



Call Recording Protocol October 2011

Background

The implementation of recording of telephone calls was agreed in order to support effective training and delivery of brilliant customer service, and to enable us to deal efficiently with internal or external complaints.

Scope

This procedure details how the call recording software is managed and by whom. The current software is supplied by Redbox Recorders (RBR2600 & Virtual Observer systems).

Care centre - Tunstall

Responsibilities

The Customer Services Service Manager is responsible for ensuring that the measures detailed in this procedure are fit for purpose and applied.

Each individual allocated access to playback calls is responsible for ensuring that they:

- Keep their password secure
- follow the IT Security Policy guidance on password security
- only access calls for the purposes outlined in this procedure.

The ICT Service Manager is responsible for:

- the ongoing maintenance of the software and any associated hardware
- the annual deletion of recordings older than the stated maximum retention period for the call
- password management (e.g. forgotten passwords)
- the back-up of software and recordings



Procedure

Which calls are to be recorded?

All calls received or made from nominated extensions will be recorded.

The areas which will have nominated extensions set to record as at end of March 2010 are:

On the Redbox system

- All extensions within the call centre at Grantham (excepting 406402).
- All desks within the Grantham Customer Services centre, Meet/Greet and switchboard. (Excludes Booths currently).
- All extensions within the area offices that are used by Customer Services staff.
- Benefits 'call centre' extensions
- Revenue 'call centre' extensions
- Repairs 'call centre' extensions

On the Tunstall System – Supported Housing

- Out of Hours emergency telephone - 01476 590044
- Care Centre office telephone – internal only
- Lone Worker telephone – internal only
- Care Centre community alarm service telephones

On the Tunstall System – Community Safety and Licensing

- CCTV emergency line – internal only??

Recording will include any internal conversations between officers whilst an external call is 'held' on any nominated extension. Once however a call is fully transferred, the recording will cease, unless the extension the call is transferred to is also a nominated extension.

Purely internal calls that are made from or to a nominated extension number will also be recorded.

It is anticipated that once call recording is established, we may extend the functionality to other areas within the Council.



Notification

For telephone callers, we will maintain a message at the beginning of all the IVR messages to advise callers;

“Calls may be recorded”

In addition, we will maintain a similar statement on our website. This protocol will also be listed within the Customer Services pages of the website for customer information.

Callers through to the Benefits team will hear an additional message relating to potential fraud;

“Your call may be recorded for training and service improvement purposes, and to help prevent and detect fraud”

Callers to the Care Centre community alarm service telephones do not hear a recorded message but are advised that calls to the line are recorded in the information leaflet when they join the scheme.

NB: should any caller insist that their call is not recorded, we will consider calling them from an unrecorded telephone or mobile.

Security

All recordings are kept within a secure server.

The system is PCI SS (payment card institute for security standards) and FSA (financial services authority) compliant. This includes that the software will not allow any ‘manipulation’ of a recording. This guarantees that any playback is a true record. (See Appendix)

‘Historical records of voice recording is regarded as non-business critical for back up and business continuity purposes. Off-site storage of back up data is not required and any restore of data will be carried out with best endeavours using on site backup.’

Access for staff

Access and playback of recordings will be carefully controlled. Only those with the appropriate authority can access calls. They are required to



maintain a secure and private password, which is auditable and traceable within the software.

The password chosen must meet minimum guidance for security as advised within the Council's ICT Usage Policy.

Access to calls may be for a number of reasons. We anticipate that the three main reasons will be for checking accuracy, answering complaints, and for training to improve service and skills.

Recorded calls can also be used to support council tax administration as the call can provide the evidence to support changes to the council tax system.

Any individual officer may request to hear call recordings in which they are personally involved, and any Service Manager may request to hear call recordings which involve a member of their team. They should make a written request detailing the reason for hearing the recording to:

- For Customer Services recordings either the Customer Services Coordinator or the Customer Services Service Manager, or in their absence, the Head of HR and Customer Service.
- For Benefits recordings either the Benefits Manager or the Revenues and Benefits Service Manager, or in their absence, the Head of Finance.
- For Revenues recordings either the Revenues Manager or the Revenues and Benefits Service Manager, or in their absence, the Head of Finance
- For Repairs recordings either the Repairs Team Leader or the Property and Facilities Manager, or in their absence the Head of Assets
- For Supported Housing recordings, the Supported Housing Manager or in their absence the Head of Housing and Neighbourhoods
- For Community Safety recordings, the CCTV Operational Supervisor or the Community safety and Licensing Manager or in their absence the Head of Environmental Services



This may include Human Resources or the Disciplinary Hearing Panel for recordings used as evidence in a disciplinary process.

Members will not normally have access to listen to recorded calls unless the call relates to them, or they have the written authorisation of the requester.

Access for external customers

Customers / callers have the right to listen to or have copies of recordings made of their own calls. We will facilitate this through whichever media is most appropriate (e.g. streaming, CD). Requests made to listen to calls from other parties on behalf of the subject will need to be made via the 'Subject Access Information Request Form' available online from the documents tab on the page for 'Data Protection'.

General Access Frequency

For Customer Services staff, within staff training and development we anticipate that there will be regular 1-2-1 development sessions between line managers and staff, during which recorded calls may be played in order to support the process. These may be monthly, bi-monthly, or quarterly. We may increase the frequency if any member of staff is under the capability procedure, if a staff member is undergoing induction, or is learning a new service.

Storage Duration

If recorded, calls made in relation to Housing and Council Tax Benefit claims will need to be stored for a minimum of six years if used as evidence in support of a benefit claim.

Recorded calls for all other services will be held for a minimum 12 months and a maximum of 24 months; there is an annual process managed by the BTAIM team to purge records older than the stated maximum periods.



Call Recording and Compliance

Statement of Compliance

Red Box Recorders solution offers a fully compliant solution that exceeds both FSA and PCI DSS requirements. Voice recordings are stored in a secure authenticated format that cannot be manipulated or altered ensuring total compliance with FSA Regulations. The technology does not allow for referencing or searching against payment card details and has security and access protection that exceeds the required standards set out by the PCI DSS.

Facts about the Regulators and Standards:

FSA – Financial Standards Authority - requires compliance to all aspects of its regulations, non compliance can result in cessation of trading and or fines and or legal proceedings – for further information refer to: www.fsa.gov.uk

MiFID – Markets in Financial Instruments Directive – came into effect on 1 November 2007, replacing the Investment Services Directive (ISD). Amendments to UK legislation and rules to transpose to its provisions were made by the deadline of 31 January and came into effect on 1 November 2007. MiFID extends the coverage of the ISD and introduces new and more extensive requirements that firms will have to adapt to, in particular for their conduct of business and internal organisation. MiFID is controlled and regulated by the FSA. – For further information refer to: www.fsa.gov.uk/pages/About/What/International/mifid/

PCI DSS – Payment Card Institute for Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection – This is a voluntary set of standards to which organisations can subscribe and so use the PCI DSS association. It has no legal bearing or rights. – For further information refer to: www.pcisecuritystandards.org

APACS - Association of Payment and Clearing Services standards make sure that the payment systems work in the most efficient, cost-effective, unambiguous way. These are standards for payment system providers to adhere to and are for manufacturers not users. – For further information refer to: www.apacs.org.uk

Regulatory & Standards Statements from FSA & PCI DSS:

These are exact extracts from the following documents published by the FSA & PCI DSS.

Organisations that need to comply with these regulations and standards should read all documentation published from these organisations to make an informed decision that best fits your specific organisations and application. The information here is to offer support in the decision making process and is not meant as guidance on FSA regulation or PCI DSS standards.

The FSA Regulations Stipulate That:

(From Policy Statement 08/1 - Financial Services Authority)

Telephone Recording: recording of voice conversations and electronic communications

Section: 11.8.10 R

A firm must take reasonable steps to retain all records made by it under COBS 11.8.5R:

- (1) for a period of at least 6 months from the date the record was created;
- (2) in a medium that allows the storage of the information in a way accessible for future reference by the FSA, and so that the following conditions are met:
 - (a) the FSA must be able to access the records readily;
 - (b) it must be possible for any corrections or other amendments, and the contents of the records prior to such corrections and amendments, to be easily ascertained;
 - (c) it must not be possible for the records to be otherwise manipulated or altered.



The 2008 PCI DSS Guidance States:

(Requirements and Security Assessment Procedures, Version 1.2, October 2008)

Protect Cardholder Data - Requirement 3: Protect stored cardholder data

3.2.2 Do not store the card verification code or value (three digit or four-digit number printed on the front or back of a payment card) used to verify card-not present transactions. Note: See PCI DSS Glossary of

Terms, Abbreviations, and Acronyms for additional information.

3.2.2 For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:

- Incoming transaction data
- All logs (for example, transaction, history, debugging, error)
- History files
- Trace files
- Several database schemas
- Database contents

Note: This does NOT refer to voice recordings and as the voice recording is necessary to be FSA compliant is specifically excluded from the 2008 guidelines. Some more unscrupulous manufacturers may be quoting old guidance which offered more ambiguity and an opportunity to sell. Please see additional articles from the PCI DSS website below.

Quotes from PCI DSS on Voice Recording:

The PCI standard Council States in FAQ about voice recording

(Taken from PCI DSS Website, Nov 2008)

Question:

Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of the PCI DSS?

Answer:

This response is 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 by the payment brands). This response is intended to provide clarification for call centers regarding their potential storage of card validation codes and values, and their compliance with the PCI DSS. It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after transaction authorization. Call centers may find themselves in the position of receiving cardholder data which includes sensitive authentication data, and they may be unable to delete this sensitive data since individual elements cannot easily be deleted from an audio recording. To clarify, these call centers and all cardholder data are IN SCOPE for PCI DSS. However, if the storage of card validation codes and values meets the unique circumstances described in this response AND these values are protected according to all applicable PCI DSS requirements, those card validation codes and values may be stored. If commercially reasonable technology exists to delete these data elements, then these elements should be deleted. If the individual data elements within an audio file can never be queried, then only the physical and logical protections defined in PCI DSS version 1.1 must be applied to these audio files. Additionally, if these audio files that can never be queried are copied to magnetic tape media, that media must also be protected in accordance with PCI DSS. However, if card validation codes and values stored on audio files are subject to technology that allows for the capture and transposition of the speech/audio data into a format that can be queried (for example digital or other file formats), then the sensitive authentication data, including card validation codes and values, must not be stored and must be deleted immediately after authorization. Again, this response applies only to call centers and card validation codes and values. All other cardholder data captured by call centers must be protected in accordance with the PCI DSS, including PCI DSS requirement 3.4. In addition, this response does not to apply to any other entity besides call centers, and all other entities must protect all cardholder data in accordance with PCI DSS, including requirements 3.2 and 3.4



White Paper
Technical Information

PCI Question of the Quarter - 06 March 2008

(Taken from PCI DSS Website, Nov 2008)

I just got Winter 2008 newsletter from the PCI Council. In addition to reinforcing the Council's commitment to education (e.g., Bob Russo is speaking at our PCI Workshop in May) there was a neat feature: the question of the quarter. It deals with call centers and recordings that may include cardholder information, including CVV2/CVC2. Since many institutions have automated voice response units or use call centers for phone-a-thons, I thought I'd post the question and answer here. IMHO, the answer and approach are instructive in that they focus on the intent of the requirement and match it to the business realities:

Question:

Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of the PCI DSS?

Answer:

This response is 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 by the payment brands). This response is intended to provide clarification for call centers regarding their potential storage of card validation codes and values, and their compliance with the PCI DSS.

It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after transaction authorization. Call centers may find themselves in the position of receiving cardholder data which includes sensitive authentication data, and they may be unable to delete this sensitive data since individual elements cannot easily be deleted from an audio recording. To clarify, these call centers and all cardholder data are IN SCOPE for PCI DSS. However, if the storage of card validation codes and values meets the unique circumstances described in this response AND these values are protected according to all applicable PCI DSS requirements, those card validation codes and values may be stored. If commercially reasonable technology exists to delete these data elements, then these elements should be deleted.

If the individual data elements within an audio file can never be queried, then only the physical and logical protections defined in PCI DSS version 1.1 must be applied to these audio files. Additionally, if these audio files that can never be queried are copied to magnetic tape media, that media must also be protected in accordance with PCI DSS.

However, if card validation codes and values stored on audio files are subject to technology that allows for the capture and transposition of the speech/audio data into a format that can be queried (for example digital or other file formats), then the sensitive authentication data, including card validation codes and values, must not be stored and must be deleted immediately after authorization.

Again, this response applies only to call centers and card validation codes and values. All other cardholder data captured by call centers must be protected in accordance with the PCI DSS, including PCI DSS requirement 3.4.

In addition, this response does not to apply to any other entity besides call centers, and all other entities must protect all cardholder data in accordance with PCI DSS, including requirements 3.2 and 3.4

Contacts & Information:

For further information on Red Box Recorders products and solutions or to discuss compliance and standards further please speak to your local Red Box Recorders representative.



Red Box Recorders Limited
The Coach House, Tollerton Hall
Tollerton, Nottingham. UK
NG12 4GQ
Tel: +44 (0) 115 937 7100
Fax: +44 (0) 115 9377494
Email: sales@redboxrecorders.com
Web: www.redboxrecorders.com