SECURING TELEPHONE PAYMENTS

PCI scope reduction for MOTO

Stakeholder positioning and approach to technology selection. Structured approach to scope reduction, meeting business requirements and defining a robust business case that meets the requirements of all stakeholders.

Always delivering the right balance between customer experience, compliance and cost.

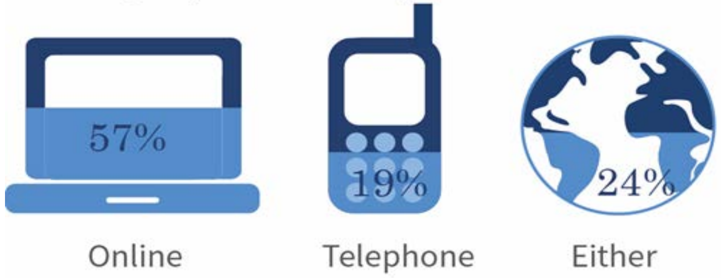
Content

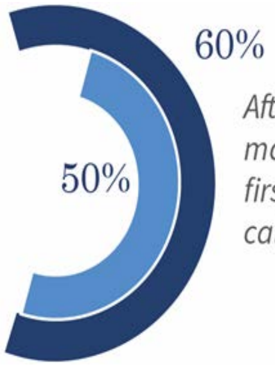
- The UK publics view on data security – per and post data compromise
- The merchants position
- PCI DSS in a nut shell
- The secure payments ecosystem
- The acquirers position
- The PCI Standards Security Council position
- The merchants challenge to secure telephone payments
- 3 step process to technology selection
- Considerations in technology selection and cost comparisons
- Compliance3 credentials and engagement model

Source: Compliance3 Consumer response to data breach. 2017

Customer view on data security

How do you prefer to share personal information?

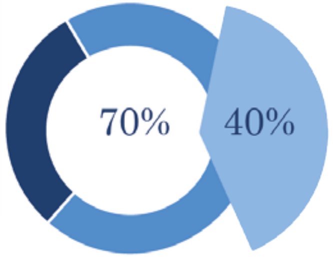




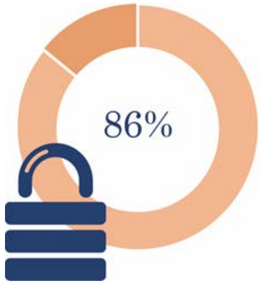
After a data breach 50% of males and 60% of females first response would be to call the customer helpline

80% want companies who don't do enough to protect payment card data to be named and shamed

3/4 of consumers believe a breached company should inform ALL customers when payment card data is compromised

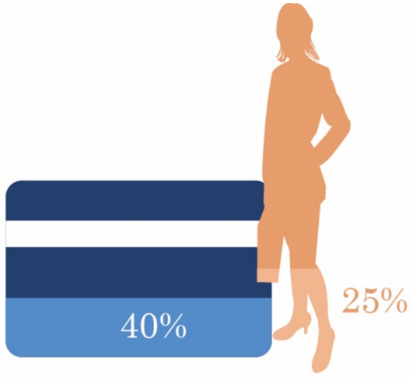


70% would tell close friends and relatives with 40% telling everyone they know that they were a victim of data breach



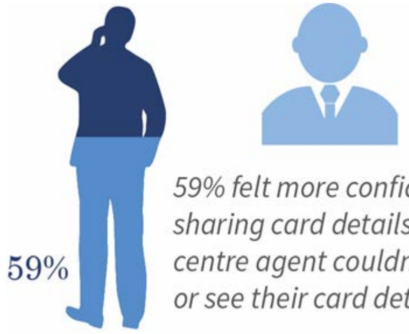
86% have felt uncomfortable during a call, due to the amount of information they were being asked to share.

Over 60% were confident that their personal data was being stored safely and securely

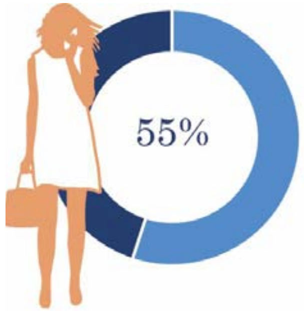


40% of consumers wouldn't buy from a breached brand whist a further 25% wouldn't buy for a while

70% want an apology and compensation after a breach



59% felt more confident sharing card details if the call centre agent couldn't hear or see their card details



55% would feel more confident sharing information if call centres complied to international data security standards

Over half would be happy to receive a compensation package worth between £20 - £100.

The Merchants position

Every merchant wants to **grow their business.** They can do that by either by increasing the **number of customers**, increasing the **number of times a customer buys** and / or, getting each customer to **spend more** when they do buy.

All merchants know that **a positive customer experience** is central to driving sales. Being able to offer card payments across all communications channels, including the telephone is key, so **secure telephone payments are important.**

In order to do that, **the merchant has to be certified as PCI DSS compliant** to meet their **contractual obligations** with their Acquirer, however, the merchant often see's PCI DSS compliance as **an unnecessary burden.**

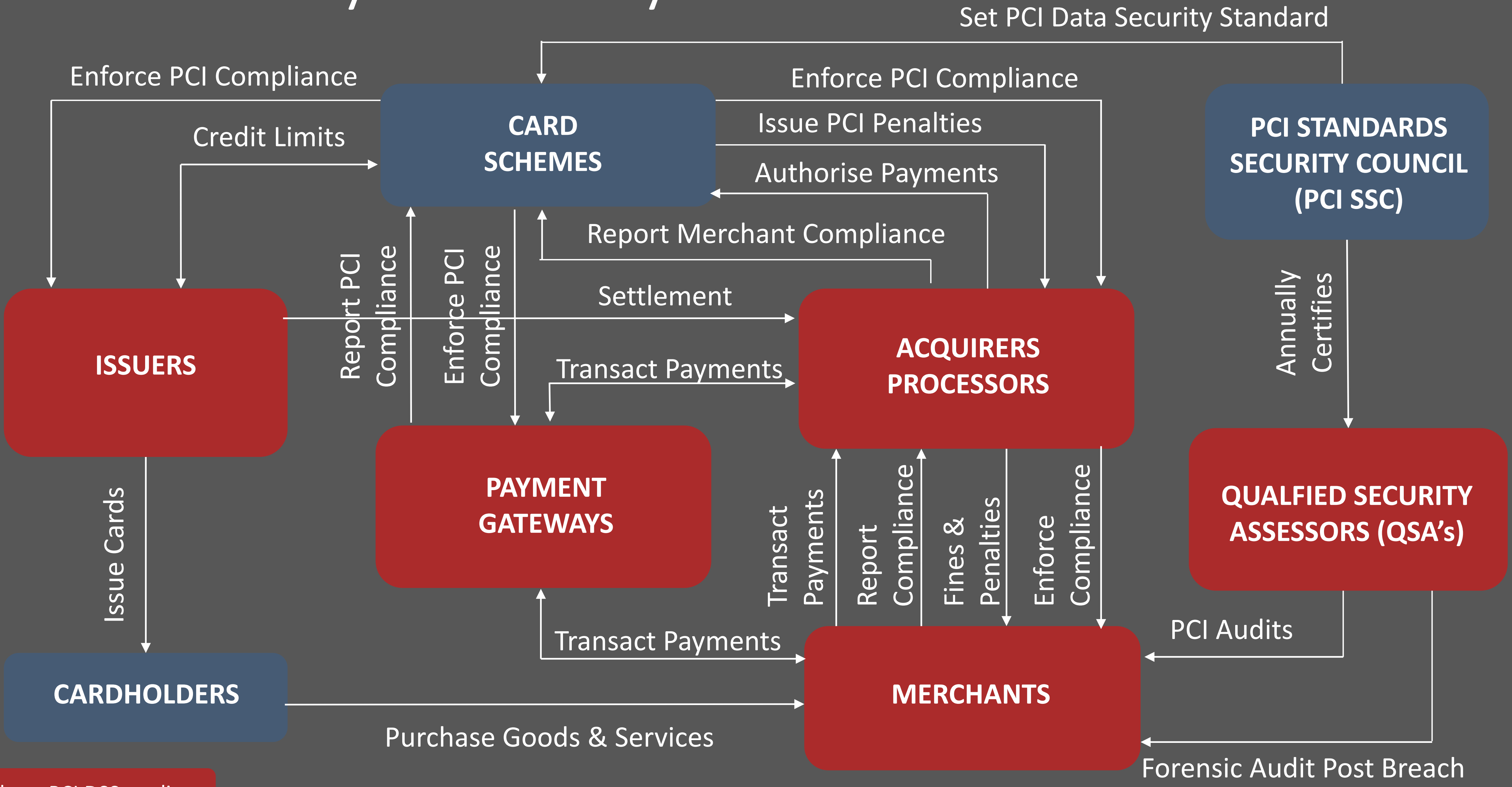
PCI in a nut shell

Established by the **payment card schemes**, as **a unified standard**, to baseline the **minimum data security requirements** necessary to **protect payment card data** within the **merchant environment** and the supporting **secure payments ecosystem**, which means issuers, acquirers and payment gateways

PCI DSS also extends to **other third party service providers** (TPSP) that **store, process or transmit payment card data, or impact the security of**. That means that the merchant has the responsibility **to ensure all their TPSP**, and those that may impact on the security of the payment card data, **are certified as PCI DSS compliant** and that the merchant monitors that compliance

NOTE: A TPSP could be a **telephone service provider** (not carriers), **payment solution** providers and **call centre** service providers.
For all supporting information please refer directly to: https://www.pcisecuritystandards.org/

The Secure Payments Ecosystem



Set PCI Data Security Standard

Enforce PCI Compliance

CARD SCHEMES

Enforce PCI Compliance

Credit Limits

Issue PCI Penalties

Authorise Payments

PCI STANDARDS SECURITY COUNCIL (PCI SSC)

Report Merchant Compliance

Report PCI Compliance

Enforce PCI Compliance

Settlement

Annually Certifies

ISSUERS

Transact Payments

ACQUIRERS PROCESSORS

PAYMENT GATEWAYS

Issue Cards

Transact Payments

Report Compliance

Fines & Penalties

Enforce Compliance

QUALFIED SECURITY ASSESSORS (QSA's)

Transact Payments

PCI Audits

CARDHOLDERS

MERCHANTS

Purchase Goods & Services

Forensic Audit Post Breach

🟥 Where PCI DSS applies

The Acquirers position

Provides the **Merchant Account** to the merchant with a Merchant ID (MID) and within the acquirers contract to supply the MID, there are terms that **commit the merchant to be PCI DSS compliant** which means, meet the minimum data security standards to store, process or transmit payment card data. It's an obligation of the Acquirer to **report the compliance status of their merchant portfolio to the payment card schemes** in accordance with the requirements of the individual payment card schemes

As the **contracting party** between the merchant and the card schemes, the Acquirer **Terms and Conditions with the Merchant** describe the implications of **non-compliance with PCI DSS**

The PCI Standards Security Council’s position

Working with **acquiring banks** to support **a channel by channel approach** to achieving and maintaining **PCI DSS compliance**

Use technology to **devalue the data** & get risk off the table.

Stephen Orfei. GM PCI Standards Security Council. Nov 2015

If you **limit exposure of payment data** in your systems, **you simplify compliance and reduce the chance of being a target** for criminals.

Troy Leach. CTO PCI Standards Security Council. Dec 2016

The Merchants challenge to secure telephone payments

●●●

How do you use technology to **devalue the data** & get risk off the table?

How do you **limit exposure of payment data** in your systems, and **simplify compliance to reduce the chance of being a target** for criminals?

ANSWER:

Reduce PCI DSS scope by deploying technology that prevents spoken payment card data entering your MOTO payments environment.

How? Take the 3 step approach to technology selection

Step 1. The customer experience

Customer experience is core to all merchants business requirements. The first question. Should the agent remain in constant voice contact with the customer for the entire duration of the transaction or not? These are described in the soon to be published PCI Standards Council Secure Telephone Payment Guidelines as ‘ATTENDED’ or ‘UNATTENDED’. The ‘UNATTENDED option might mean a fully automated experience with no agent interaction on the call, or it might mean that only the payment component of the call is automated.

ATTENDED

Agent stays in constant voice contact with the customer for the entire duration of the payment transaction.

UNATTENDED

Agent is NOT in constant voice contact with the customer for the entire duration of the payment transaction.

3 step approach to technology selection

●●●

Step 2. Current & future requirements. Digital transformation and cost of delivery

However, customer experience is not the only consideration. Understanding the merchants progress towards digital transformation, the customer contact strategy by media type, about the current telephony infrastructure and it's migration pathways, all these need to be considered alongside the time, cost and effort in maintaining compliance . This decision will ultimately be about establishing agreement between stakeholders and achieving a balance between customer experience and the overall time, resources and cost of delivering and maintaining PCI DSS compliance.

TELEPHONY BASED SOLUTIONS

Telephony route can be complex, often lengthy time lines, some significant costs in set up, monitoring and maintenance and more significantly, does nothing to reduce either transaction charges or chargebacks.

DIGITAL SOLUTIONS

Digital route is much simpler as a project to deploy (having no dependency on telephony), which means lower deployment costs, reduced costs of monitoring and maintenance, reduces transaction charges and significantly reduced chargebacks.

3 step approach to technology selection

●●●

Step 2. Current & future requirements – Impact on cost per transaction

Cost will always be a big factor. This is the step in the process where the type of solution selected has the biggest impact on ongoing transaction charges. In a nutshell, the digital channel turns an unsecure MOTO payment into a secure e'comm payment by invoking 3D Secure. Unsecure MOTO payments are charged at a higher rate by the acquiring bank. Whilst this charge may vary from acquirer to acquirer, an average would 0.3%, that's 30p in every £100 average transaction value (ATV)

TELEPHONY BASED SOLUTIONS

Whilst the telephony route offers the customer the choice of using their telephone handset (landline or mobile) to input payment card data, stolen card data can be used and unknowingly processed by the merchant potentially resulting in a chargeback and loss of stock.

DIGITAL SOLUTIONS

The digital route requires the customer to use their smartphone or a connected device to receive an SMS and / or email. Whilst a network connection is all that's required (not an internet connection) the transaction is treated as a website transaction and invokes 3 D Secure. This creates a liability shift, taking the cost of fraud away from the merchant to the acquirer and issuer.

3 step approach to technology selection

Step 3. Channel and vendor selection

In an emerging technology market, vendor selection should be very much evidence based. Which means seeking evidence to support sales claims and speaking directly to vendors existing clients to validate delivery and operational effectiveness. Check vendor PCI DSS compliance certification and QSA sign off, ensuring that the AoC covers the services being offered. If services are being resold, check the resellers insurance position and support offering.

TELEPHONY BASED SOLUTIONS

Whilst there are a number vendors offering UNATTENDED solutions (IVR based), there are much fewer offering ATTENDED solutions (circa 15 globally) and there even less that can offer a secure position against recognised industry patents. Supplies vary little in terms of deployment options and overall architecture, however there are significant variances in price, resilience, project management, deployment timelines and GDPR readiness.

DIGITAL SOLUTIONS

As in the telephony channel, there are numerous vendors in the UNATTENDED space. The ATTENDED space is new and there are a very limited number of providers. Each operates a slightly different architecture and delivery a similar customer experience. Pricing too is much the same, however, there are significant differences in GDPR readiness, PCI DSS awareness and evidence of PCI compliance certification. Ask too about SLA’s and resilience, the differences are significant. That means be prepared to ask for a valid AoC and do not accept that service providers are not required to have one.

Summary

	UNATTENDED	ATTENDED
TELEPHONY BASED SOLUTIONS	• Fully automated or Semi Attended IVR options • Different CRM integration options available • Configurable payment options • Focus on cost reduction, saving AHT and reduce agent cost per transaction	• ATTENDED telephone payment with automated agent updates on payment • SIP ready with no need for expensive hardware • None SIP options available • Full CRM integration available • Focus on delivering best customer experience
DIGITAL SOLUTIONS	• UNATTENDED Link • Standard offering from most Payment Gateways & PSP's • Simple email or SMS link • Transfer of risk by invoking 3DS reducing chargebacks • CRM integration available • Focus on cost reduction • Can be used in proactive marketing & debt collection	• ATTENDED telephone payment with automated agent updates on payment • SMS & emailed link • Transfer of risk by invoking 3DS reducing chargebacks • Full CRM integration available • Focus on balancing customer experience & cost

FEATURES & BENEFITS

- All technology options reduce PCI DSS scope. Both 'digital' options and the unattended telephony option take the entire telephony environment out of scope. However, the 'attended telephony' option is highly dependent on solution design, so check scope with a QSA before implementation.
- All solutions can be deployed with tokenisation solutions which reduce risk and helps support a 'channel by channel' approach to simplifying compliance certification.
- For merchants who are not Level 4 and processing less than 1 million new card (not token) transactions per annum, then SAQ A can be completed for the MOTO channel as part of a 'channel by channel' approach agreed with the merchants acquirer which helps reduce the time, cost and effort in compliance certification.
- Both digital solutions turn an unsecure MOTO payment into a secure ecomm payment. This means lower transaction costs and , when 3DS invoked by the merchant, shifts the burden of fraud from the merchant to the acquirer and issuer, which means a much lower volume of change backs for the merchant, reducing costs.

PCI DSS scope reduction technology selection considerations

1

Type of payment and customers motivation to pay:

What is the type of payment? Is this a sale or is this debt recovery? Is this a simple commodity sell which requires high levels of consideration and agent interaction or is it a commodity purchase? Debt collection for example requires a high degree of customer / agent interaction as do purchases requiring more consideration, where a strong sales component exists. Conversely, buying a car parking ticket or paying for Council Services requires much less merchant or agent support and where services are commoditised, cost is a greater consideration in service delivery.

2

Customer experience now and future:

Where does customer experience sit in the merchants list of priorities for the service being delivered and the customer type? What are the merchants digital transformation plans in terms of using social media and linking their contact centre to their website via chat? What does this mean for future voice communication and sales volumes? How does the merchant plan to align their current and future customer communication channels with their ability to take payments?

3

Existing technology transition projects:

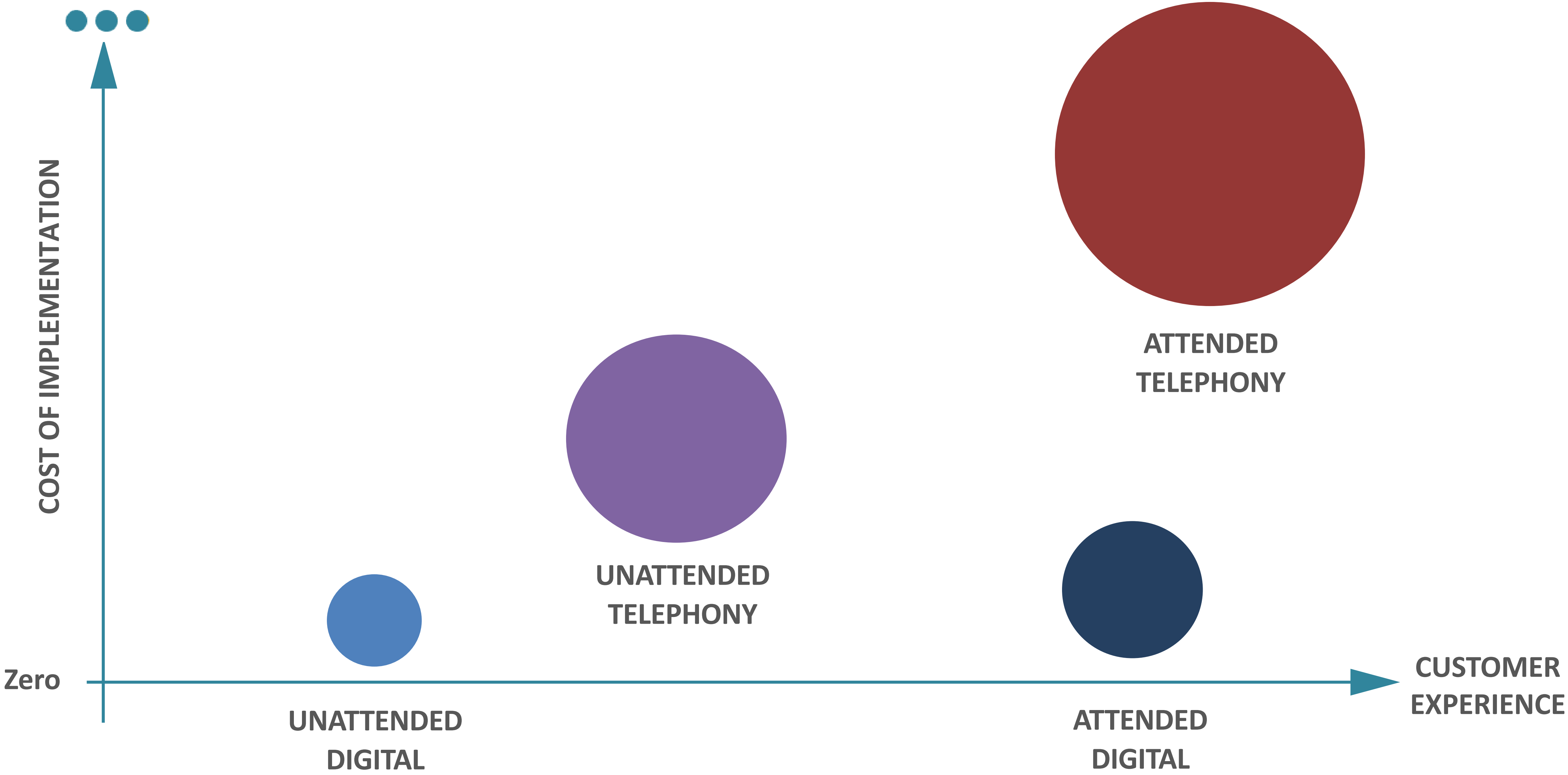
What existing telephony or data security transition projects are in play (e.g. digital transformation, ‘cloud’ transition, CRM systems change and / or GDPR project implementation) and what constraints (if any) do they have on delivering payments compliance across the payment channels? What are the dependencies on integration, timelines and costs? Where do outsourced providers fit into the mix?

4

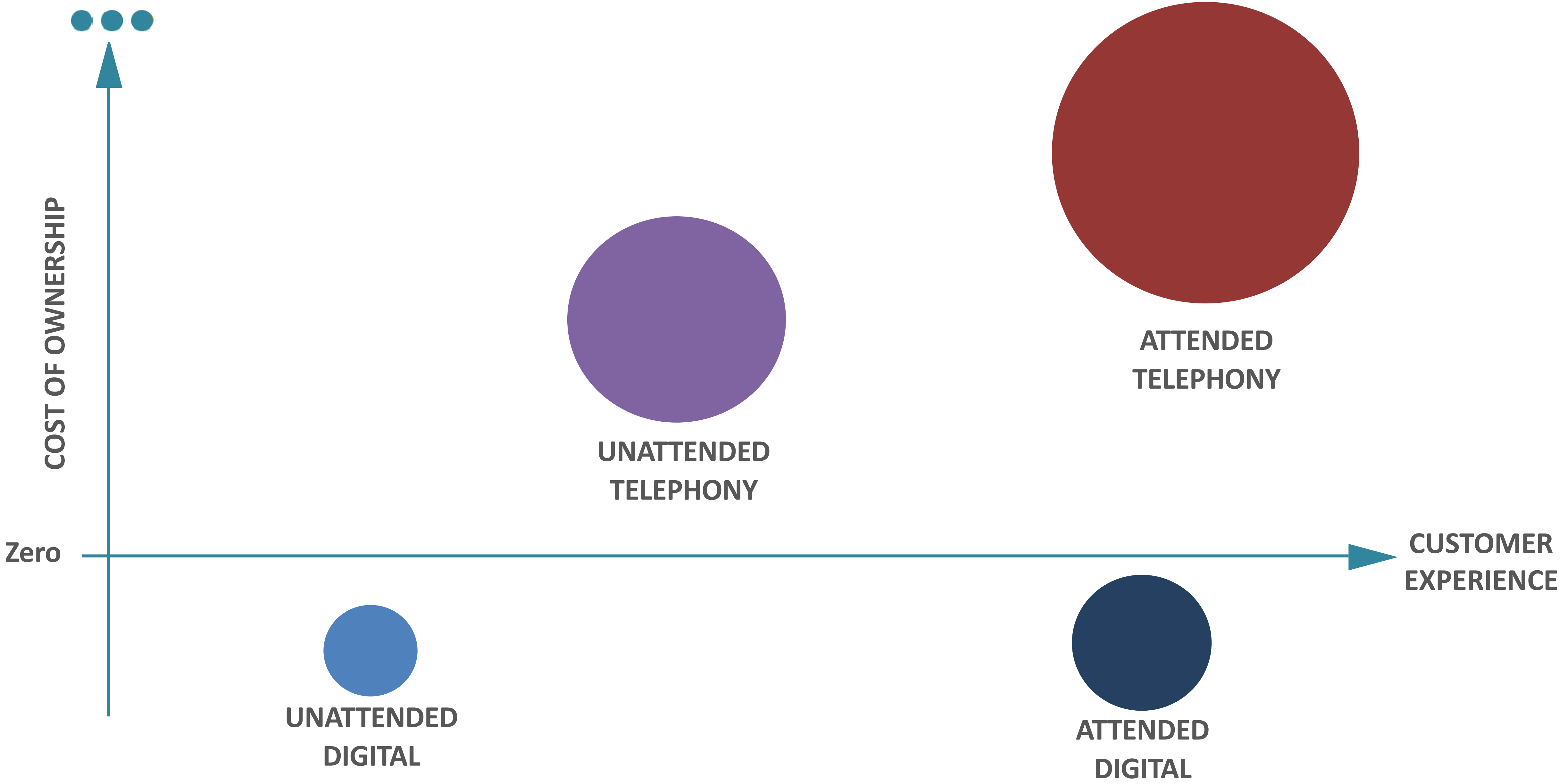
Cost and time:

What are the cost and time constraints to maintain or deliver payments compliance certification? Has a business case been produced considering all of the elements above to get a detailed understanding of cost of maintaining payments compliance over time, say a 3 to 5 year term? Has the merchant started a detailed evaluation of their payments compliance status, what their technology options are and the work streams required to produce a business case?

Securing telephone payments - implementation



Securing telephone payments – cost of ownership



Cost comparison. Telephony ATTENDED vs. Digital ATTENDED

Scenario

- UK Insurance Company – November 2017
- Single site contact centre supported by single telephony provider with single CRM
- Spoken payment card data in telephone environment via 19,522 new card MOTO transactions per annum
- E-comm 178,435 new card transactions per annum
- Continuous cover (using tokenisation) 208,522 transactions per annum
- MOTO chargebacks @ 80 to 100 per month

Volumes and costs

- 19,522 MOTO transactions per annum (Assume £20K)
- ATV £220
- 1,200 chargebacks p.a. @ £25 (charge) + £10 internal cost
- MOTO:Ecomm Acquirer cost vector 0.3%* (66p)
- Telephone Channel ATTENDED Yr. 1. £120K (£70K + £50K*)
- Telephone Channel ATTENDED Yr. 2 onwards £50K* p.a.
- Digital Channel ATTENDED @ Yr.1 £20K (£10K* set up plus £0.50* per trans)
- Digital Channel ATTENDED @ Yr. 2 onwards £10K* p.a.

Cost vector

- Digital Channel Yr. 1 @ £20K. £100,000
- Less 0.3%* x £220 (66p) x 20,000 new transactions = £13,200* p.a.
- Less cost of chargebacks @ £42,000 p.a.

- **Cost vector between Telephone Attended and Digital Attended, based on stated MOTO activity levels (circa 20K) new card MOTO transactions per annum:**
  - Yr. 1 @ £155,200* (set up + transaction + vector + chargebacks)
  - Yr. 2 onwards @ £95,200* per annum (trans + vector + c'backs)
  - **Cost vector over 3 years @ £345,600***

** Numbers will vary by Acquirer and technology vendor*

Impact on cost. DO NOTHING vs. Digital ATTENDED

Scenario

- UK Insurance Company – November 2017
- Single site contact centre supported by single telephony provider with single CRM
- Spoken payment card data in telephone environmemnt via 19,522 new card MOTO transactions per annum
- E-comm 178,435 new card transactions per annum
- Continuous cover (using tokenisation) 208,522 transactions per annum
- MOTO chargebacks @ 80 to 100 per month

Volumes and costs

- 19,522 MOTO transactions per annum (Assume £20K)
- ATV £220
- 1,200 chargebacks p.a. @ £25 (charge) + £10 internal cost
- MOTO:Ecomm Acquirer cost vector 0.3%* (66p per transaction)
- Digital Channel ATTENDED @ Yr.1 £20K (£10K* set up plus £0.50* per trans)
- Digital Channel ATTENDED @ Yr. 2 onwards £10K* p.a.

Cost vector

- Digital Channel Yr. 1 @ minus £20,000.
- Plus 0.3%* x £220 (66p) x 20,000 new transactions = £13,200* p.a.
- Plus cost of chargebacks* @ £42,000 p.a.

- **Cost vector between DO NOTHING and Digital ATTENDED, based on stated MOTO activity levels (circa 20K) new card MOTO transactions per annum:**
  - Yr. 1 @ £35,200* (- set up + transaction + vector + chargebacks)
  - Yr. 2 onwards @ £45,200* per annum (-trans costs + vector + c'backs)
  - **Cost vector over 3 years @ £135,600***

** Numbers will vary by Acquirer and technology vendor*

Compliance3. Our credentials

- Successfully working with leading brands and their acquirers since 2012 supporting the selection and implementation of PCI DSS scope reduction technologies
- Delivering a world first for large multi channel retailer. No Card Data Environment (CDE) but still having compliant access to 150 million call recordings with card data present.
- **World leading experts in technology selection and deployment to reduce the cost, time and effort in achieving and maintaining PCI DSS compliance**
  - Background in customer contact management for large international consumer brands managing inhouse and outsourced contact centre estates and change management programmes within those
  - Technology agnostic with a detailed knowledge and deep understanding of the scope reduction technology supply chain across UK, Europe, North America and Asia
  - Supporting technology selection and deployment projects for large BPO providers and directly to merchants using a wide range of technologies to take unsecure telephone payment channels out of scope of PCI DSS
  - Lead authors of the new Secure Telephone Payment Guidelines due to be published by PCI SSC in Q2 2018

Compliance3. What we do

World leading experts in achieving and maintaining **PCI compliance** in **contact centres.**

Technology agnostic offering **advisory and delivery** services, Compliance3 helps contact centres cost-effectively **achieve and maintain** PCI compliance.

In doing so, we help **protect our clients' revenues and margins** and significantly **reduce the risk** of reputational damage and consequential revenue loss – as well as **reduce the costs** associated with **maintaining compliance**.

Compliance3. Our engagement model

Supporting your entire PCI DSS compliance journey

1. ✓ LOCATE

The tasks?

- **Step 1.** What are the possibilities?
- **Step 2.** What are the dependencies?
- **Step 3.** What needs to be done – and what are the associated work streams?

2. ✓ PREPARE

The business case?

- **Step 1.** What are the ‘business requirements’?
- **Step 2.** What is the right balance of solutions to meet the requirements?
- **Step 3.** What is the cost benefit balance and payback time?

3. ✓ PROVISION

The delivery?

- **Step 1.** PoC - defined with measurement criteria agreed
- **Step 2.** Implementation managed and internal team supported
- **Step 3.** PoC evaluation, sign off and roll out

4. ✓ MANAGE

The ongoing management?

- **Step 1.** Scope – document all payment volumes across all channels
- **Step 2.** Scope - all PCI DSS mgm’t and reporting processes
- **Step 3.** Plan and deliver PCI DSS management programme to support existing resources and reduce time, cost and effort

Thank you

John Greenwood

07767 354 354
john@compliance3.com