

Protecting telephone-based card payment data

PCI SSC Guidelines Update SIG

Presentation to The UK Cards Association, Acquirer SIG & PCI Standards Security Council

John Greenwood – Document Author
London

9th June 2016



Our starting point

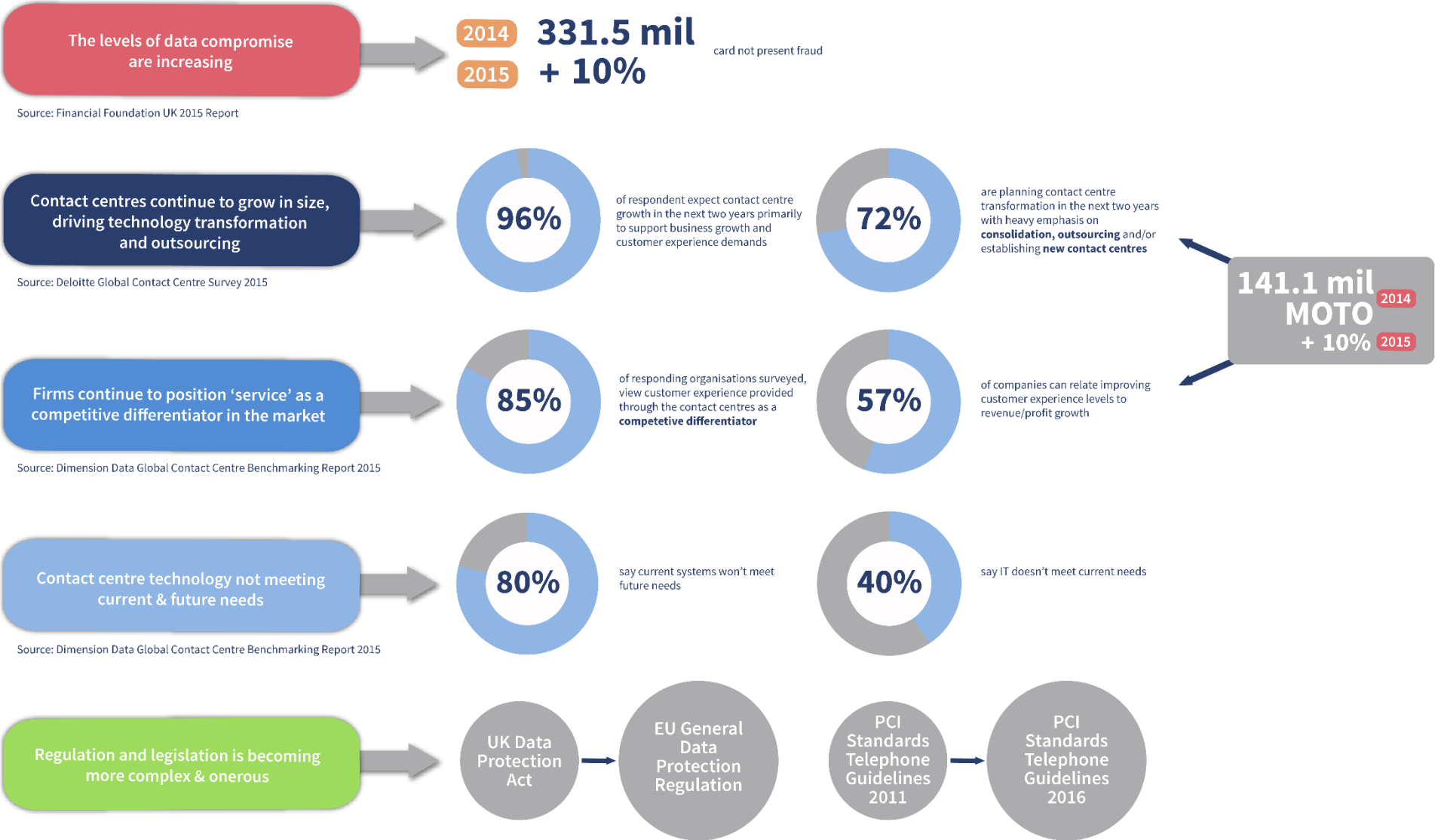
- PCI DSS Version 2.0 from March 2011
- Limited / no vendor input
- Focus on stored card data and call recording
- Limited vendor input
- Opportunity to update to V3.x
- Bring in vendor input
- Initiated by JK, Semafone, Eckoh, Trustwave & Vendorcom
- Chaired & authored by Compliance3
- Kicking off with a new Semafone draft



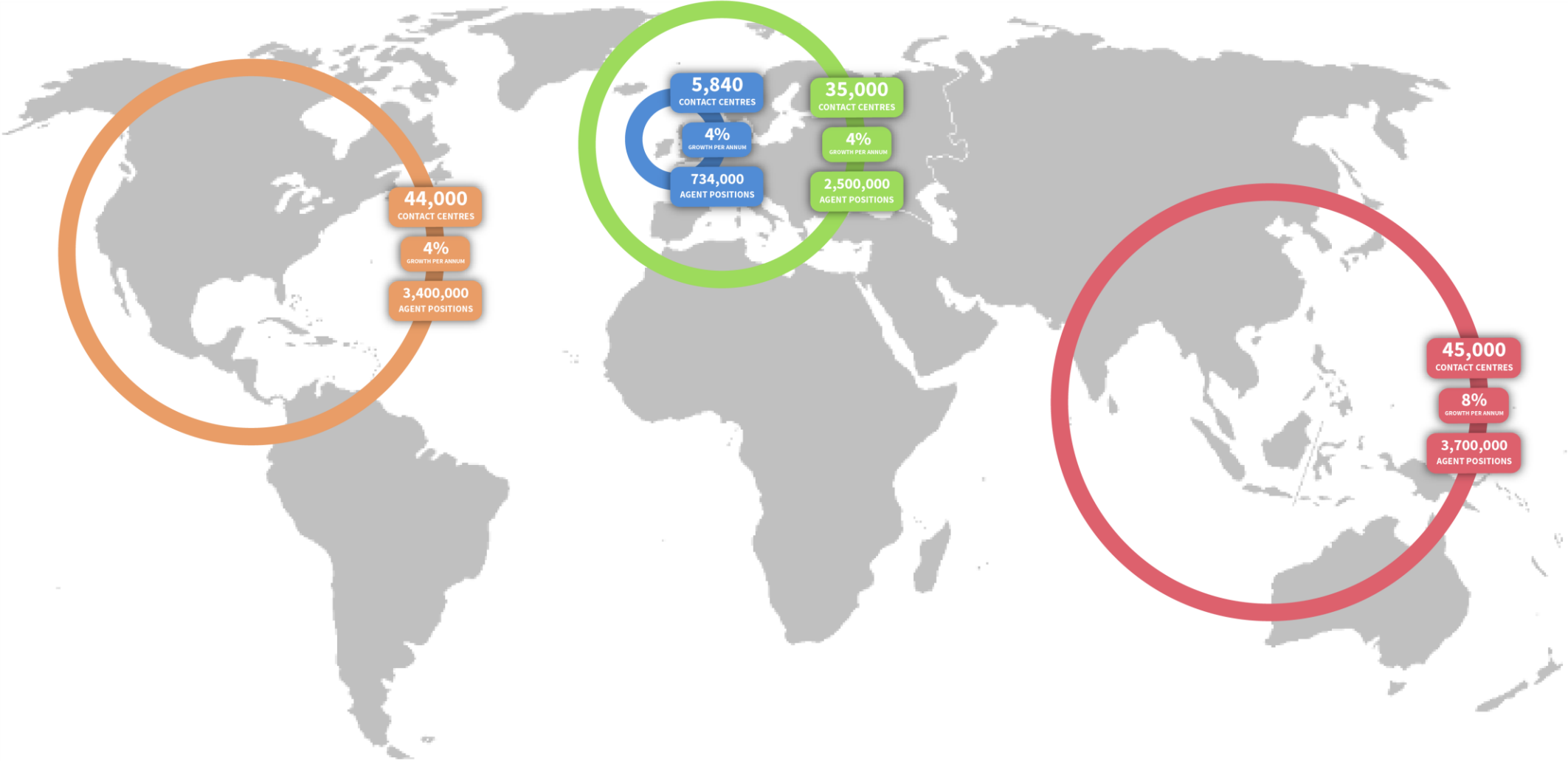
Basic principles of the S.I.G

- Vendorcom S.I.G. with reach to non-members inc US vendors
- Same title - Telephone not call centre or contact centre
- Same format & headings
- Utilise as much existing text as possible
- Update rather than replace
- Factual not opinionated
- First draft to JK before end of Oct
- Be in a position to publish by 31st Jan

Validating the problem: the data



The scale of the challenge: the opportunity



“Using technology to devalue the data.”

“To get risk off the table.”

*Stephen Orfei
GM PCI Security Standards Council
2015 European Community Meeting.
Nice - November 3-5 2015*

Approach: to be as inclusive as possible



S.I.G. challenges: what was ahead of us?

- Emphasise WHY?
- Identify WHO and confirm the audience
- Different understanding of common terms e.g. DTMF solutions, PCI DSS Scope, CDE & CP Data Flow Diagram
- Different understanding of impact on scope e.g. pause resume
- Educate and simplify the messages
- Keep text relevant & not vendor or technology type specific
- Embracing a 'collective view' — Vendors, QSA's, Acquirers / PSP's & PCI SSC

Solutions: what we did

- Used as much PCI SSC published content as we could
- Leverage existing content
 - Third-Party Security Assurance Information
 - Managing Shared Responsibilities with Third Party Service Providers (TPSP)
 - Small Firms Guidelines
- Existing Glossary supported by NEW GLOSSARY filling the gaps
- NEW TERMS “Telephone Environment” & technology groups
 - “Type 1 – Attended”
 - “Type 2 – Unattended”
 - “Type 3 – Partial scope reduction”
- Pictures paints etc – Use of diagrams to help simplify & educate

New guidelines: content headings

1. Introduction – what and who?
2. Why are Telephone Environments at risk?
3. Why are Telephone Environments in scope?
4. Key risk areas associated with telephone payments
5. Common approaches to securing Telephone Environments
6. Potential PCI DSS scope reduction based on technology type
7. Guidelines on PCI DSS Guidelines on TPSP's
8. Summary & Appendices (Glossary & Contributing Organisations)

New guidelines: who?

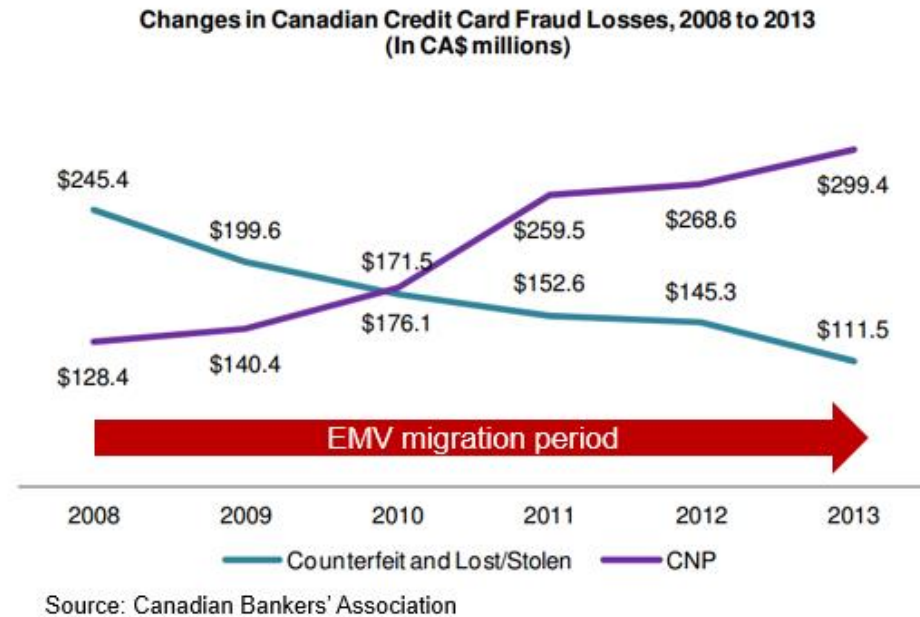
This document seeks to provide guidance to ALL business entities that *store, process and or transmit* CHD as a result of an interaction with a customer over the telephone in any business environment as well as the Qualified Security Assessor (QSA) and Internal Security Assessor (ISA) communities that support them.

This includes merchants of all sizes as well as Third Party Service Providers (TPSP) that take Mail Order Telephone Order (MOTO) payments, issue refunds or manage repeat transactions on behalf of merchants.

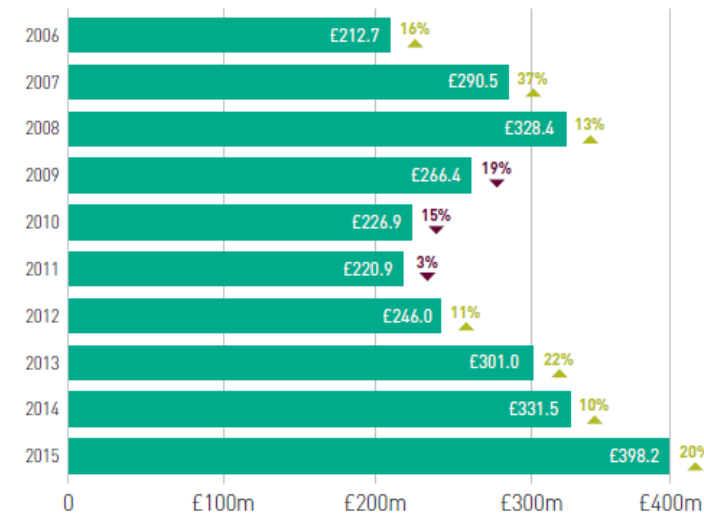
The guidance in this document therefore applies to any person within the business that *stores, processes and or transmits* CHD over the telephone as part of a MOTO transaction. This includes;

- Business entities that use telephony as a significant proportion of their card acceptance payment channels and do so in high volumes or have plans to accept high volume telephony payments.
- Merchants that are considering outsourcing telephony payment acceptance to a call centre operator.
- Acquirers. Issuers and other industry professionals including QSA's, ISA's, TPSP's, the Call & Contact Centre community and all associated technology vendors.
- Small enterprises in all business sectors. The PCI Council website provides additional guidelines specifically aimed at helping small business apply PCI DSS. This is a helpful addition to this document and can be found at <https://www.pcisecuritystandards.org/>

New guidelines: why?



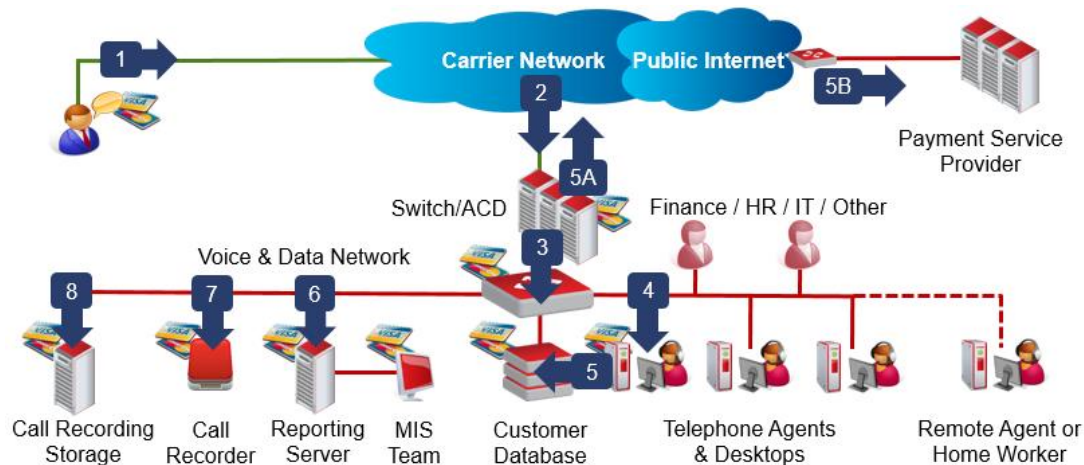
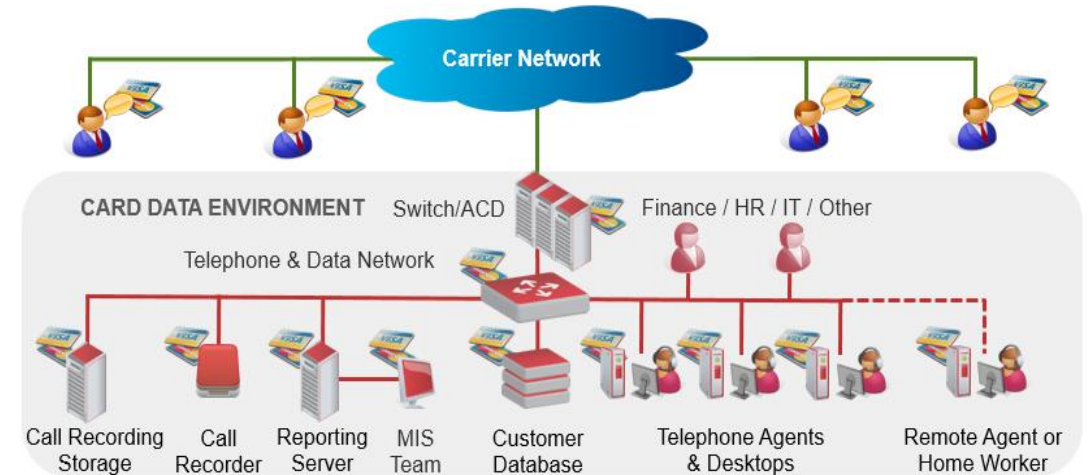
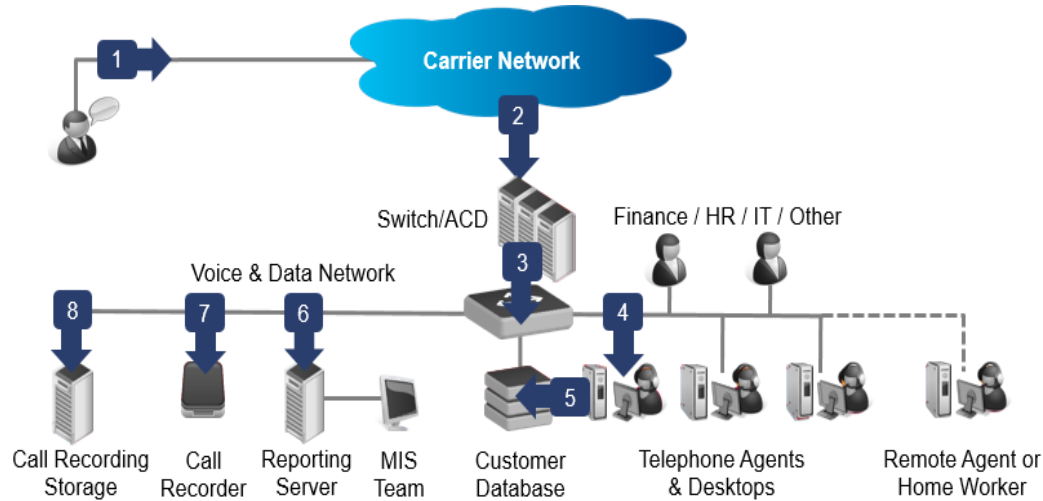
REMOTE PURCHASE (CNP) FRAUD LOSSES ON UK-ISSUED CARDS 2006–2015
Arrows show percentage change on previous year's total



Detective Chief Inspector Mark Wilkie of the UK's, South Yorkshire Police in a statement he made in 2011. **“Call centre internal compromise is the biggest form of up and coming fraud in the UK.”**

Two years later, in their 2013 Annual Report, Financial Fraud Action UK (the body conducting the CNP fraud study above) wrote, **“Chip and Pin fraud is now migrating away from the internet to other card-not-present channels, such as the telephone.”**

New guidelines: scope & CDE explained



It is the responsibility of the business themselves to determine the CDE and the Scope of the Telephone Environment where the 12 PCI DSS Requirements and controls apply.

Businesses may contact a QSA if they have any questions about their Card Data Environment or Scope when using technology options, compensating controls or combinations of both.

Full listings of QSA firms that are locally available can be found on the PCI Council website <https://www.pcisecuritystandards.org>.

New guidelines: specific advice in different operational areas

Best managed using a modular approach.

Signposting People – Process - Technology

- IT networks and telephony systems (e.g. switches, IVRs, MS Active Directory, DHCP etc)
- Agents, Customer Service Representatives and or Operators
- Physical Environment (Agent, Customer Service Representatives and or Operators)
- Agent Desktop / Operator Terminal and their order processing systems
- Voice and Screen Recordings
- Scope creep and corporate / other networks not involved in payments being brought into Scope and / or being a potential access vector to CHD

New guidelines: voice recordings

Where an entity, via a technology malfunction or otherwise, has failed to prevent the storage of SAD after authorisation (even though it has always been part of the businesses contractual obligations with the Card Brands and / or their Acquirer) the business MUST take all possible steps to immediately delete those recordings and if uncertain, contact a QSA or their Acquirer for advice on legitimate remediation options.

Where conflicting business or legislative requirements exist, the business may consult with their Card Brands, their Acquirer and or a QSA, in considering options to manage those historical call recordings, some of which are listed below:

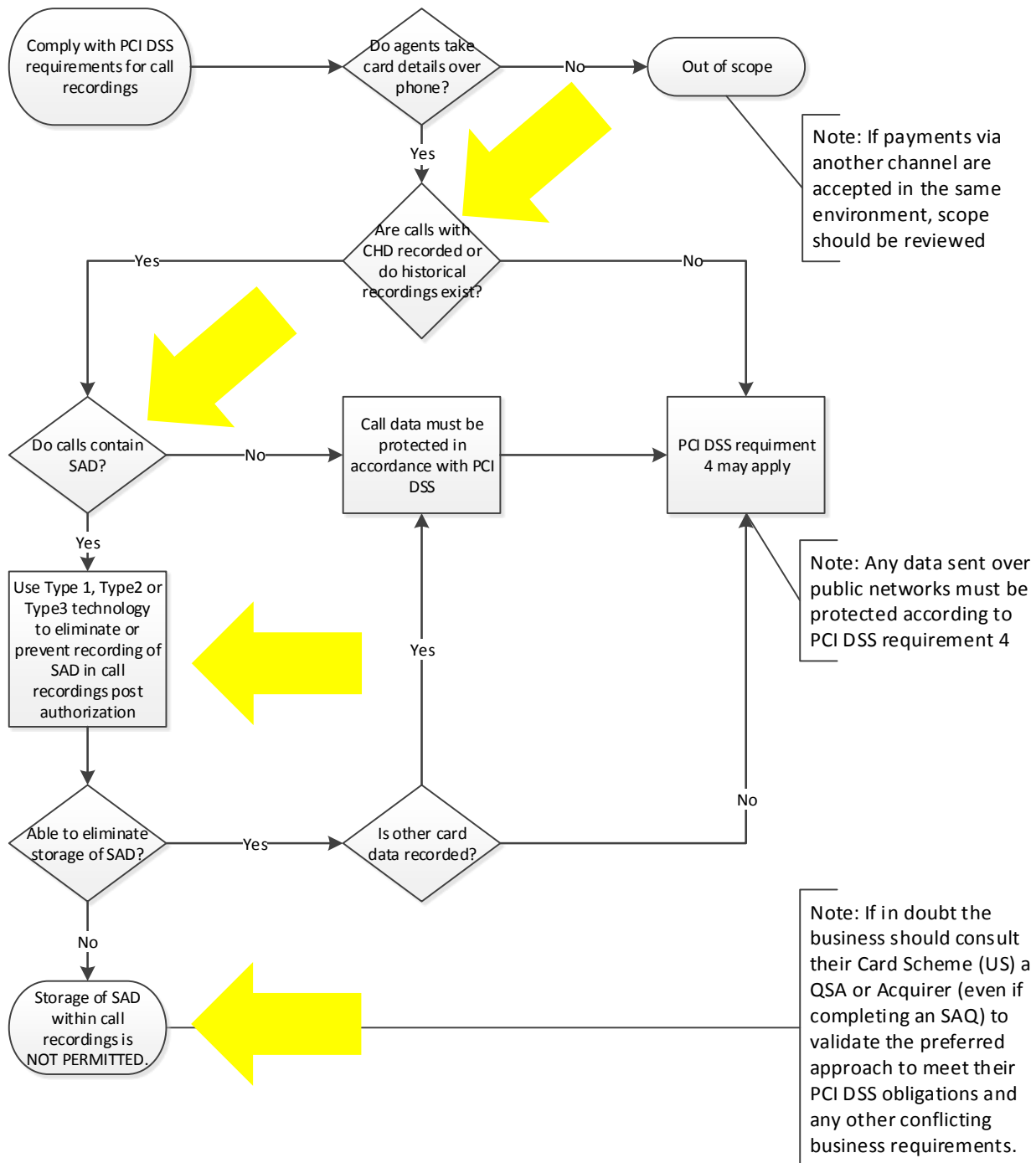
Removing call recordings from the call recording solution and deleting it using a secure delete function

Taking the historical call recordings offline and securing them in a PCI DSS compliant manner outside the Telephone Environment with an appropriately PCI DSS certified TPSP that may or may not allow remote PCI DSS complaint access to those historical call recordings.

Having made every effort to delete SAD, vaulting the call recordings in a PCI DSS compliant manner, enforcing dual access controls and allowing only single call recordings to be retrieved from vaults at a time.

Note that there may well be local or regional laws that may govern the retention of audio recordings and PCI DSS expressly states that any such laws will take precedence.

If technologies are available to fulfil PCI DSS requirements without contravening government laws and regulations, these technologies should be used.



Changes

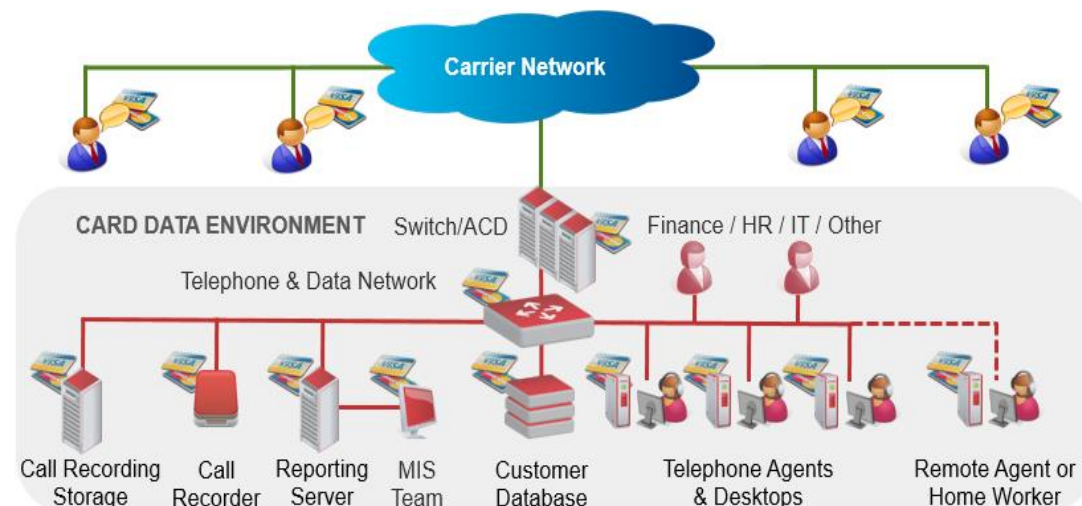
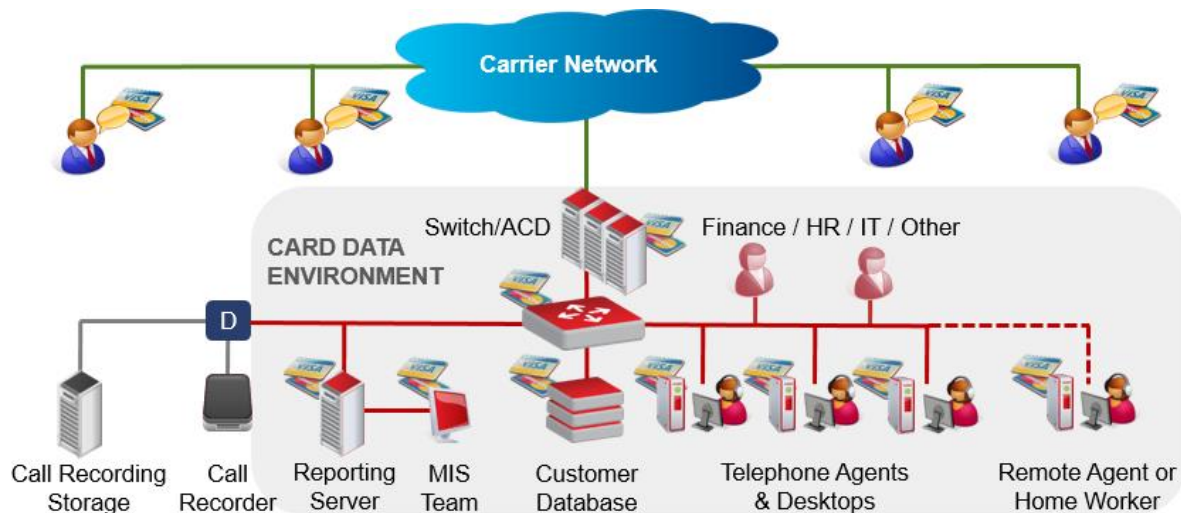
- Simplify – telephony types
- Considered historical call recordings
- Added technology deployment to reduce scope
- Noted referral to Scheme, QSA & Acquirer

New guidelines: clarity on technology types to reduce scope

- **Type 1. Attended** – where the Agent remains in direct voice contact with the customer for the entire duration of the transaction.
- **Type 2. Unattended** – where the Agent does not remain in direct voice contact with the customer for the entire duration of the transaction.
- **Type 3. Partial** – Part Scope Reduction where only part of the Telephone Environment is taken out of Scope – which means applying ALL Requirements Controls to the reduced CDE.

New guidelines: clarity on manual pause resume & scope

Evidence from QSA's, Acquirers, card schemes and merchants since the last publication of these guidelines, has shown that Pause Resume solutions can be problematic and have been shown to require constant monitoring to ensure no CHD enters the Call Recorder or Call Recording Storage. This has led the PCI Standards Security Council to make a significant change to the guidelines securing telephone based data within Call Recorders and the Call Recording Storage.





Whilst it remains the business entities choice and that **manual** Pause Resume may continue to be a helpful part of a risk reduction approach, **the PCI Standards Security Council now consider that deployment of manual Pause Resume technology will NOT take the Call Recorder or the Call Recording Storage out of scope of PCI DSS**

This means that if a business entity has historically only deployed **manual** Pause Resume believing Diagram 6 (above) best described their CDE, then that is no longer the case and Diagram 3 (on page 7) now applies.

New guidelines: overview of technology impact on scope by type

KEY:

 PCI Requirements that may be taken OUT OF SCOPE depending on technology deployed

 PCI Requirements that will remain IN SCOPE depending on technology deployed

PCI DSS GOAL	PCI DSS REQUIREMENTS	TECHNOLOGY DEPLOYED		
		TYPE 1 'ATTENDED'	TYPE 2 'UNATTENDED'	TYPE 3 'PARTIAL'
Build and Maintain a Secure Network and Systems	1	Potential for NO CDE TO EXIST Taking Requirements OUT OF SCOPE Scope & CDE dependent on point of point of technology deployment.	Potential for NO CDE TO EXIST Taking Requirements OUT OF SCOPE Scope & CDE dependent on point of point of technology deployment.	ALL REQUIREMENTS APPLY To the areas of the Telephone Environment THAT ARE IN SCOPE. Scope and CDE dependent on the technology and the point of deployment.
	2			
Protect Card Holder Data	3			
	4			
Maintain Vulnerability Management Programme	5			
	6			
Implement Strong Access Control Methods	7			
	8			
	9			
Regularly Monitor & Test Networks	10			
	11			
Maintain an Information Security Policy	12	REQUIREMENT 12 WILL ALWAYS APPLY. Irrespective of technology selected and deployed. Special attention to Requirement 12.8 is using TPSP.		

New guidelines: summary of sections

1. Introduction.

If your business is not a card scheme or telephony carrier supplying carrier services, and your business *stores, processes* and or *transmits* CHD over the telephone as part of a MOTO transaction, then the guidelines in this document apply to you.

If you are a QSA, ISA, Issuer, Acquirer or a Third Party Service Provider supporting part of a merchants MOTO payment process, then this document also applies to you.

The section also introduces a new term, Telephone Environment which is defined in the new Glossary section as the “*General term used to describe a MOTO transaction completed in any business location that may store, process or transmit payment card data via the telephone. This description covers MOTO transactions only within small and large offices locations, hotel reception desks, customer service teams, call and contact centres.*”

2. Why are Telephone Environments at risk?

Evidence from consumer markets where risk mitigation technologies such as EMV and point to point encryption (P2PE) are being implemented for card-present (CP) transactions (Canada & UK) is showing that criminals are increasingly turning to card-not-present (CNP) fraud. Studies show that CNP fraud is increasing year on year.

Telephone based transactions are at risk because of the open exposure to spoken card holder data and the vast differences in the security of the environments where telephone based MOTO payments are taken.

3. Why are Telephone Environments in scope of PCI DSS?

Telephone Environments are in scope when card holder data is spoken by the customer and listened to by the person taking the call.

The diagrams in this section describe clearly what infrastructure and technology equipment makes up the Card Data Environment and is therefore in scope.

This section also makes clear that is the entities responsibility to define scope and if in doubt refer to a QSA (or your internal ISA) who will be able to provide expert guidance whilst referencing the guidelines detailed in this document.

4. Key risk areas associated with telephone payments

This section starts by describing the complexity of telephone environments. Every business entity needs to evaluate the risks for their own Telephone Environment using a modular approach. This section covers the following areas typical areas of risk associated with telephone payments;

- IT networks and telephony systems (e.g. switches, IVRs, MS Active Directory, DHCP etc)
- Agents, Customer Service Representatives and or Operators
- Physical Environment of the Agent, Customer Service Representatives and or Operators
- Agent Desktop / Operator Terminal and their order processing systems
- Voice and Screen Recordings
- Scope creep and corporate / other networks not involved in payments being brought into Scope and or being a potential access vector to CHD

The section also provides a flow diagram to support decision making when securing the call recording process and call recording storage. This guidance stresses that PAN & SAD cannot be stored together and promotes seeking further guidance from your Acquirer, Card Scheme or QSA if in doubt.

New guidelines: summary of sections (continued)

5. Common approaches to securing Telephone Environments

Entities should first consider why taking payments over the phone is essential to their customer experience and business model.

Based on taking payments over the telephone being an ongoing business benefit, this section strongly promotes an overall approach to minimise the CDE and reduce the scope of PCI DSS. This approach being proven to reduce the time, cost and effort of delivering and maintaining PCI DSS compliance and ongoing certification.

The section then simply groups all available technologies into three types,

- Type 1. ATTENDED – where the Agent remains in direct voice contact with the customer for the entire duration of the transaction.
- Type 2. UNATTENDED – where the Agent does not remain in direct voice contact with the customer for the entire duration of the transaction.
- Type 3. PARTIAL – Part Scope Reduction where only part of the Telephone Environment is taken out of Scope – which means applying ALL Requirements Controls to the reduced CDE.

A general explanation of each technology type is then provided supported by diagrams illustrating the impact of each technology type on the CDE and PCI DSS Scope.

The document also highlights a key change from previous PCI SSC's guidelines as applying to manual Pause Resume technology. Whilst the new guidelines position the technology as an effective part of a risk reduction approach, the document makes clear that manual Pause Resume no longer takes the Call Recorder and Call Recording Storage out of PCI DSS scope.

6. Potential PCI DSS scope reduction based on type of technology deployment

This section provides an overview of the impact of each technology type (Type 1 ATTENDED, Type2 UNATTENDED and Type3 PARTIAL) on overall scope, considering each PCI DSS Requirement.

The section makes clear that irrespective of the level of scope reduction, Requirement 12 will always apply, with specific attention drawn to Requirement 12.8 (managing Third Party Service Providers)

7. Clarification of the PCI DSS Guidelines for Third Party Service Providers (TPSP's)

This section provides an overview of existing PCI SSC documentation relating to the management of Third Party Service Providers (TPSP).

The aim of this section is to provide a handy reference rather than seeking to replicate existing documents.

8. Additional content

- **This summary.** Providing an overview of the document.
- **Appendix1.** Providing a new GLOSSARY of terms relating directly to the document and not covered elsewhere within existing PCI SSC documentation
- **List of contribution organisations.** Providing an acknowledgement of the contribution of the Special Interest Group facilitator, the documents author and the supporting contributions from the Acquiring Banks, QSA firms and all different technology vendors.

New guidelines: participating organisations

SIG facilitator: Vendorcom

Document author: Compliance3

Acquirers

Barclaycard
Worldpay

QSA Firms

Coalfire
Foregenix
NCC Group
Trustwave

Carrier

Vodafone

Technology Vendors

Aeriandi
C3
Compass Plus
Content Guru
Datadivider
Eckoh
IntraNext Systems
Paytel Solutions
PCIPal
SemaFone
Syntec
Ultra Communications

Glossary of Terms & Abbreviations

Term	Description
3-D Secure	3-D Secure is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions. Also known as Verified by Visa, MasterCard SecureCode, J/Secure and American Express SafeKey.
ACD	Acronym for Automatic Call Distributor. A programmable device deployed in the telephone or data network capable of directing telephone calls (data) to a predefined termination point. Also see Switch.
Agent	Person or persons employed by a business whose role it is to make or take telephone calls.
Agent Desktop	An Agent's personal computer connected to a network.
Call Flow	A call flow is a road map of how calls will be handled from the moment they enter the telephone system to the end of the call. Call flows can be used to handle even the most complex call scenarios.
Call Recording	General description of the file containing the recording of a telephone call.
Call Recording Storage	General description of a hardware device capable of storing call recordings and providing functionality to support those call recordings being searched, played back and downloaded.
Carrier	A telecom carrier is a company that is authorized by regulatory agencies to operate a telecommunications system.
CDE	Acronym for card data environment.
CNP	Acronym for card not present, a term that generally describes a transaction where the customer is not present.
CRM	Acronym for Customer Relationship Management system. A customer or booking database or reservation system.
Customer	The person calling or being called by a business.
Customer Contact Strategy	General description of an approach to maintain contact with customers that may include contacting the customer or receiving contact with the customer across different channels or media.
Customer Service Representative or CSR	Person or persons employed by a business whose role it is to make or take telephone calls and serve customers. Please also refer to Agent and Operator.
Customer Experience	A general term describing how the customer is managed by an Agent or CSR.
Data Breach	A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
Demarcation Point	In telephony, the demarcation point is the point at which the public switched telephone network ends and connects with the customer's on-premises wiring. Also the dividing line which determines who is responsible for installation, maintenance and service. A network interface device can often serve as the demarcation point.
Devalue Data	Used to describe a general approach to make data less attractive and less valuable to criminals and organized crime. To take risk off the table. In the context of securing telephone-based payments, this means taking spoken card data out of the Telephone Environment by preventing card data being spoken to the Agent and to prevent the possibility (and capability) of payment card data being recorded.

Term	Description
DTMF. Also known as Touch-Tone.	Acronym given to Dual Tone Multi-Frequency. A telecommunication signalling system using the voice-frequency band over telephone lines between telephone equipment and other communications devices and switching centers. Known in the USA under the trademark Touch-Tone for use in push-button telephones.
EMV	Eurocard Mastercard Visa standard for Card Present transactions
ISDN	Acronym given to an Integrated services for digital network. Described as a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
IVR	Acronym for an interactive voice response application. An automated application that allows the customer to make choices by pressing the required digit on their telephone handset.
MOTO	Standing for Mail Order Telephone Order
Operator	Person or persons employed by a business whose role it is to make or take telephone calls.
Operator Terminal	An Operator's personal computer (connected to a network).
Pause Resume	General description of manual or automated applications that pause and resume the call recording application at the point that a customer speaks their payment card data.
PABX / PBX	Acronym given to a Public Automated Branch Exchange or Public Branch Exchange. Also see Switch
PDQ	Standing for 'Process Data Quickly', PDQ machines are also known by a number of other names including credit card machines.
PSTN	Acronym given to the public switched telephone network. This is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication.
Scope	A general description of the Card Data Environment where the PCI DSS should be applied.
Scope Reduction Strategy	A structured plan that a business would document to reduce the size of their CDE by reducing their ability to store, process or transmit payment card data. This may be achieved through a change in Customer Contact Strategy, the deployment of technologies described in this document and the use of Third Party Service Providers.
Screen Recordings	The recordings of Agent Desktop screens showing the data that they are capturing / entering into the CRM system or customer or booking database or reservation system, etc.
SIP	A VoIP and streaming media service based on the Session Initiation Protocol (SIP) by which Internet telephony service providers (ITSPs) deliver telephone services and unified communications to customers equipped with SIP-based private branch exchange (IP-PBX) and Unified Communications facilities.
Switch	General term given to a device that directs telephone calls or data to a single or multiple predefined destinations within a network.
Telephone Connectivity	The connectivity of one telephony service to another or to telephony related equipment. See also Demarcation Point.
Telephone Environment	General term used to describe a MOTO transaction completed in any business location that may store, process or transmit payment card data via the telephone. This description covers MOTO transactions only within small and large offices locations, hotel reception desks, customer service teams, call and contact centres.
Voice Recordings	General description for recorded telephone calls.
VoIP	Acronym for Voice over Internet Protocol. A method that enables people to use Internet Protocol as the transmission medium for telephone calls by sending voice data in packets.

Next steps: discussion points

- Review & sign off by PCI SSC
- Message communication
 - Acquirer community
 - QSA community
 - Contact centre community
 - Industry groups (UK, EU, North America, APAC)
 - Merchant groups
- PCI Community
 - Regional community meetings
 - General communication

Thank you for your attention. Questions?

John Greenwood

john@compliance3.com

+44 7767 354 354

