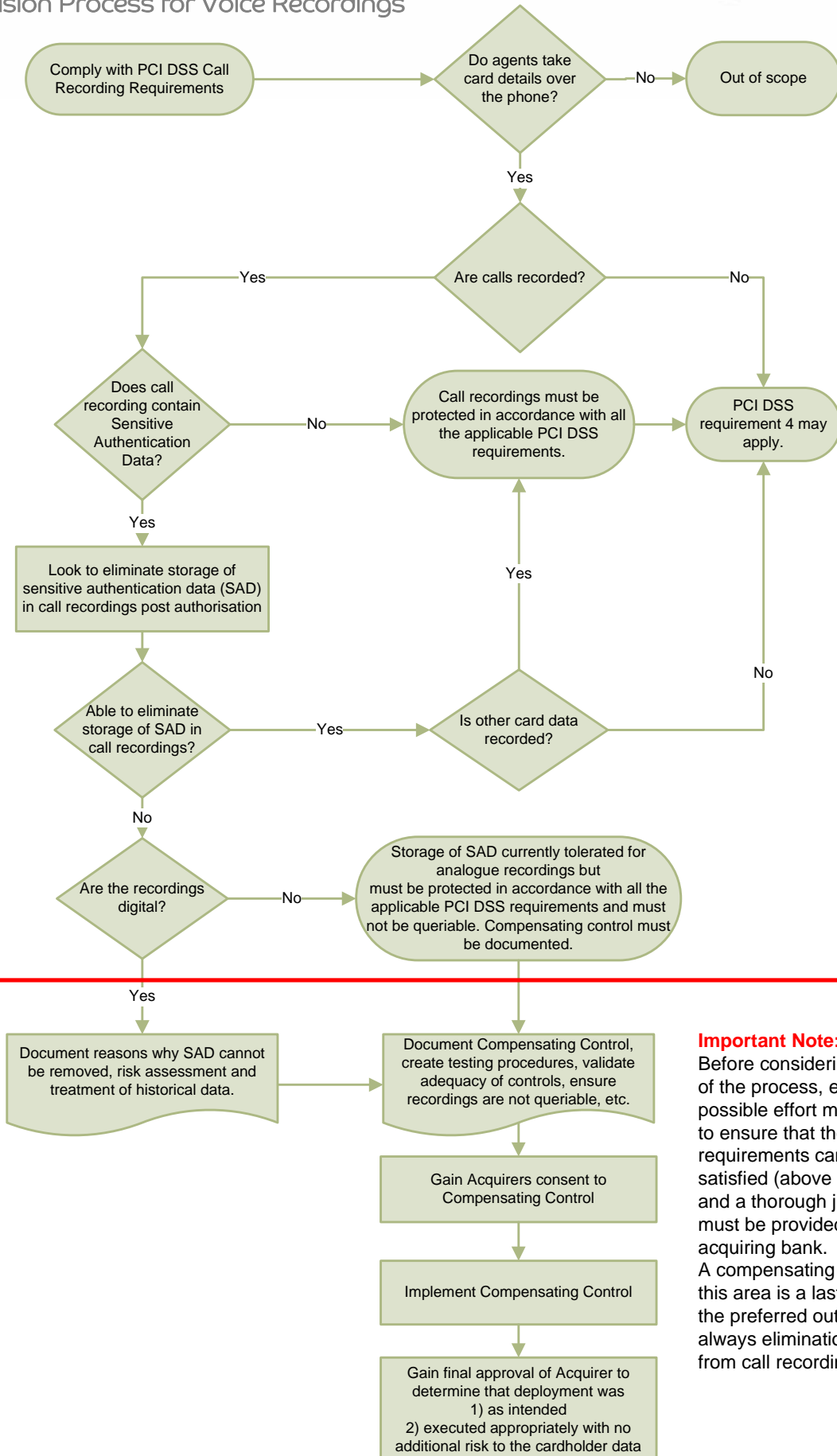
This requirement does not supersede local or regional laws that may govern the retention of audio recordings. (END)

What this means: essentially, the Card Verification Value (CVV) must not be retained post authorisation. In any event, and as a last resort, where a CVV is retained it must be held subject to additional security controls to meet the intent of the Standard, but always via a compensating control.

Where to start

The following page shows the process a merchant should follow when assessing the risk for their call centre operations and aims to further clarify the FAQ above.

Decision Process for Voice Recordings



Note: if payments via another channel are accepted in the same environment, scope should be reviewed.

Note: the call recording FAQ addresses data at rest, for completeness, we remind merchants of the need to secure data over public networks (Req. 4).

Important Note: Before considering this part of the process, every possible effort must be made to ensure that the requirements cannot be satisfied (above the red line) and a thorough justification must be provided to the acquiring bank. A compensating control in this area is a last resort and the preferred outcome is always elimination of SAD from call recordings.

Hints & tips for call centre managers (1)

Call centre managers will need to ensure that an **appropriate retention policy** is implemented and maintained.

This is part of requirement 3.1 and 3.2 and may include:

- Ensuring that payment card data is only stored when absolutely necessary, and that a disposal procedure is in place.
- Limiting 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 governance, legal and QA departments to work out a compromise between what is needed to adhere to the PCI-DSS and regulatory compliance requirements.
- Never allowing for the card validation code (referred to as CAV2, CVC2, CVV2, or CID) to be stored in a digital audio or video format (e.g. wav, mp3, mpg, etc.). If the QA/recording solution cannot block the audio or video from being stored, the code must be deleted from the call recording after it is stored.

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:

- Only allowing access to the full PAN on a need-to-know basis.
- Segmenting contact centre 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 masked PAN.
- Considering solutions where the agent does not have to enter card information into the system.
- If the above is not possible, requiring agents to enter payment card information as it is given to them and then mask the information once they verify its accuracy. This may mean sourcing agent desktop applications that can mask card information once it has been entered and verified.

Hints & tips for call centre managers (2)

Call centre managers will need to ensure that transmission of cardholder data across public networks is encrypted.

This is part of requirement 4 and may include:

- Using 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 public network. This includes ensuring that each at home agent and supervisor is using a VPN with strong encryption protocols such as SSL/TLS.
 - Ensuring that voice traffic is transmitted over a VPN into the corporate network (Requirement 4.2)
 - Ensuring that the public network segment that carries screen and voice recording is encrypted (Requirement 4.1)
 - Ensuring that at-home/ remote agents and supervisors encrypt their wireless networks using strong cryptography¹ (Requirement 2.1.1 and 4.1.1). Please note that Wired Equivalent Privacy (WEP) protocol is no longer permissible for any new wireless implementations and will not be allowed for any new wireless implementation after 30th June 2010 (Requirement 4.1) and Barclaycard recommends the use of WPA2.
 - Making sure that the VoIP voice stream is encrypted whenever sent over an open or public network using strong encryption protocols.
 - If not using an enterprise VoIP-based telephone solution, requiring agents to use analogue 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)
- Ensuring 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 stored recordings are not played back over a speaker phone if payment card information is included
- Preventing 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)

¹ Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). SHA-1 is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher).

See NIST Special Publication 800-57 (<http://csrc.nist.gov/publications/>) for more information.

Hints & tips for call centre managers (3)

Call centre managers will need to ensure that cardholder information (and at a minimum, the PAN) is encrypted using strong cryptography when stored.

This is part of requirement 3.4 and may include:

- Ensuring the data within the QA/recording and CRM solutions are encrypted using strong cryptography.
- Never allowing for the card validation code (referred to as CAV2, CVC2, CVV2, or CID) to be stored in a digital audio or video format (e.g. wav, mp3, mpg, etc.). If the QA/recording solution cannot block the audio or video from being stored, the code must be deleted from the recording after it is stored. If a call centre manager feels that there may be difficulty with achieving this, they must discuss this with their acquiring bank. The overriding preference is for the elimination of SAD from recorded audio and video, and compensating controls will only be considered in extreme circumstances.

Call centre managers will need to ensure that proper user authentication is implemented for staff, agents and administrators.

This is mainly part of requirement 8.1 to 8.5 and may include:

- Restricting 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 play-back 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).
- Segmenting contact centre 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 masked PAN.
- Ensuring at-home/ remote agents and supervisors use a two-factor authentication process.
- Ensuring that agents and supervisors do not share user IDs and passwords.
- Ensuring that at-home/remote agents are prohibited from copying, moving, and storing cardholder data onto local hard drives and removable electronic media when accessing cardholder data via remote-access technologies (Requirement 12.3.10).

Hints & tips for call centre managers (4)

Call Centre managers will need to ensure that they adhere to an **Information Security Policy**. Whilst the development of the policy itself may not be their responsibility, they should ensure that requirement 12 is met for their operation.

This may include:

- Developing daily operational security procedures that are consistent with PCI-DSS requirements and clearly defining the responsibilities of all employees and contractors.
- Develop usage policies for critical employee-facing technology to define proper use of these technologies for all employees and contractors.
- Assigning an individual or team specific security responsibilities.
- Implementing a formal security awareness program so that all employees are conscious of the importance of payment card security and make sure that all employees and contractors are properly trained and knowledgeable about all security policies and procedures.
- Annually reviewing 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
- Barclaycard recommends monitoring of at-home/ remote agents more often than in-house agents, in addition to screening of potential employees prior to hiring to minimise the risk of attacks from internal sources (as covered by requirement 12.7). In any instance, call centre managers should ensure that controls are implemented to monitor policy compliance for on-site, remote and at-home users.

Finally, call centre managers should also consider the following:

- Ensuring that at-home agent and supervisor PCs have personal firewalls installed and operational (Requirement 1.4)
- Ensure that at-home agents and supervisor PCs have the latest version of the corporate virus protection software and definition files (Requirement 5.1)
- Ensure that at-home agent and supervisor PCs have the latest approved security patches installed (Requirement 6.1).
- Requiring agents and supervisors to use only company-supplied systems (Requirement 12.3)

What to ask your call centre provider

How does the call centre system help you comply with the PCI DSS guidelines and how does it automatically remove sensitive credit card information from recorded calls?

If you take credit card details over the phone, ask your supplier to prove that they are "PCI DSS compliant" and to explain how they remove the 3-digit credit card verification value from their recordings, automatically (with no manual intervention by your staff). Apart from not recording calls at all, any other suggested solution to PCI DSS (such as encryption for sensitive authentication data), will not be compliant.

How will the call centre system comply with any future changes in legal regulations or codes of practice?

It is important that any call recording system purchased now can cope with future changes in the law, regulations and industry best practice. Organisations need to ensure that their recording system is as future proof as it can be. Suppliers must be able to prove that regardless of any constraints or changes the government, Financial Services Authority or any other body may impose on call recording, their system is flexible enough to adapt almost instantly.

If your call centre system is not compliant with the standard, what liability is your supplier prepared to take in the event of a data compromise due to vulnerabilities on their system?

Barclaycard can help you with contractual clauses.

If encryption is proposed, tapes or disk drives (if using VOIP recording systems) used to record the information must be clearly labelled, inventoried and encrypted following PCI DSS encryption guidelines.

Pay particular attention to sensitive authentication data, storage is not permitted.

Access to the physical tapes as well as logical access to the product used to record the calls should be restricted.

All interaction with the recordings should be logged.

Storage and backup of the recording solution must not become a backdoor to this solution. Organisations must satisfy themselves with the supplier's recommended process for data backups and archiving.

A destruction policy should be put in place such that recordings are not kept any longer than necessary. This also helps you meet the 5th principle of the UK Data Protection Act 1998: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

It is advisable to find a call recording product allowing you to track logical and physical access to media containing data. It should also provide encryption features, strong authentication and detailed reporting and logging.

Work with your QSA and your acquiring bank to put in place a compensating control that fits your business model and maintains the highest security levels. If required, you will need to demonstrate that due to FSA compliance regulations (or other business reasons), you may need to store this data and demonstrate that you are using every available means to protect the data to meet the original intent of PCI DSS relevant controls. Encryption of sensitive cardholder information is not a "by default" option and will always be done via a compensating control.

Barclaycard: innovation and responsibility

- Barclaycard is innovative - First to introduce credit cards in 1966 & contactless technology in 2007.
- Trusted brand with 11.9 million customers, and one in five credit cards in the UK in our portfolio
- We continually invest in technology in order to remain ahead of our competitors and enhance our service to customers
- We are a responsible lender, adapting and improving our products and services to help our customers.
- We help retailers acquire payments and help them meet their business objectives with easy to set up and cost-effective acquiring package.
- Leading the way in payment security:
 - PCI Security Standards Council Board of Advisors member
 - PCI SSC Participating Organisation
 - Dedicated Payment Security Team
 - Online resources
 - Publications
- We are a responsible business by treating our people, our local communities and the environment well.

References

Barclaycard payment security and PCI DSS Information
www.barclaycard.co.uk/pcidss

Payment Card Industry Security Standards Council
www.pcisecuritystandards.org/index.html

Visa downloads and resources (where vulnerability guidance can also be found)
www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp

Contact us

For more information on this paper and other payment security matters please email
PCIDSS.Guide@barclaycard.co.uk

This document is available in large print, Braille and audio by calling [0844 811 6666](tel:0844 811 6666)

*Calls may be monitored or recorded to maintain high levels of security and quality of service. For BT business customers, calls to 0844 811 numbers will cost no more than 5p per minute, min call charge 5.9p (current at April 2010). The price on non-BT phone lines may be different.

Barclaycard is a trading name of Barclays Bank PLC. Barclays Bank PLC is authorised and regulated by the Financial Services Authority. Registered in England. Registered No. 1026167. Registered Office: 1 Churchill Place, London E14 5HP