PCIpal ®

This is the World*

The State of Security in
the Eyes of Consumers

*United States, United Kingdom, Australia, Canada

Contents

The trust of consumers regularly mirrors their spending and loyalty, according to our latest research:

To get an accurate temperature check on sentiment and behavior changes when it comes to data security from a global perspective, PCI Pal conducted market research in the United States via AYTM, the United Kingdom via Atomik Research, Australia via YouGov and Canada via Environics Research. In each region, at least 2,000 consumers were surveyed to glean insights into the sentiment around the onslaught of data security breaches and hacks.

Our findings suggest that a combination of recent high-profile breaches, headlines devoted to new and upcoming consumer data privacy regulations around the world, and personal experience have put security concerns at the forefront for global consumers.

As the rate of security breaches continues to grow, consumer attitudes in the US, UK, Australia and Canada seem to be changing significantly - with a vast majority of consumers now reporting that trust in security practices, or lack thereof, influences not just where they shop, but also how, and how much they spend.

The findings suggest that it's not just online threats that consumers are concerned about. There's a growing number of respondents refusing to conduct financial transactions on the phone and reporting that they are uncomfortable sharing sensitive data such as credit card information over the phone. This demonstrates the importance for organizations to mitigate these concerns, particularly for those operating contact centers that take payments over the phone.

Our full findings and commentary are included in this e-book. If our research findings pose any questions we haven't answered in the e-book or you'd simply like to discuss your specific requirements in more detail, please get in touch.

GET IN TOUCH

U.S. +1 866 645 2903

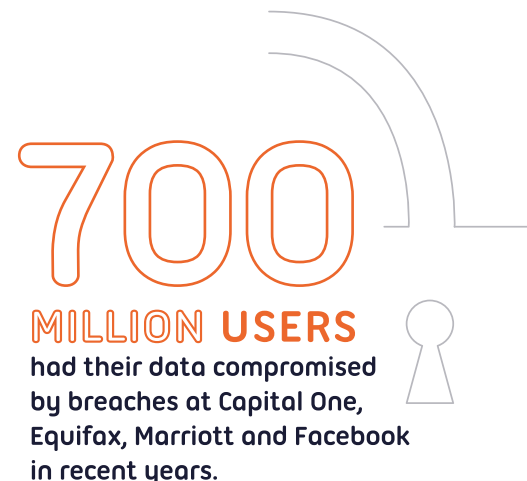U.K. +44 207 030 3770

AUS 02 7202 0294

info@pcipal.com

www.pcipal.com

CHAPTER 1

A brief history of global consumer data privacy

Businesses and consumers around the world are migrating their presence online, and consequentially, cybercriminals have taken notice of the wealth of information that has been uploaded for their taking. Financial data, contact information, medical data, social security numbers and other forms of highly personal data are stored in corporate networks and databases that are hosted in public, private and hybrid cloud environments. As this data rapidly accumulates, sophisticated hackers have refined their tactics to bypass security protections and gain access to restricted data that they can then sell on the dark web.

There are many assorted laws and regulations in place to protect consumer data privacy: the PCI Data Security Standard, the California Consumer Privacy Act, Europe's General Data Protection Regulation, Canada's Personal Information Protection and Electronic Documents Act, Australia's

700 MILLION USERS had their data compromised by breaches at Capital One, Equifax, Marriott and Facebook in recent years.

Consumer Data Right and other legislation currently in the works. But from a global perspective, amid this myriad of laws, data privacy regulations are fragmented and in need of standardization.

This is evidenced by the growing rate and sophistication of data security breaches on a global scale, including:

- Data breaches at Capital One, Equifax, Marriott and Facebook, which compromised the data of more than 700 million users.
- The British Airways breach which reportedly affected 500,000 customers.
- The Westpac breach that exposed the personal data of nearly 100,000 Australians.
- The hack of Canada's two largest banks, Bank of Montreal and the Canadian Imperial Bank of Commerce's Simplii Financial, which resulted in the theft of 90,000 customers' data.

As a result of the influx in data breaches, more consumers are aware that they are in no way safe, especially as more people are forced to resolve the short and long term damages caused by an organization's weak data privacy practices. A security breach resulting in identity theft that severely damages a victim's credit score in the long term. In response, consumers across the globe are putting security front and center and holding businesses accountable for the frivolous management of data.

CHAPTER 2

## Today's consumers care about data security and privacy

Based on the findings of the reports, consumers are rightfully concerned with security threats. 44% of Americans, 38% of Brits, 33% of Australians and 37% of Canadians claim to be victims of a security breach. Unsurprisingly, the research also showed a significant change in how consumers around the world are thinking about and reacting to bad security hygiene.

The vast majority of Americans, Brits, Australians and Canadians now express concern when sharing personal data with organizations both on and offline, and only 3% (US), 9% (UK), 6% (Australia) and 15% (Canada) of consumers imagine there to be no problem with data security practices in their respective regions.
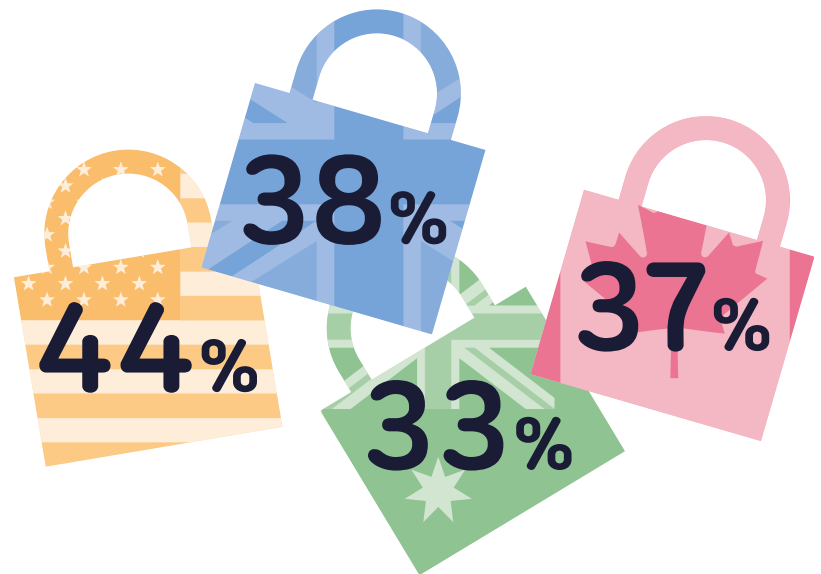
38%

37%

44%

33%

44% of Americans, 38% of Brits, 33% of Australians and 37% of Canadians claim to be victims of a security breach.

RETAIL

19%
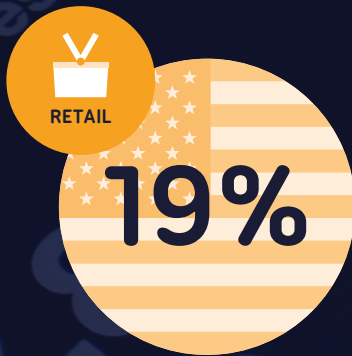
19% of Americans rated retail as the least trustworthy industry.

FINANCIAL

41%
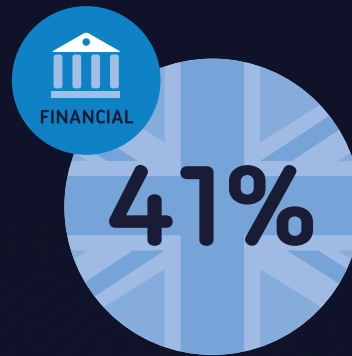
41% of Britons rated financial services as the least trustworthy industry.

RETAIL

50%

50% of Australians rated retail as the least trustworthy industry.

RETAIL

65%

65% of Canadians rated retail as the least trustworthy industry.

Global businesses need to understand this drastic change in perception and address it head on, or risk losing valuable revenue.

The research found that consumers were particularly wary of certain industries:

- US consumers rated the retail and travel industries worst, at 19% and 16.4% trust respectively.
- UK consumers rated the financial services, retail and travel industries worst, at 41%, 40% and 35% trust respectively.
- Australian consumers rated the retail, travel and financial services industries worst, at 50%, 40% and 36% trust respectively.
- Canadian consumers rated the retail and travel industries worst, at 65% and 41% trust respectively.

Across the board, consumers trusted the retail and travel industries least. These findings aren't necessarily surprising if we consider the global brands that have been breached, and the numerous reports of credit card data that have been stolen from big name retailers, such as Macy's, Lord & Taylor and Under Armour.

Businesses 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 an organization obtains consumer data. Consumers in every region expressed concerns about having to read their credit card information over the phone, and many are only comfortable sharing information over the phone with certain companies that they trust. Here are the figures for each region, respectively:

- In the US, over 40% of Americans are uncomfortable reading their credit card information over the phone and 58% of consumers are only comfortable sharing information over the phone to select companies that have earned their explicit trust
- In the UK, 55% and 44%
- In Australia, 49% and 43%
- In Canada, 42% and 58%

Speaking sensitive personal details out loud allows anyone on either side of the phone call to obtain your information, so it's understandable that this worries consumers. Businesses can ameliorate 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 it's bottom line.

Speaking sensitive personal details out loud allows anyone on either side of the phone call to obtain your information.

OVER 40%

OF AMERICANS
are uncomfortable reading credit card information by phone

55%

OF UK CUSTOMERS
are uncomfortable reading credit card information by phone

49%

OF AUSTRALIANS
are uncomfortable reading credit card information by phone

59%

OF UK CUSTOMERS

would prefer companies to undergo regular security audits

57%

OF AUSTRALIANS

would like companies to undergo regular security audits

62%

OF CANADIANS

would feel more comfortable if companies underwent regular audits

So what would make consumers feel better about data security in general? Responses varied only slightly throughout regions:

- In the US, almost half of consumers would feel more comfortable if companies underwent regular security audits and put in place verification systems; another third would feel safer if Social Security Numbers (SSNs) were not required for transactions, especially after the Equifax hack. Almost a quarter of consumers would feel safer if businesses were federally mandated to protect consumer data, hence the creation of GDPR-like laws.

- In the UK, six out of ten consumers (59%) would prefer companies to undergo regular security audits and put in place verification systems; 58% suggested that full disclosure of a company's security compliance and audits would make them feel more secure.

- In Australia, 57% would like companies to undergo regular security audits; another half would feel safer if sensitive personal information was not required for transactions; and 49% would prefer that businesses are federally mandated by stricter regulation around consumer data protection.

- In Canada, 62% would feel more comfortable if companies underwent regular security audits; another half would feel safer if sensitive personal information was not required for transactions; and 49% would prefer that businesses are federally mandated by stricter regulation around consumer data protection.

The best solution for any organization operating call centers 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 with current and future regulatory requirements.

CHAPTER 3

Consumers are taking a stand and holding organizations accountable

The changes in consumer perception have transformed the way that people engage and spend their money with businesses. The regional breakdowns below demonstrate that consumers are increasingly uncomfortable with the corporate management of consumer data. These findings provide insight into how consumers' perceptions about a company affect their spending behaviors and the lengths they will go to protect themselves:

- In the US, almost 80% of consumers claim they will change their spending habits based on their trust in a brand's security, and a whopping 89% of consumers no longer trust that their information is safe with companies. That 89% has begun pressing businesses on their security practices in order to assess where they should spend their money.

- 28% of US consumers ask companies directly how security is handled or conduct their own research before trusting a company with their information. 62% are regretful of not vetting security practices better, and intend to do so in the future.

80%

OF CUSTOMERS

in the US claim they will change their spending habits based on their trust in a brand's security

- In the UK, 85% of consumers claim they will change their spending habits with brands that have been the subject of a security breach or hack.
- 22% of UK 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 vetting security practices better, and intend to do so in the future.
- In Australia, 74% of consumers claim they will change their spending habits based on their trust in a brand's security. More specifically, 36% say that they would spend more with a trusted and secure brand, 24% say they would stop spending with a brand they believe has insecure data practices and 14% say they would spend less with a brand they believe has insecure data practices.
- 23% of Australian consumers ask companies directly about their security practices or do their own research, and 58% report regretting not vetting a company's security practices better before shopping with a company.
- In Canada, 65% of consumers claim they will change their spending habits based on their trust in a brand's security. More specifically, 30% say that they would spend more with a trusted and secure brand, 21% say they would stop spending with a brand they believe has insecure data practices and 14% say they would spend less with a brand they believe has insecure data practices.
- 24% of Canadian consumers ask a company directly about their security practices or do their own research, and 61% report regretting not vetting a company's security practices better before shopping with them.

But what does this all mean for the bottom line of organizations worldwide? On top of facing massive fines that vary by region (In Europe, GDPR lays out up to four percent of annual global turnover), the research found that consumers around the globe are fundamentally reassessing their relationships with companies that have been breached.

- In the US, 83% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and over a fifth (21%) of consumers claim they will never return to a business post-breach.
- In the UK, 44% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and 41% of consumers claim they will never return to a business post-breach.
- In Australia, 43% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and 43% of consumers claim they will never return to a business post-breach.
- In Canada, 58% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and a fifth of consumers claim they will never return to a business post-breach.

83%
OF US CONSUMERS
claim they will stop spending with a business for several months in the immediate aftermath of a security breach

41%
OF UK CUSTOMERS
claim they will never return to a business post-breach

For any business engaging with consumers, these findings are clear, loud and grave warnings to ensure that they implement online and voice payment security measures, or face potentially disastrous long-lasting revenue and reputational consequences.

This applies to call centers which often serve as the front line for consumers dealing with questions about security. The findings highlight the importance of not just having a thorough security process in place, but also of training customer service employees to answer questions about a company's security practices. Managers must make sure consumer-facing employees understand, and can accurately share the company's ongoing initiatives around securing customer 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 forget) a security lapse, but that forgiveness comes at a price. The regional breakdown is as follows:

- In the US, if a company is hacked, 41% of consumers want the business to admit responsibility and invest money in improving its security efforts, 26% want a third party to confirm its ecosystem is safe before spending with them again and 21% go even further to require the company to announce PCI Compliance to earn back trust. In total, 88% of consumers require businesses to make additional investments in their security after they are hacked.

- In the UK, if a company is hacked, 43% of consumers want the business to admit responsibility and invest money in improving its security efforts, 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.

- In Australia, if a company is hacked, 44% of consumers want the business to admit responsibility and invest money in improving its security efforts, 37% want a third party to confirm the company's system is safe and another 37% want the company to announce security compliance to earn back their trust.

- In Canada, if a company is hacked, 33% of consumers want the business to admit responsibility and invest money in improving its security efforts, 26% want a third party to confirm the company's system is safe and another 28% want the company to announce security compliance to earn back their trust.

Businesses should view repairing trust after a breach a last resort. Instead, they should adequately prepare themselves for the increasing likelihood that one will inevitably occur. That means companies must take steps now to protect consumers. The first step is to make is to make sure there isn't any sensitive information stored in the company's ecosystem to steal by descoping the business from the requirements of PCI DSS.

44%
OF AUSTRALIANS
want the businesses to admit responsibility and invest money in improving security

26%
OF CANADIANS
want a third party to confirm the company's system is safe after a hack

CHAPTER 4

PCI Compliance and how PCI Pal can help brave the security storm successfully

Companies have spent fortunes to protect themselves from security breaches, as demonstrated by spiraling 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 organizations 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 fantastic starting point 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 meant to give organizations an alternative to security requirements that could not be met due to legitimate technological or business constraints). Research conducted by Verizon showed that organizations 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 effective

long-term fraud prevention solutions for businesses looking to combat cyber criminals. Being fully compliant with PCI DSS takes away the bandage and stitches the problem permanently, becoming vital for the survival of businesses around the world, both in terms of reputation and finance.
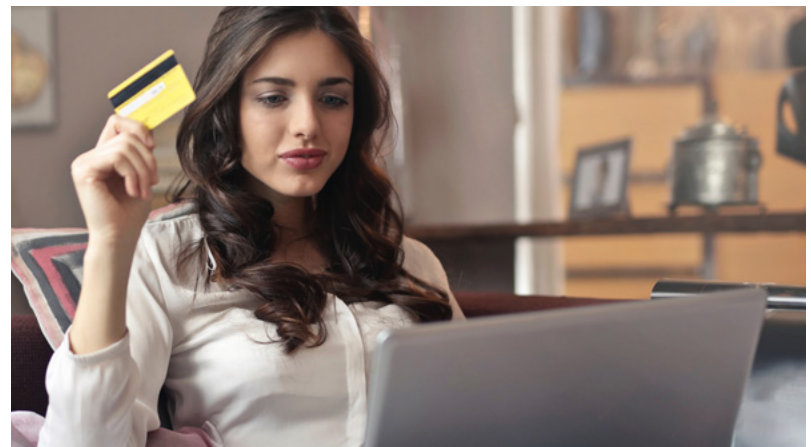
The best example that comes to mind is the storage of data in systems. Rather than investing time and money in protecting data from would-be hackers, simply make sure there's nothing there to steal. The less customer data stored, the less risk there is of that data being stolen.

Once easier said than done, there now exists technology to help businesses descope from the requirements of 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 the network environments from the requirements of 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. Our products typically result in a 20-30 second reduction in average call handling time which provides savings and operational efficiencies to our customers.

Through our experience across the contact center 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 omnichannel 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.

"*Once easier said than done, there now exists technology to help businesses descope for PCI DSS, protecting their business' bottom lines and reputation.*"

ALLSAINTS CASE STUDY

Find out how this global fashion brand is using PCI Pal to ensure compliance

AllSaints is a global fashion brand based in East London, which operates in twenty-seven countries, with over two hundred stores globally.

AllSaints' Compliance Challenge

The AllSaints customer experience team were facing a number of problems in creating a seamless customer journey. Time-consuming for both agent and customer, AllSaints needed to join up their various systems and provide a payment solution that would be smooth and painless for both parties.

AllSaints' customers are typically quite tech savvy, with an "on the go" lifestyle, so they needed a convenient secure payment solution that would make customers feel comfortable and confident when placing phone orders.

How PCI Pal Solved AllSaints' PCI Problem

AllSaints is a 24/7 digital business operating on a number of different

platforms in a multi-lingual environment, so we needed to create a flexible, robust and reliable solution that would tick all the boxes in terms of legislation, accessibility and best practice.

There was also an education requirement, so our expert consultants took the time to advise AllSaints' contact center agents on how to make and process PCI Compliant payments, and how to protect customer details across the various customer experience touchpoints.
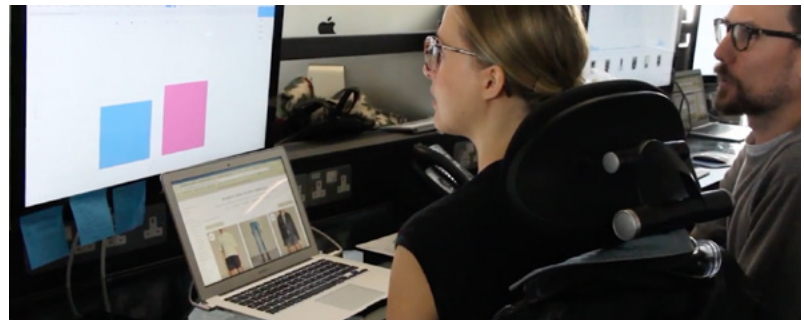
We worked in close partnership with the customer experience team to iron out any potential issues and were able to deliver the project on time and within budget.

The Result

Since implementing a PCI Pal solution, AllSaints has seen a two-thirds reduction in how long it takes to process a phone sale, which means they handle more calls and take better care of their customers. The new secure payment solution was certainly put to the test over their peak Black Friday and Christmas periods!

Customers can now shop with confidence, safe in the knowledge that their cardholder data and personal details are secure. An improved telephone order system also means customers can call the AllSaints team at any time if they're having difficulty placing an online order, or if they'd simply like agent support with a transaction.

"The PCI Pal team are very proactive and easy to get hold of. They've always gone out of their way to adapt their solutions as our business needs have evolved. We would certainly recommend PCI Pal, not only are they digital, safe and secure, but they're also very forward-thinking, so great for any retail e-commerce business."

Heather Gibson, Brand Experience Director, AllSaints

CHAPTER 5

Rebuilding trust and reputation in the aftermath of a breach

There's no doubt that this shift in consumer sentiment should be concerning for businesses, especially retailers and travel-related organizations. Hacks are at an all-time high, and trust is at an all-time low, meaning business revenue is at risk. Therefore, 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 the research is that businesses across regions stand to lose a significant portion 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 company's reputation could impact the 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.

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

Invest in technology

We're specifically talking about PCI DSS technology. Adhering to 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 exists to help businesses descope from the requirement of PCI DSS, ensuring that valuable, hacker-attracting data doesn't cross into a business' ecosystem. 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.

Methodology & market research

To uncover changing consumer sentiment and behaviors around data security from a global perspective in the last year, PCI Pal conducted market research in key markets, including the United States, the United Kingdom, Australia and Canada:

- 2,000 US consumers with a household income above $25K were surveyed via AYTM
- 2,002 UK consumers with a household income above £20K were surveyed via Atomik Research
- 2,000 Australian consumers with a household income between $35-$700K AUD were surveyed via YouGov (in partnership with Natterbox)
- 2,000 Canadian consumers with a household income between $30K-$650K CAD were surveyed via Environics Research

CHAPTER 6
Your Annual PCI Checklist

If you operate a contact center 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 organizations 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 Center?

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 center, 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 center 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 center 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 recognizes and processes the key tones on your phone.

DTMF Masking – Disguises the key tones as a contact center 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 center 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 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 recognize 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 organization that provides cardholder data processing, storage, or transmission services.

Tokenization – 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.S. **+1 866 645 2903**

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

AUS **02 7202 0294**

info@pcipal.com

www.pcipal.com

Award winning secure
payment technology

Safeguarding reputations and trust