semafone
secure voice transactions

How to Take your Contact Centre Out of Scope for PCI DSS

Reducing Cost and Risk in Credit Card Transactions for Contact Centres

Contents

4 Executive Summary

6 PCI DSS Background

8 PCI DSS – What's Involved

10 Two Ways to Eliminate the Need for Customer Card Data

13 The Challenge for the Contact Centre

14 How Semafone Removes Card Data from the Contact Centre

15 Removing Card Data from Call Recordings

16 Reducing the Scope of PCI DSS Audits for the Contact Centre

19 The Cost of Compliance

20 Take your Contact Centre out of Scope

22 Glossary

Executive Summary

PCI DSS and the battle against card fraud

It is now a decade since version 1.0 of the Payment Card Industry Data Security Standard (PCI DSS) was released. PCI DSS was the result of an agreement between five different payment card companies; Visa, MasterCard, American Express, Discover, and JCB. It was designed to ensure that merchants meet minimum levels of security when storing, processing and transmitting cardholder data. Ten years later, the PCI DSS standard is still in place worldwide and is now in its third incarnation.

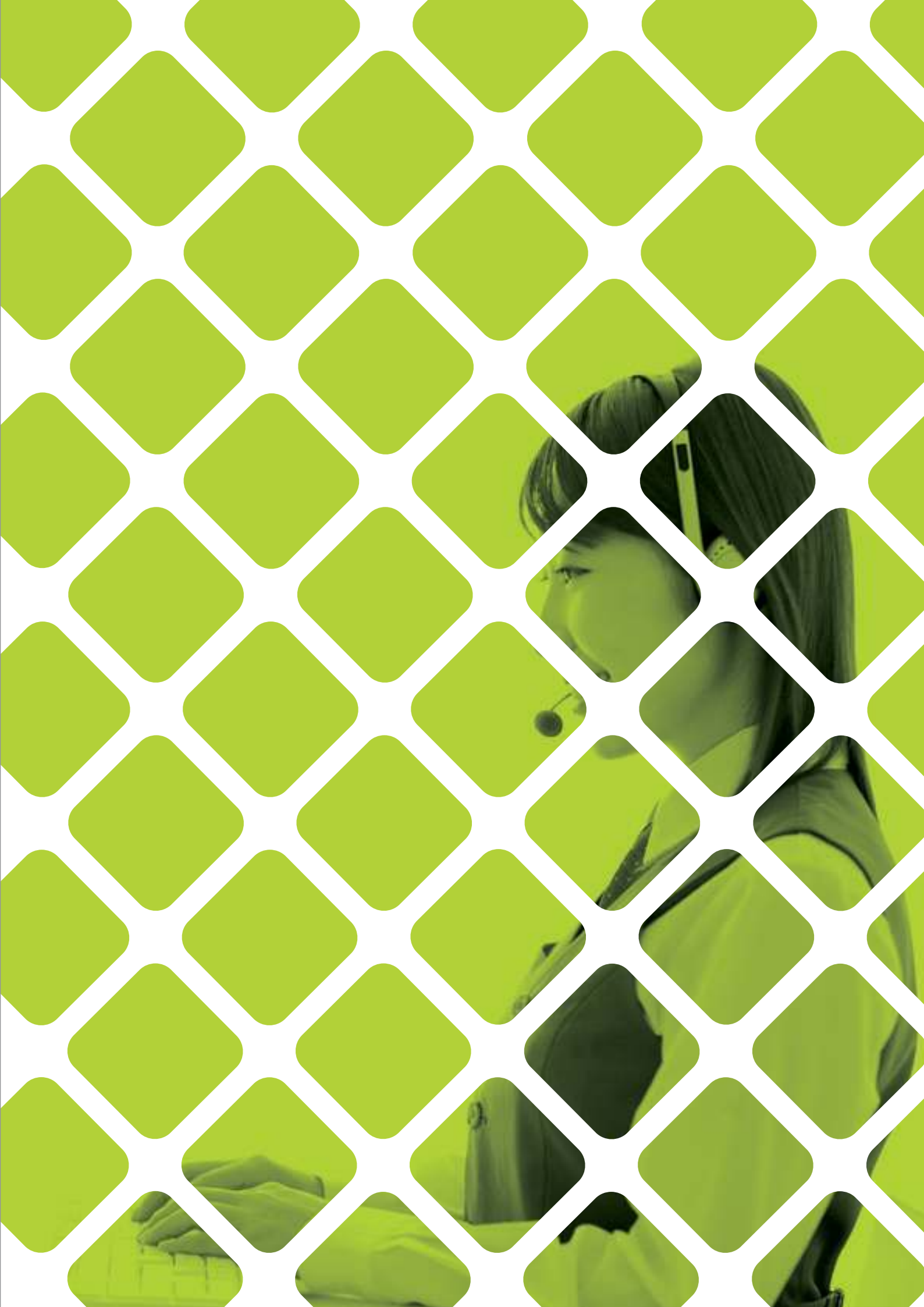
The battle against payment card fraud continues to rage. Between 2011 and 2012, fraud losses on UK credit and debit cards increased by 14 per cent to £388 million per year, according to statistics from financial services trade body *Financial Fraud Action*[1]. These revelations were followed by the Ponemon Institute's 2013 *Cost of Data Breach*[2] survey, which reported that UK organisations suffering data security breaches now face costs of over £2 million per incident.

The need for PCI compliance has never been greater. Yet while board level awareness of the standard has increased dramatically, the cost and complexity of implementation is still a concern. As new technologies have emerged to help merchants to comply with the standard, it has become increasingly apparent that by far the most effective and painless way of complying with PCI DSS is to minimize, or eliminate altogether, the customer card data that they hold in their infrastructure. Known as "de-scoping", this has become the holy grail of PCI DSS compliance.

Two key technologies; tokenisation and point-to-point encryption, have contributed to simplifying the process for both high street and online retail channels, but telephone payments continue to pose additional challenges. The close integration between telephony and the IT infrastructure, and the need to record customer calls, serve to make the task significantly more difficult.

To address this, Semafone® has incorporated these technologies into a unique solution which offers contact centres a secure method of handling card payments that are made over the phone. Semafone's patented payment method removes the risk of fraud and achieves PCI compliance by ensuring that payment information is neither seen nor heard by the contact centre agent, nor processed through the IT infrastructure of the organisation.

1. Financial Fraud Action - Fraud the Facts 2013 http://www.financialfraudaction.org.uk/publications/
2. Ponemon: Cost of Data Breach 2013 http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013



Introduction
PCI DSS Background

The Payment Card Industry Data Security Standard (PCI DSS) is the proprietary information security standard defined by the major card companies to help combat fraud and protect consumer card data.

Its members include Visa, MasterCard, American Express, Discover and JCB. PCI DSS applies to all organisations that store, process or transmit cardholder information, from any of these members' cards.

The type of annual assessment required varies according to "level", which is defined according to the volume of payment transactions that are handled. Level 1 organisations, with over six million payment transactions per year, must have their annual compliance assessment carried out by an independent Qualified Security Assessor (QSA). Those handling between one and six million payment transactions are classed as Level 2 and can receive sign-off from an Internal Security Assessor (ISA), while the majority of companies with less than 1 million payment transactions per year are classed as Level 3 or Level 4 and are able to use a Self-Assessment Questionnaire (SAQ).

The current version of the standard *(v3.0 since November 2013[3])* specifies 12 requirements, organised into six "control objectives".

3. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI DSS Requirements

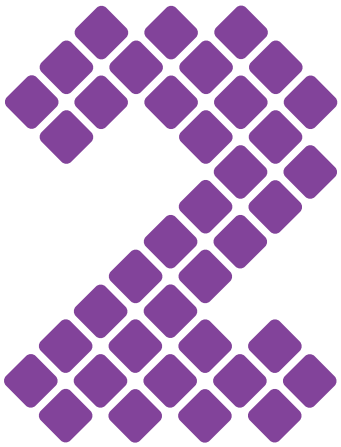
Control Objective	PCI DSS Requirement
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management programme	5. Protect all systems against malware and regularly update anti-virus software or programmes 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. Identify and authenticate access to system components 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

PCI DSS – What's Involved

PCI DSS has five types of SAQ to be completed. The table shows how different types of SAQ require fewer controls and can therefore cut the cost of PCI DSS compliance.

Description	No. of Controls
A. Card-not-present (e-commerce or mail/telephone order) merchants, with all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*	4
B. Merchant only uses imprint machines and/or standalone dial-out terminals, not connected to any other systems or the internet, with no electronic cardholder data storage.	29
C-VT. Merchant only uses web-based virtual terminals, with no electronic cardholder data storage.	60
C. Merchants with payment application systems connected to the internet, with no electronic cardholder data storage.	80
D. All other merchants (not included in descriptions for SAQs A through C above) and all service providers defined by a payment brand as eligible to complete an SAQ.	286

"The most effective and painless way of complying with PCI DSS is to minimize, or eliminate altogether, the customer card data held in the merchant's infrastructure"



Ways to Eliminate the Need for Customer Card Data

PCI DSS requires that merchants must eliminate, render useless, substitute or secure (encrypted to the standards of PCI DSS) all cardholder data.

It was once rare that cardholder data could be totally eliminated as it was required for refunds, future purchases, loyalty programs, reconciliation, etc. Today, however, merchants can do this using tokenisation to substitute their stored card data with “tokens”. This is happening on the high street through point-to-point encryption and in ecommerce through hosted payment pages.

PCI DSS Applicability Information

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	✓	✓
		Cardholder Name	✓	×
		Service Code	✓	×
		Expiration Date	✓	×
	Sensitive Authentication Data	Full Track Data	×	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	×	Cannot store per Requirement 3.2
		PIN/PIN Block	×	Cannot store per Requirement 3.2

1 Point-To-Point Encryption

Point-to-point encryption, known as P2PE, can be used to protect and secure cardholder data between two end points. In July 2013, the PCI Security Standards Council issued a *guide*[4] to solution requirements and testing procedures for point-to-point encryption, with the goal of reducing the scope of PCI DSS assessment for merchants using such solutions.

P2PE solutions can help reduce the PCI DSS scope of merchants by eliminating clear-text account data from a merchant's environment, or by isolating the P2PE environment from clear-text account data that is present in any other of the merchant's payment channels.

2 Tokenisation

Tokenisation can replace cardholder data, i.e. the credit or debit card number, with non-sensitive data that can be used as a reference or a token. The card data is then vaulted, usually by a third party, where again it is protected through encryption.

Format-Preserving Encryption and Tokenisation

Encryption and tokenisation can both be used, so that the encrypted value or the token retains the format of the original card number. It is also possible to retain the first six digits (the Banking Identification Number – BIN – which identifies the issuing bank) and the last four digits which do not need to be masked for PCI DSS, so they can be used by production applications and viewed by users.

"Tokenisation and point-to-point encryption have contributed to simplifying the PCI compliance process for both high street and online retail channels"

4. Point to point encryption solution requirements and testing procedures: https://www.pcisecuritystandards.org/documents/P2PE_v1-1.pdf

"Making telephone payments PCI compliant is challenging. The close integration between telephony and the IT infrastructure, and the need to record customer calls, make the task significantly more difficult"

The Challenge for the Contact Centre

Technology and services for the de-scoping of high street and online retailers are already well established, with chip and PIN machines where the customer is present and payment pages hosted by the merchant's Payment Service Provider (PSP) for online transactions.

However, the contact centre has its own distinct issues, with four specific challenges to address for PCI DSS compliance:

- The physical contact centre environment
- Call and screen recordings
- VoIP and telephony network
- Agent desktops and data network

Securing the Physical Contact Centre Environment

PCI DSS requires that employees are screened for security purposes. If paper and pens are available, however, then other controls come into play. Any writing paper needs to be secured and later destroyed so that cardholder data cannot be reconstructed. As a result, many contact centres have adopted paperless environments with only white boards and markers available.

Agents' access to cardholder data also means that PCI DSS requires a policy covering access to mobile phones, the web and email, as staff could theoretically use these tools to transmit cardholder data out of the merchant's environment. Draconian measures such as the prohibition of pens, paper, mobile phones, personal effects, email access and web access can have a very negative impact on the contact centre. Staff retention becomes difficult in a working environment in which all employees are treated as potential thieves. To have no email or web access within a contact centre is also impractical as both are often required to fulfil day to day activities.

Call and Screen Recordings

Customers share both cardholder data and Sensitive Authentication Data (SAD) i.e. the PAN (Permanent Account Number), expiry date, issue number and their security code (CVV2, CVC2, etc). If merchants don't take the security code then the call recordings can be protected through encryption.

PCI DSS does not permit the capture of the security code on call recordings even if these recordings are encrypted. The PCI's paper, *Protecting Telephone Based Payment Card Data*[5], outlines the challenges of the contact centre. Likewise, screen recordings must not capture the security code and therefore this must be masked on the screen.

VoIP and Telephony Network

VoIP is often missed by organisations but this is in scope if card data is spoken aloud over these networks and has to adhere to all the same PCI DSS compliance controls.

Agents Desktops and Data Network

The fact that contact centre agents generally input customers' cardholder data on their behalf brings the contact centre agent's desktop into scope for PCI DSS, as the machine is being used to enter this cardholder data. This is still the case if the agent is typing the card details into a hosted payment page provided by the payment service provider.

As the contact centre desktop is connected to the merchant's network; this also immediately brings the data network into scope.

5. https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf

Removing Cardholder Data from the Contact Centre

Semafone is an accredited PCI DSS Level 1 Service Provider with a patented & PA DSS certified contact centre solution that shields all PAN and CVC2 data from agents, agent desktops, data network, VoIP network, call and screen recordings.

Agents do not hear or see cardholder data, call recordings do not capture either the PAN or CVC2, and screen recordings only capture asterisks and the last four digits of the PAN.

Agents do not ask cardholders to say their card details out loud; instead, they ask them to use the telephone keypad to enter their PAN and CVC2. Semafone masks the DTMF (Dual Tone Multi-Frequency) tones made by the cardholder's keypad and replaces them with a flat tone. This is achieved while voice communications continue between the agent and the cardholder.

The agent can then call up Semafone's 'enable payment' page for the merchant's preferred Payment Service Provider (PSP), passing across the cardholder name, transaction reference, amount and any other payment details required for authorisation (such as cardholder address). The agent will only see asterisks on the Semafone hosted web page as the cardholder enters their card data. Other than the last four, no other digits of the PAN and CVC2 are transmitted to the page.

The agent then verbally collects further payment details such as the "valid from", "valid to" and issue number and enters these details into Semafone's payment page. If the cardholder makes a mistake, they can tell the agent who will then reset the PAN or CVC2 field from a button on the hosted web page, or simply press the "star" button on their phone.

From the first six digits of the PAN (the BIN) Semafone can determine the length of the PAN. Once the last digit of the PAN has been entered by the cardholder, the agent receives a visual cue as the last four digits of the PAN being displayed on the Semafone hosted web page. Semafone performs a Luhn check (an algorithm that validates the card number) and if this fails Semafone shows the agent a message indicating that an invalid card number has been entered. The agent is then able to ask the cardholder to re-enter their card details.

Once the transaction details have been collected, the agent can request authorisation. Semafone combines the details from its hosted payment page with the PAN and CVC2 it has collected from the cardholder's DTMF tones. Semafone then securely transmits these transaction details to the merchant's PSP through the PSP's Application Programming Interface (API) service.

The PSP returns to Semafone with results including the authorisation code and the transaction token. These can be displayed by the Semafone hosted page or posted back to the agent application.

Removing Card Data from Call Recordings

Call recordings are an essential part of the modern contact centre and are mandated by the FCA (Financial Conduct Authority) for financial companies when handling collections over the phone. Recording may also be required for dealing with complaints, or used by managers for training and instruction purposes.

It is important, however, that customers' credit card data is not retained in the recordings. Semafone manages this requirement by automatically removing the card data from the recordings as they happen. The call recording will capture all voice communications but DTMF tones are masked and only a flat tone is recorded. It is therefore impossible to reverse engineer any card data from the call recording and Semafone has put the call safely outside PCI DSS scope.

The Semafone approach has several advantages over the alternative approach of Pausing recordings:

1. Pausing call recordings is often in conflict with regulatory bodies that mandate complete recordings.
2. Triggering "pause" and "resume" by hand is not a robust approach. Human error can too easily result in either the capture of card details on the call recording (and thereby the loss of PCI DSS compliance) or the missing of important sections of the call, which can cause major issues for quality monitoring and business improvement.
3. Pausing the call recording does nothing to take the following elements out of scope for PCI-DSS, leaving all of them to be addressed individually in order to achieve compliance:
   - The physical contact centre environment
   - The VoIP and telephony network
   - The agents' desktops and data network

"Customers' credit card data should not be retained in call recordings."

Reducing the Scope of PCI DSS Audits for the Contact Centre

Semafone – On-Premise

Where a merchant does not have Semafone hosted by their telephony carrier, but located on their own premises or at their datacentre, it is still possible to limit the scope of PCI DSS. The Semafone environment can be segregated by firewalls or deployed to a DMZ, so that the merchant's core network is de-scoped. Importantly, this will include the contact centre environment, including the agents' desktops.

If the merchant has no customer facing transactions it will be able to complete an SAQ C for the Semafone environment but will not need these controls outside of the segregated area. As agents do not hear or see card data there is no requirement to secure the physical contact centre environment.

For merchants with cardholder present transactions then a SAQ D will be required but again these controls will be required only in the Semafone environment within the contact centre. This means that agents can have web access, email access, mobile phones and the use of paper and pens at their desks, which creates a more productive environment and ensures higher rates of staff retention.

Level 1 Merchants Gain

Level 1 merchants need a QSA to complete their Report on Compliance (ROC) and may need to address the full 286 controls within SAQ D. If the merchant qualifies for SAQ C, however, with the permission of their acquirer the amount of controls could be reduced to, for example, just 80.

The story can be even better for Level 1 merchants qualifying for SAQ A (a growing list, including utilities such as gas, electric, water, phone, cable, satellite TV, and ecommerce businesses such as Amazon, eBay, LastMinute.com and Expedia). Qualifying for SAQ A means that with their acquirer's consent they could report "Not Applicable" to 282 of the 286 controls, leaving only a possible 4 within scope.

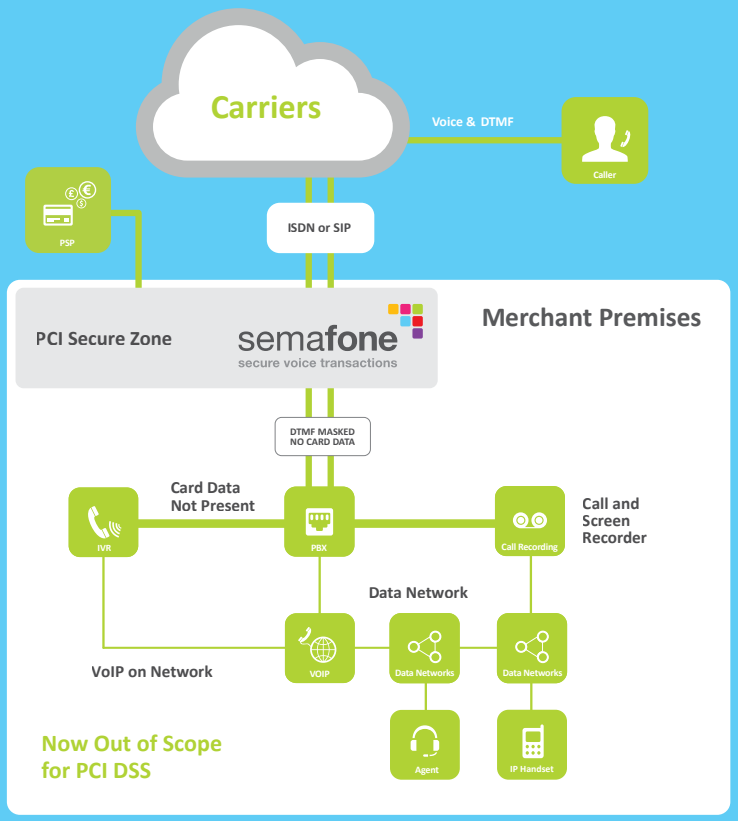
Semafone – Carrier Hosted Solution

By capturing and transmitting card data (PAN and CVC2), Semafone is in scope for PCI DSS. Semafone is available from a number of carriers and can be deployed within the infrastructure of the merchant's telephony rather than being deployed at the customer's premises.

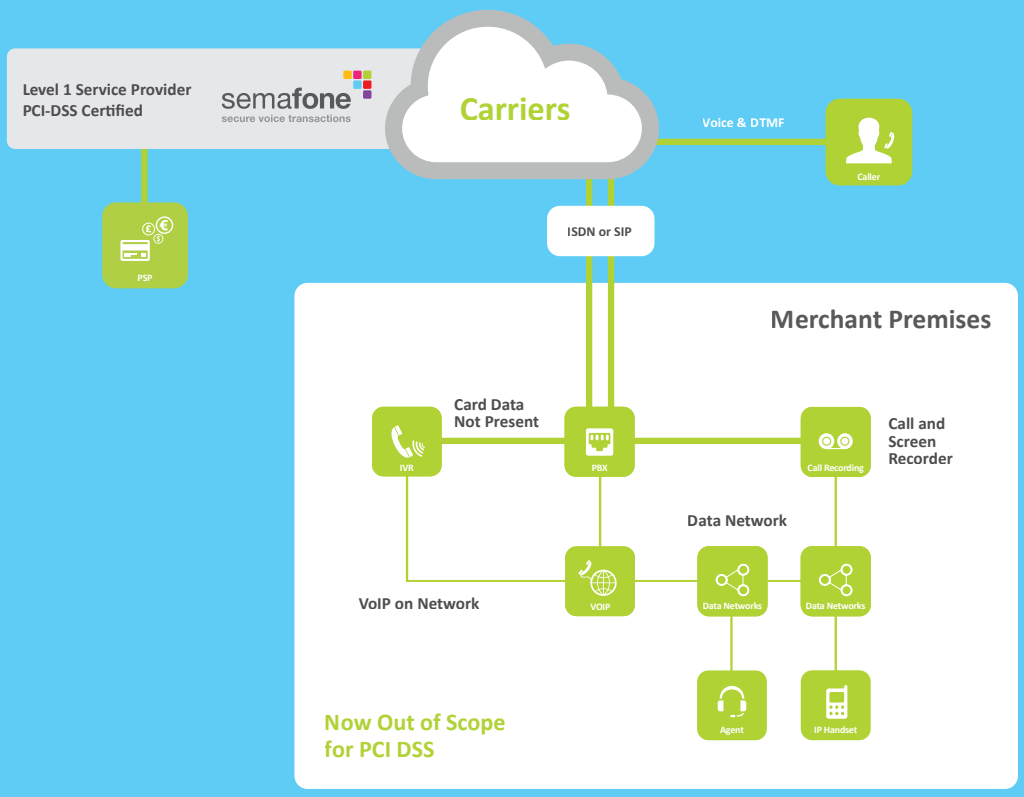
Although Semafone's solution within the carrier will have to be PCI DSS certified, the merchant will be deemed to have outsourced its payment process for PCI DSS purposes, as it will not have handled any cardholder data.

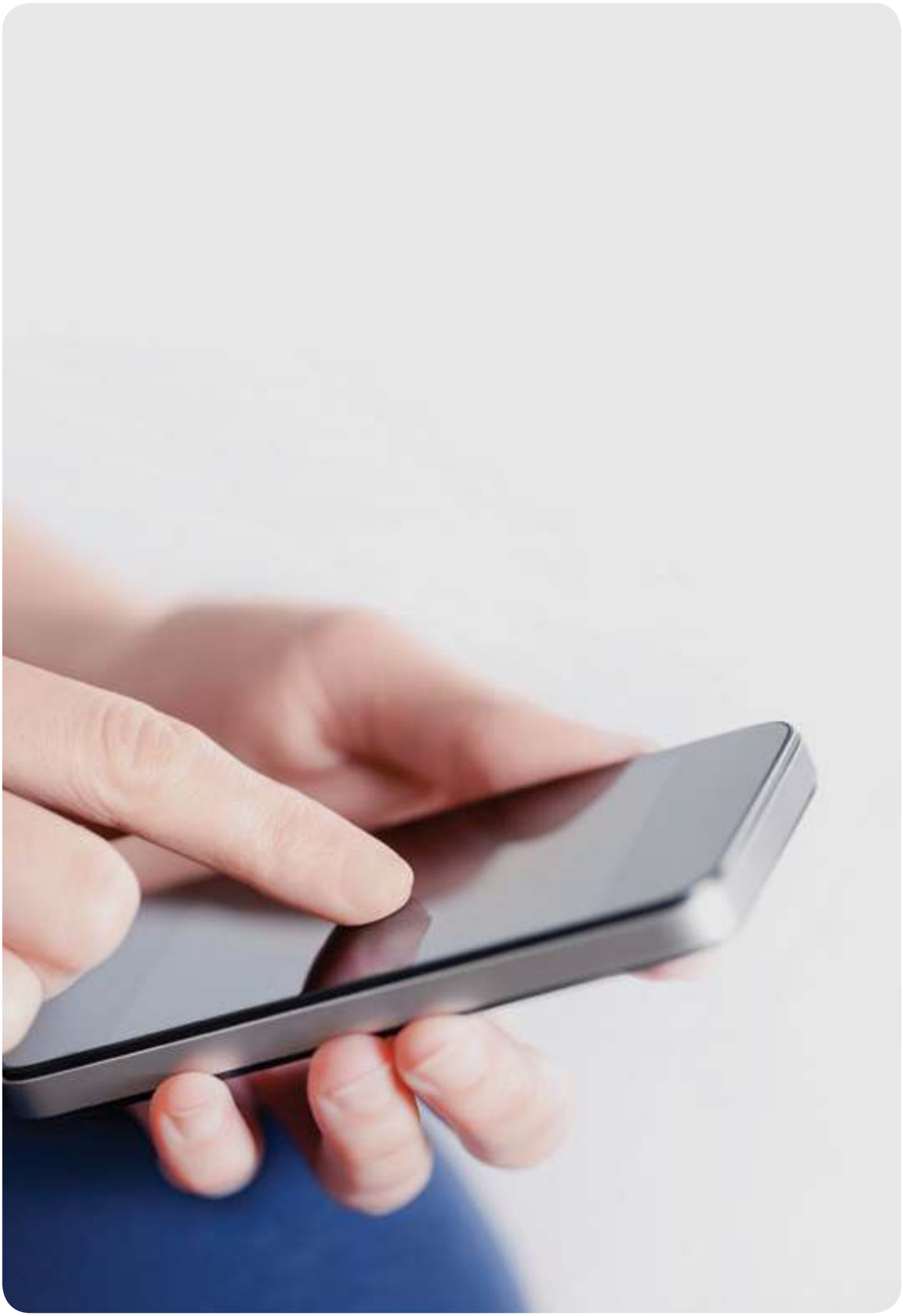
In this case, if the merchant has no customer facing card transactions, a SAQ A form may be completed, with the addition of attesting to two statements ("Restrict physical access to cardholder data" and "Maintain a policy that addresses information security"), leaving just four controls to implement for PCI DSS.

Semafone On-Premise Deployment



Semafone Carrier Hosted Deployment





The Cost of Compliance

The Ponemon Institute reported in March 2010 that Tier 1 merchants are spending £150,000 for their annual PCI DSS audits. Ten per cent of these merchants were spending more than £330,000.

These costs have not decreased. In July 2012 MasterCard added the requirement that all Level 2 merchants need an external audit through a qualified QSA or those organisations using internal auditors should have attended and passed the PCI Internal Security Assessor (ISA) training.

Retaining compliance is also expensive. While for smaller merchants, operating at level 3 or 4, compliance can be achieved relatively cost effectively, large enterprises can often find themselves spending a six figure sum. Most of these expenses are incurred by technology, such as new hardware, logging tools and security patches, along with all the hardening, maintenance and testing that comes with these.

By removing the need to handle customer card data, merchants can significantly reduce the costs of implementing and maintaining PCI DSS compliance.

Reducing PCI Audit Scope Cuts Costs

Reducing PCI scope from SAQ D to SAQ C can drive down PCI compliance and audit costs by more than 75 per cent. For merchants with no customer-facing transactions that can de-scope to SAQ A, the reduction is closer to 85 per cent. Reducing the size of a merchant's card data environment also significantly reduces the cost of achieving and maintaining PCI DSS compliance.

"Reducing the scope of the PCI audit can drive down compliance costs by more than 75%"

Take your Contact Centre out of Scope

PCI DSS compliance is continual and not just an annual audit

Merchants need to set long term objectives to reduce the risks that they run by handling cardholder data and to measure the ongoing cost of doing so. For most organisations this will involve the avoidance of managing cardholder data. The ability to achieve this on the high street and online has been well understood for some time, but the Achilles heel within the contact centre remains.

> "Semafone can reduce costs, ease the PCI DSS administrative burden and contribute to a more productive working environment for staff"

Semafone is the only company to offer a patented payment method that allows merchants to close the gap in their descoping strategy by allowing them to remove their contact centres from the scope of PCI DSS compliance. Semafone can reduce costs, ease the administrative burden and contribute to a more productive working environment for staff, helping merchants to finally realise the cost savings that they want to achieve.

Advantages of Semafone for Contact Centres

- Significantly reduced costs for PCI DSS compliance
- Zero negative impact on staff working conditions
- Enhanced security and service levels for customers

What Makes Semafone Unique

- Semafone offers a patented PA DSS certified solution
- The company is an accredited PCI DSS Level 1 Service Provider
- Semafone is a registered Visa Level 1 Merchant Agent

Semafone Delivers

- Carrier class technology
- Scalability from 50 to 10,000+ seats
- Open & flexible architecture
- Integration with leading payment processors and payment gateways

Glossary

AOC	Attestation of Compliance
API	Application Programming Interface
BIN	Banking Identification Number
CVC	Card Verification Code
CVV	Card Verification Value
DTMF	Dual Tone Multi-Frequency
DMZ	De-Militarized Zone
FCA	Financial Conduct Authority
ISA	Internal Security Assessor
P2PE	Point-to-Point Encryption
PA DSS	Payment Application Data Security Standard
PAN	Primary Account Number
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
POI	Point of Interaction
PSP	Payment Service Provider
PTS	PIN Transaction Security
ROC	Report on Compliance
SAD	Sensitive Authentication Data
SAQ	Self-Assessment Questionnaire
QSA	Qualified Security Assessor
VoIP	Voice over Internet Protocol

secured by semafone®

PCI Security Standards Council
PARTICIPATING ORGANIZATION

Semafone holds UK patent #GB 2473376 covering a number of aspects of the use of dual tone multi-frequency signalling (DTMF) to capture payment card data during a live phone call and pass it to a payment system.

More information is available at **www.semafone.com**.

semafone

secure voice transactions

+44 (0)845 543 0822

info@semafone.com

www.semafone.com

@semafone

Google+

LinkedIn

3 The Billings Walnut Tree Close Guildford Surrey GU1 4UL