THIS IS THE UK

The State of Security in the Eyes of UK Consumers 2018

Contents

The trust of UK consumers regularly mirrors their spend, according to our latest research

PCI Pal conducted a consumer market research study, in November 2018, through Atomik Research. 2,002 consumers were surveyed across the UK with a household income above £20k p.a.

We wanted to uncover sentiment and behaviour changes when it comes to data security. Our findings suggest that the combination of high-profile recent breaches and the headlines devoted to new data privacy regulations such as the GDPR, combined with personal experience, have put security concerns at the forefront for UK shoppers.

While security breaches are not new, consumers' attitudes towards them seem to be changing significantly - with the vast majority of UK consumers now reporting that trust in security practices, or lack thereof, influences not just where but also how, and how much they spend.

Our full findings and commentary are included in this ebook. You'll see they seem to suggest that it's not just online threats that today worry consumers – 56% are uncomfortable sharing sensitive data such as credit card details over the phone, with 32% suggesting they would 'hang up and find an alternative method' if asked to give payment information over the phone.

This demonstrates that the burden to mitigate these concerns must be a focus for organisations and brands, particularly those operating a contact centre taking payments via telephone.

If our research findings pose any questions we haven't answered in the ebook or you'd simply like to discuss your specific requirements in more detail, please get in touch.

GET IN TOUCH

U.K. +44 207 030 3770

U.S. +1 866 645 2903

info@pcipal.com

1 Cornhill, London, EC3V 3ND

www.pcipal.com

CHAPTER 1

A brief history of UK consumer privacy

Credit scores are becoming more important; from getting student loans and mortgages to renting a home or obtaining a mobile phone contract, anyone with a bad credit score faces challenges.

Of course, bad financial decisions can also damage credit scores, such as paying bills late or generating too much debt, however security breaches also have the potential to cause damage should an individual's data get into the wrong hands.

In today's modern world, sadly it is rare for a week to pass without a significant data breach being reported in the media. Organisations across all industry sectors have security as a key priority around the boardroom table, as they continue to maintain systems that will secure their data from the ever growing threat of hackers.

Of course, with the EU's General Data Protection Regulation (GDPR) being enforced, it has heightened organisations' overall focus on data protection practices, yet high-profile breaches (and attempted hacks) are still happening.

Having said that, the recent stream of security breaches has started to impact consumer sentiment around data privacy; from British Airways, Ticketmaster and Vision Direct breaches to Facebook's behaviour with Cambridge Analytica, the effect has been that consumers have become increasingly concerned about their personal data. In response they are demanding that brands better protect their data, and threatening to take spend and loyalty elsewhere if they feel security is at risk of being compromised.

"The effect has been that consumers have become increasingly concerned about their personal data."

CHAPTER 2

Consumers are feeling concerned

To get an accurate temperature check on sentiment around security, we embarked on a 2,002-person study to understand just how consumers are reacting in light of the never-ending parade of security breach headlines.

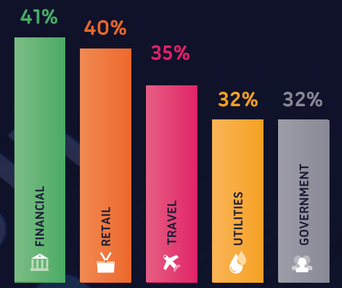
38%
OF CONSUMERS
in the UK have reported being a victim of a security breach or hack

With 38% of UK consumers reporting being a victim of a security breach or hack, it was no surprise that the research also showed a significant change in how consumers are thinking and behaving when it comes to data security.

In fact, the vast majority expressed concern when sharing personal data with brands both on and offline. Our research found that only 9% of consumers think there is no problem with data security practices. Businesses need to understand this change in perception, its potential impact on their brands, and address it head on or run the risk of losing valuable revenue.

This concern especially applies to financial services, retail and travel industries, as consumers reported trusting those companies the least with their personal data, at 41%, 40% and 35%, respectively. The finding isn't necessarily surprising with even global brands in these sectors being breached, and the numerous reports of credit card data being stolen from big name retailers such as Dixons Carphone and Under Armour.

What industries do you think are the least secure?



Brands in these high-target categories need to take extra measures to ensure their data is safe, and communicate the security investments made to consumers to restore faith in their industry.

It's not only certain verticals or types of companies that alarm consumers, it's also how brands are obtaining their personal information. Over half (55%) of consumers feel troubled when reading their credit card information over the phone, which is a real concern for contact centre businesses who are facilitating transactions in this way.

Speaking the words out loud allows anyone on either side of the phone call to obtain the sensitive information, so it's understandable that this worries consumers.

Another warning for businesses is that 44% of consumers are only comfortable sharing information over the phone to select companies that they either trust or have verified their security measures. Businesses can best solve this issue by making their security efforts known to consumers, ensuring clients that their information is safe while protecting not only the brand's reputation but also its bottom line.

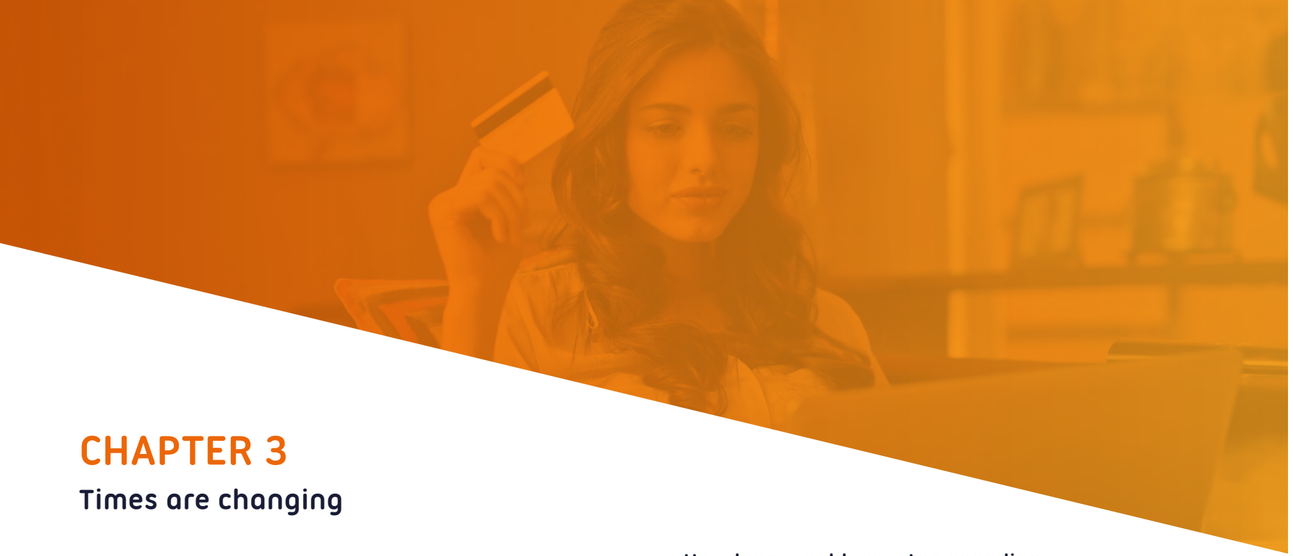
From an age group perspective, there is a marked difference in how differing ages view local versus national companies when it comes to trust, with 69% of the 18-34s preferring to trust local companies with their personal information, conversely 56% of those aged 45-65 were more likely to trust national companies.

So what would make consumers feel better?

Six out of ten consumers (59%) want companies to undergo regular security audits and put in place verification systems; a further 58% suggested that full disclosure of their security compliance and audits would make them feel more secure.

The solution for contact centres is to invest in technology that prevents customers from having to say their private information out loud. Not only will this reassure increasingly skittish consumers, but it will also ensure the business is compliant.

55%
OF CONSUMERS
feel troubled reading card details over the phone



CHAPTER 3

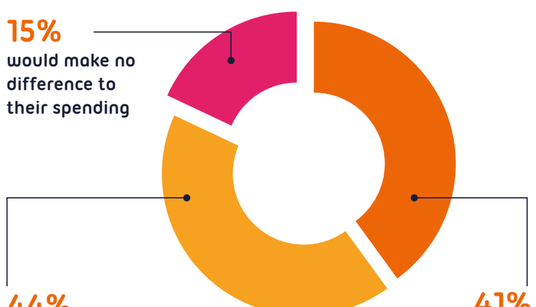
Times are changing

Changes in consumer perception are beginning to play a role in the way individuals engage and spend with brands. 85% of consumers have changed their spending habits with brands who have been the subject of a security breach or hack.

22% of consumers ask companies directly how security is handled, or conduct their own research before trusting a company with their information. Almost half (49%) are regretful of not better vetting security practices, and intend to do so in the future. Consumers are growing increasingly uncomfortable with how businesses are managing data and presenting those security efforts- they need to know more.

But what does this all actually mean for the company's bottom line? On top of facing massive fines (GDPR lays out up to £17.6m or four percent of annual global turnover, whichever is highest), our research found that a significant 41% of UK consumers said they would stop spending with a brand forever, while a further 44% said they would stop spending for at least a few months in the aftermath of a security breach.

How long would you stop spending with a brand after a data breach?



85%
OF CONSUMERS
have changed their spending habits with brands who have been breached or hacked

For any consumer facing business, these findings should serve as a clear, loud, and grave warning to ensure that they are implementing online and voice payment security measures, or face potentially disastrous long-lasting revenue and reputation consequences.

This applies to contact centres which often serve as the front line when dealing with questions about security, and managing phone payments. The finding highlights the importance of not just having a thorough security process in place, but also of training customer service employees to answer these questions.

Managers must make sure employees that are consumer facing understand, and can accurately articulate the work being done to protect personal data. If they can't, brands may lose business from fearful and uncertain consumers.

The good news for businesses is that consumers can be encouraged to forgive (if not quite forget) a security lapse, but that forgiveness comes at a price. In the event of a hack, 43% of consumers want the business to admit responsibility and invest money in improving its security efforts. But for some, that isn't enough: 50% want a third party to confirm it is safe before spending with them again, and 47% go even further to require the company to announce PCI or GDPR compliance to earn back trust.

But rather than try to go back and attempt to repair trust after a breach, businesses should adequately prepare themselves for the increasing likelihood of facing a hacker. Businesses must be taking steps now to protect consumers, and therefore, their business.

They might ask, "Well where do we start?" The simplest answer is to make sure there isn't any information in the ecosystem to steal, by descoping your business from the requirements of PCI DSS.

43%
OF CONSUMERS
want the business to admit responsibility in the event of a hack

CHAPTER 4

PCI Compliance and how PCI Pal can help

Companies have spent fortunes to protect themselves from security breaches, as demonstrated by spiralling IT budgets, but there is another way to mitigate attacks: PCI DSS. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations to ensure the protection of cardholder data.

Founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc, PCI DSS is a great foundation for any company looking to reduce their own, and their customers', exposure to data breaches.

Becoming fully compliant with PCI DSS means dropping the use of compensating controls - work-arounds introduced to give organisations an alternative to security requirements that could not be met due to legitimate technological or business constraints. Research conducted by Verizon shows that the organisations that suffered a breach of security were more likely to be using compensating controls.

In the short-term, they act as the intended bandage that they are, but practically speaking, they aren't good long-term solutions for businesses, as relying on compensating controls will not prevent fraud or breaches, thus risking a business' revenue. Being fully compliant with PCI DSS takes away the bandage and stitches the problem permanently, becoming vital for the survival of businesses, both in terms of reputation and finance.

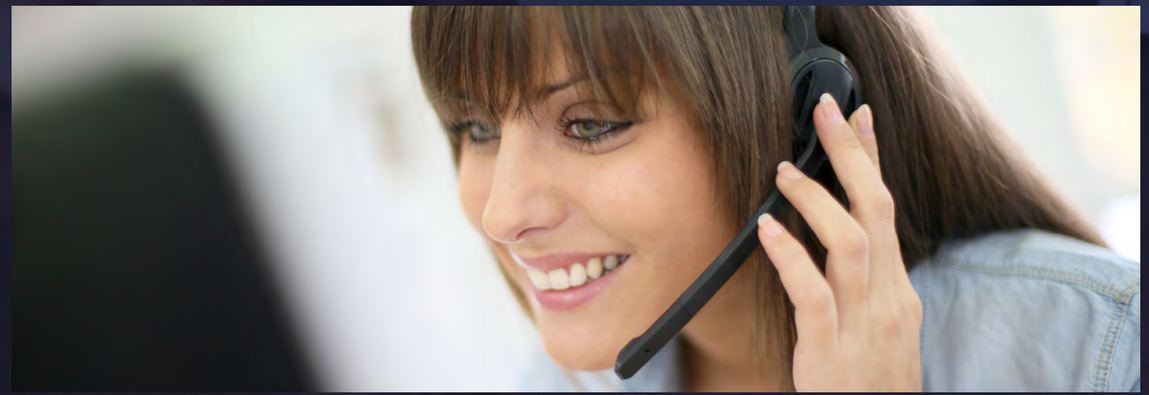
The best example that comes to mind is the storage of data in systems. Rather than investing time and money in protecting data from would-be hackers, simply make sure there's nothing there to steal. The less customer data stored, the less risk there is of that data being stolen.

Once easier said than done, there now exists technology to help businesses descope for PCI DSS, protecting their business' bottom lines and reputation, while avoiding the use of compensating controls. Enter PCI Pal.

Our core solution to the security problem, Agent Assist, seamlessly integrates with the merchant's payment gateway via our AWS cloud infrastructure, providing companies with a solution to receive payments by phone and descope environments for PCI DSS. Even better, the solution can be deployed in a number of ways. We work with each company, and partner to understand the scope of the project and which deployment method works best for them. We have simple and proven phone and API integrations so there is no impact on business operations.

Through our experience across the contact centre space, we know that customers increasingly expect to be able to interact with brands via multiple channels. Not only do we address phone, but also SMS and web chat, as they are key components of multichannel communication and require secure mechanisms to enable customers to make PCI compliant payments.

There are various security levels for service providers. We adhere to Level 1, which is the highest level of security required by the leading card companies, and maintain compliance by adhering to the latest Payment Card Industry Data Security Standards.



IFLY CASE STUDY

Securely handled payments for peace of mind for iFLY and their customers.

iFLY is the leisure company that created modern indoor skydiving. The company started trading in 2005, having created a stable wall-to-wall cushion of air in a flight chamber, which offers a realistic and safe indoor skydiving experience. iFLY in the UK helps over 150,000 people each year to experience the thrill of Indoor Skydiving across three sites in the UK; Basingstoke, Milton Keynes and Manchester. There are a total of 69 locations worldwide, with centres in the US, Canada, Europe and Asia, with more sites to follow as demand continues to grow.

The Compliance Challenge

iFLY takes its customer services seriously, in order to provide a consistent quality of service to every customer. The team of eight customer services agents handle upward of 97,000 inbound calls every year, and this number is increasing.

With every call being recorded for training and monitoring purposes, the management was aware that it needed to change the way payment card transactions were being manually handled over the phone to comply with the Payment Card Industry Data Security Standard (PCI DSS).

Explains Alyson Williams, Finance Manager – Group for iFLY: “One of our challenges was to ensure we became PCI DSS compliant. At the time, we were manually capturing and inputting card details to our system, without pausing the call recording, and we knew this had to change.”

“Regulation got us focused: failure to comply would create financial penalties across the entire business, which would be significant.”

“We needed to identify a solution that would enable us to maintain our call recording process yet provide a safe and anonymous way for customers to provide their payment information – and importantly, without impacting the overall customer experience.”

How PCI Pal Solved iFLY’s PCI Issue

iFLY took the decision to identify a partner to manage its Customer Service Team’s payment card security and was recommended to contact the team at PCI Pal for help.

Matthew Lippert, Assistant Manager of iFLY said: “We needed to find a way of continuing to record our calls without the fear that we’d captured sensitive card data. I would complete online certificates to show compliance for our online business, and began to realise that we were no longer compliant because of the call centre. Help was needed and we were recommended by a consultant to contact PCI Pal.”

The PCI Pal Agent Assist solution enables call centre agents to securely capture payment card data using DTMF (Dual Tone Multi Frequency), while the agent maintains full conversation with the customer.

Agent Assist integrates with the call flow and, at the point of payment, intercepts the telephone keypad tones as they are entered by the customer. This means the call handler doesn’t hear or see the card data, yet the customer and agent can still have a conversation throughout the process but the sensitive card data is prevented from reaching the agent or iFLY’s environment.

Continues Alyson: “For us, PCI Pal’s Agent Assist was a sensible solution. Not only would it mean we were compliant, but it also integrates with our existing call centre systems and payment providers meaning we didn’t have to make dramatic changes to our existing working processes.”

“There was no re-engineering of our call handling or system upgrades. Instead, we’ve been able to integrate Agent Assist and deliver a seamless call flow for both our customers and our call handlers.”

The Results

When asked to consider the results achieved by implementing PCI Pal’s Agent Assist, Alyson is quick to respond: “When completing the annual PCI Self-Assessment Questionnaire, we’ve gone from being Certificate D, to the highest Certificate A for our PCI compliance. This gives us peace of mind that we are compliant and not living in fear of financial fine implications.”

She continues “The Agent Assist platform is easy to implement, easy to use and creates less work for the team. Taking payment card details over the phone has become more efficient and we haven’t had to make changes to the way our team operates or make any major adaptations to any of our systems.”

Feedback from customers has also been positive, as Matthew adds: “Anecdotally, customers are commenting on inputting their card details on their keypad as a positive step. It’s something people are becoming used to doing and with financial security being a priority for consumers, they are happy that we can demonstrate just how secure our systems are.”

“We are really pleased with how Agent Assist is today supporting us. The solution is extremely effective, the team has been brilliant in supporting us deliver this project and we now have a very stable solution that enables us to take card details in a compliant way, while continuing to record our calls.”

Matthew Lippert, Assistant Manager, iFLY

CHAPTER 5

Tipping the balance, safeguarding trust

There's no doubt that this shift in consumer sentiment should be concerning for businesses, especially financial and retail organisations. Hacks are at an all-time high, and trust is at an all-time low, meaning that their revenues are at risk. Businesses need to make moves now to protect their reputation, revenue, and customers.

If you're hacked, say goodbye to sales revenue and your brand reputation

Arguably the most alarming finding in our research was that businesses stand to lose 41% of their sales revenue forever if they are hacked. That doesn't include the fines from the government, lawsuits, or any other potential negative outcome from a breach.

The damage sustained by your brand's reputation could impact your ability to acquire new customers for years to come, but there are steps that a business can take to salvage and assure consumers that their data is safe again.

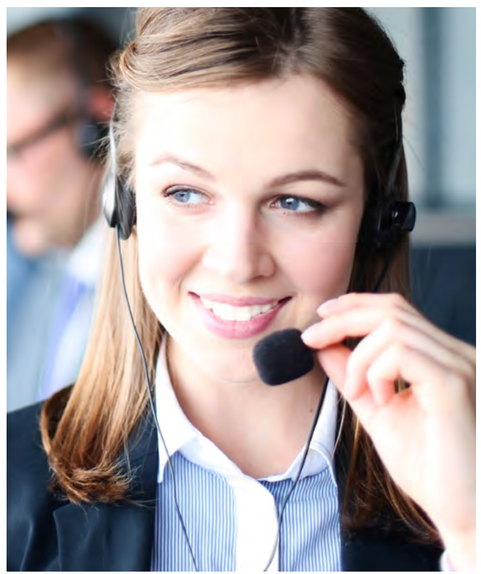
As mentioned before, the simplest answer to this is to make sure there isn't any information to steal - by descoping your business from PCI DSS.

Invest in technology

We're specifically talking about PCI DSS technology. Achieving PCI compliance is the perfect starting point for any company looking to reduce their own, and their customers', exposure to data breaches.

Technology such as PCI Pal's Agent Assist exists to help businesses descope from PCI DSS, ensuring that valuable, hacker-attracting data doesn't cross into a business' environment.

To put it another way, rather than investing time and money in a 'vault' to protect valuable data from external hackers, or even internal agents, this technology ensures that there is nothing in the vault to guard.



Own up to your mistakes, as well as your solution

We've seen the headlines over the past few years sounding alarm bells about the number of data hacks occurring each year. It happens so often that breaches no longer surprise anyone, and reinforces the distrust of companies. Consumers across the board want to see businesses not only investing in technology, but also be able to tell consumers about it in layman's terms when asked.

Transparency is going to be key for earning, keeping, and potentially having to rebuild consumer trust.

CHAPTER 6

Your Annual PCI Checklist

If you operate a contact centre that takes card payments from customers over the phone or via SMS and web chat, there are certain checks you must perform to ensure the security of cardholder data.

The Payment Card Industry Data Security Standard (PCI DSS) is the information security standard for organisations that handle card payments from the major card schemes, including Visa, MasterCard, American Express, Discovery and JCB.

To remain compliant, the following checks must be performed annually to maintain security and mitigate the risks of a compromise of card or personal data. It's worth noting that if you're using a hosted solution like PCI Pal then most of the PCI DSS requirements will already be met.

Although the Payment Card Industry Security Standards Council (PCI SSC) sets the security standards, each card provider also has its own programme for compliance, validation levels and enforcement.

Compliance is not enforced by the PCI SSC however, but rather by the individual card issuer or acquiring banks.

You can find more information about compliance for each card scheme from the following links:

- American Express – americanexpress.com/datasecurity
- Discover Financial Services –
- discovernetwork.com/fraudsecurity/disc.html
- JCB International – jcbeurope.eu/business_partners/security/pcidss.html
- MasterCard Worldwide – mastercard.com/sdp
- Visa Inc – visa.com/cisp
- Visa Europe – visaeurope.com/ais

What is the PCI Compliance 3-Step Process?

There are three continuous steps that should be carried out to ensure PCI DSS requirements are met:

1. Assess – You must identify cardholder data and take an inventory of your IT assets and business processes for payment card processing, then assess them for vulnerabilities that could lead to a compromise of cardholder data.

2. Remediate – You must fix any vulnerabilities and not store any cardholder data that you do not need.

3. Report – The final step is to compile and submit compliance reports to the banks and card schemes you do business with, along with any remediation validation records if applicable.

Which PCI Standards Do I Need to Maintain?

Your merchant level dictates the standards you will need to maintain for PCI DSS compliance. There are four levels of merchant based on the number of transactions you process every year. This dictates whether you need an annual security assessment carried out by a PCI SSC-accredited qualified security assessor (QSA), or if you can complete a self-assessment questionnaire (SAQ).

What Annual Checks Should I Perform in My Contact Centre?

Regardless of the assessment method required, the following steps must be taken each year:

- Complete an annual risk assessment
- Ensure third parties that store, process and/or transmit card data have maintained their PCI DSS compliance and are still registered with the card schemes
- If you are using a third party application in your contact centre, make sure the product and particular version you are using is Payment Application Data Security Standard (PA DSS) compliant
- If you use an integrator to bring the products together, make sure they are certified to the required standard to do so.
- Train your staff to follow PCI DSS procedures
- Make sure you only store data that is essential and that it is encrypted and/or masked
- Protect your data network and make sure you are using a firewall and up-to-date anti-virus software
- Perform network scans on a quarterly basis. These have to be performed by an approved scanning vendor (ASV)
- You should also discuss security with your web hosting provider to ensure they have secured their systems appropriately. Web and database servers should also be hardened to disable default settings and unnecessary services
- Annual pin entry device (PED) tests need to be run to identify any vulnerability
- Any software or hardware you use to process transactions should have approval from the Payment Card Industry Security Standards Council (PCI SSC)

Reduce Your PCI Compliance Concerns

If this all sounds like a lot to deal with, you might like to consider partnering with a hosted PCI solution provider. Our smart PCI solutions, like Agent Assist, can be seamlessly integrated with your contact centre operation to ensure compliance without compromising the customer experience.

CHAPTER 7

A PCI Glossary

Acquirer – The financial institution that processes your payment card transactions.

Agent Assist – A secure, PCI DSS compliant solution that uses DTMF masking to disguise a customer's key tones when a contact centre agent takes a payment over the phone.

AOC – Attestation of Compliance – a form that allows you to attest to your PCI DSS assessment results.

Audit Trail – A sequential log of your system activities.

CDE – Cardholder Data Environment – The entire environment (personnel, software, and hardware) in which data is stored, processed, and/or transmitted.

Console/Non-console Access – Direct or indirect access to a mainframe, server, or system.

CVSS – Common Vulnerability Scoring System – A method of ranking the seriousness of system vulnerabilities.

Data-flow Diagram – A comprehensive diagram documenting the flow of sensitive data through your system or network.

DESV – Designated Entities Supplemental Validation – An extra level of security validation required by some payment brands or acquirers.

DPA – Data Protection Act – the Act and relevant legislation regarding data security in the UK.

DTMF – Dual-Tone Multi-Frequency signalling – the system that recognises and processes the key tones on your phone.

DTMF Masking – Disguises the key tones as a contact centre agent takes a payment over the phone by masking them with a monotone beep so that the agent has no way of accessing card information.

De-scope – To remove your contact centre from the scope of PCI DSS entirely by using a third party service provider to process, transmit and/or store all card data.

DoS – A denial-of-service attack in which a hacker disables a system by overloading it with requests.

E2E – End-to-End Encryption. An encryption solution that does not meet P2PE standards.

GDPR – General Data Protection Regulation – The EU's new standard for data security.

ICO – The Information Commissioner's Office – the UK's data protection regulator.

IDS – Intrusion detection system.

IPS – Intrusion prevention system.

IVR – Interactive Voice Response – An automated system that allows a computer to recognise and process speech and DTMF tones.

Multi-factor Authentication – The requirement of two or more levels of authentication to gain access to sensitive data or systems.

OS – Operating system.

P2PE – Point-to-Point Encryption – A standard of encryption for the secure transmission of data from the POI to processing.

PCI DSS – Just testing!

PCI SSC – The PCI Security Standards Council.

PFI – PCI Forensic Investigator – The person who investigates system breaches to analyse when, how, and why they occurred.

POI – Point of Interaction – The point at which cardholder data is taken.

QSA – Qualified Security Assessor – A PCI SSC-qualified PCI DSS assessor.

ROC – Report on Compliance – The report made after a PCI DSS assessment.

SAQ – Self-Assessment Questionnaire – the self-assessment section of a PCI DSS assessment.

Service Provider – A third-party organisation that provides cardholder data processing, storage, or transmission services.

Tokenisation – The use of tokens to represent sensitive data so that data is never accessible by the merchant.

Please let us know if there are any other PCI terms you regularly come across, but don't understand. We'll give you a full explanation and will add them to our PCI glossary!

Thank you

We hope you found this eBook useful. If you have any further questions about PCI compliance or would like to find out more about PCI Pal, please visit our website or get in touch with our expert consultants today.

GET IN TOUCH

U.K. **+44 207 030 3770**

U.S. **+1 866 645 2903**

info@pcipal.com

1 Cornhill, London, EC3V 3ND

www.pcipal.com

Award winning secure payment technology

Award winning secure payment technology

www.pcipal.com