THIS IS AMERICA

The State of Security in the Eyes of U.S. Consumers 2018

Contents

US consumers increasingly put their money where their trust is, according to our latest research

Earlier this year PCI Pal conducted market research, through AYTM, surveying 2,000 consumers across the United States with a household income above $25k. We wanted to uncover sentiment and behavior 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 and California Privacy Law, and personal experience have put security concerns front and center for American shoppers.

While security breaches are not new, US consumers' attitudes towards them seem to be changing significantly - with the vast majority of Americans 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 the findings seem to suggest that it's not just online threats that worry consumers - 28% question how their data is being recorded when on the phone and almost half (42%) are uncomfortable sharing sensitive data such as credit card details over the phone. Given that 66% of all call centers are based in The Americas, the burden of security provisions to mitigate these concerns, must be a focus for organizations and brands that rely on telephone customer service practices.

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.S. +1 866 645 2903

U.K. +44 207 030 3770

info@pcipal.com

615 South College Street, Charlotte, NC 28202, USA

www.pcipal.com

CHAPTER 1

A history of U.S consumer privacy

In the past, U.S. consumers tended to look away or forgive brands in the aftermath of a breach. Why? Because U.S. banks have taken responsibility for stolen card information and refunded consumers if money in their accounts was missing. This meant that many Americans weren't thinking about where their credit card data was going.

We all know that credit scores are key to living comfortably in the United States. From getting student loans and mortgages to renting a home or obtaining a cell phone contract, an adult with a bad credit score loses their ability to live as they desire. Americans can damage their credit themselves by making bad financial choices such as paying bills late or collecting too much debt, but low credit scores aren't always because of delinquent behavior; security breaches can also cause damage when an individual's PII gets into the wrong hands.

One of the results of last year's massive Equifax hack is that those responsible potentially now have access to personal, private data and consequently, their financial future. Because of lax protection laws and no consequences, the valuable information that can make or break an American's success is out there for the taking. This detail, in combination with the recent rush of security breaches, has started to impact consumer sentiment around data privacy.

This shift is not without good reason. In July, the Identity Theft Resource Center reported a staggering 668 security breaches carried out in 2018. That pace is the equivalent of around four breaches per day for every single day of the year. From Target and Home Depot breaches to Facebook's behavior 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 dollars and loyalty elsewhere if they feel their security is being compromised.

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

In an attempt to address these concerns, California passed new privacy legislation, AB 375. Similar to the E.U.’s GDPR, AB 375 brings greater transparency to the ways in which personal data is used and traded, giving previously absent strength to U.S. consumers. AB 375 specifically gives consumers the right to ask businesses about what type of personal information is being collected, as well as requiring businesses to disclose the purpose of collecting or selling the information, and who is receiving it. The law actually goes further to state that consumers can initiate civil action if they believe any company wasn’t protecting their personal data with the utmost care.

Given shifting consumer opinion, it is likely that AB 375 is the tip of the iceberg for the US and we’ll start to see more GDPR-like laws appear across states. This ebook takes a deep dive into how consumers are reacting to data security issues, and provides guidance to brands on how to mitigate the risks to their businesses given the current security crisis.

CHAPTER 2

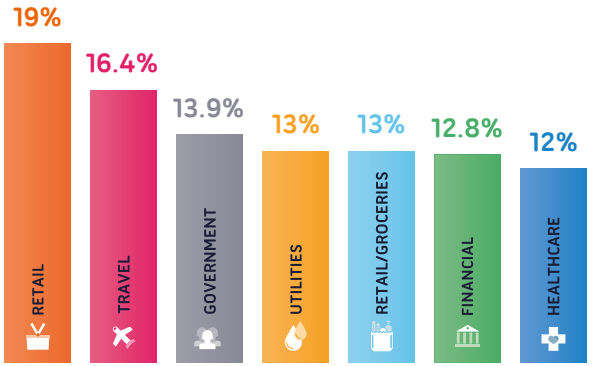
Times are a-changin': consumers don't feel safe anymore

To get an accurate temperature check on sentiment around security, we embarked on a 2,000-person study to understand how consumer are reacting in light of the never-ending parade of security breach headlines.

With about half (44%) of U.S. consumers reporting being a victim of a security breach, 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. The vast majority of Americans now expresses concern when sharing personal data with brands both on and offline. In fact, our research found that only 3% of consumers think there is no problem with data security practices in the U.S. Businesses need to understand this change in perception and address it head on, or risk losing valuable dollars.

This concern especially applies to the retail and travel verticals, as consumers reported trusting those companies the least with their personal data, at 19% and 16.4%, respectively. The finding isn't necessarily surprising with even global brands, such as British Airways, being breached, and the numerous reports of credit card data being stolen from big name retailers such as Macy's, Lord & Taylor, and Under Armour. One recent report suggested that almost 90% of the login attempts made on online retailers' websites are by hackers using stolen data, suggesting that consumer concerns are well-founded.

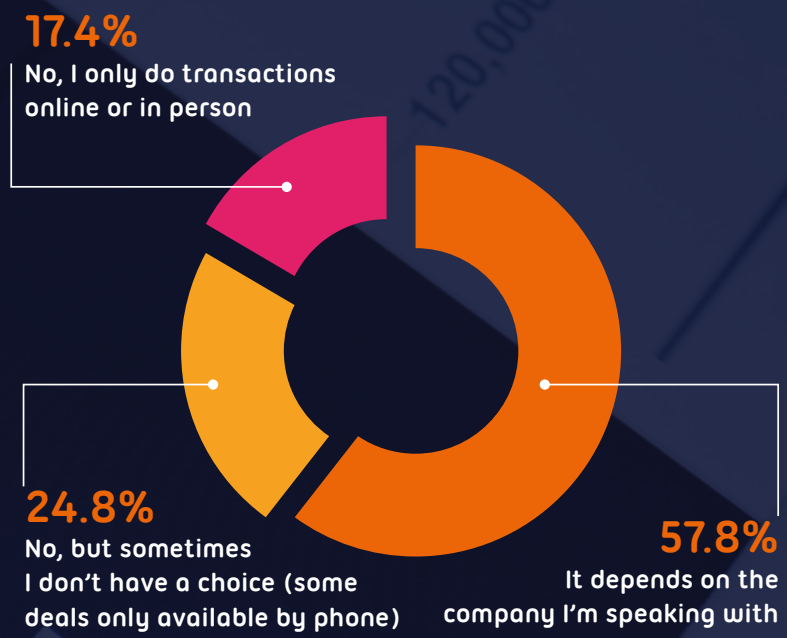
What industries do you think are the least secure?



As such, 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.

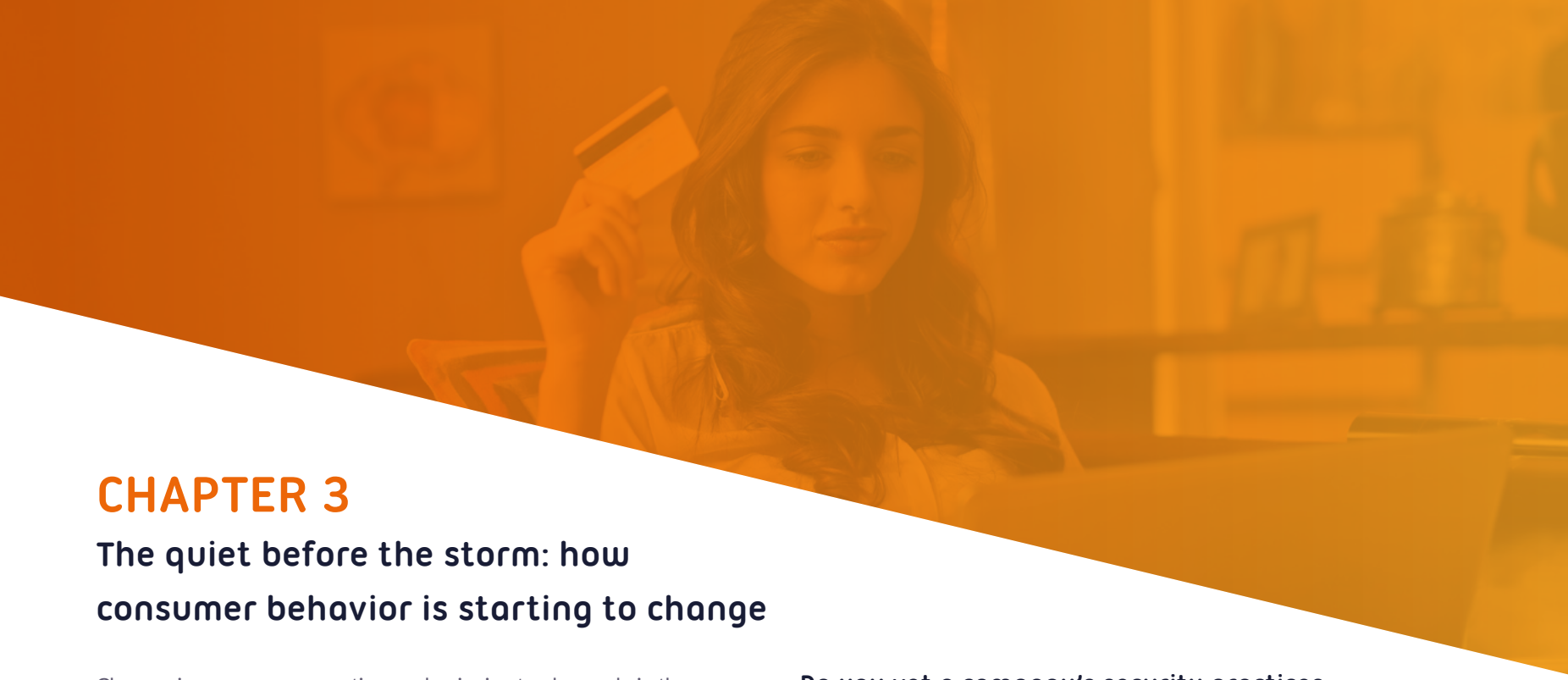
It's not only certain verticals or types of companies that alarm consumers, it's also how brands are obtaining their personal information. Over 40% of consumers feel troubled when reading their credit card information over the phone, which is a real concern for call center businesses who are facilitating transactions. Speaking the words out loud allows anyone on either side of the phone call to obtain your information, so it's understandable that this worries consumers. Another warning for businesses is that 58% 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 it's bottom line.

Are you comfortable reading your credit card number over the phone to complete a transaction?



So what would make consumers feel better about data security in general? Almost half want companies to undergo regular security audits and verification system; another third would feel more safe if SSNs were not required for everything, 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.

The solution for 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 regulatory requirements.



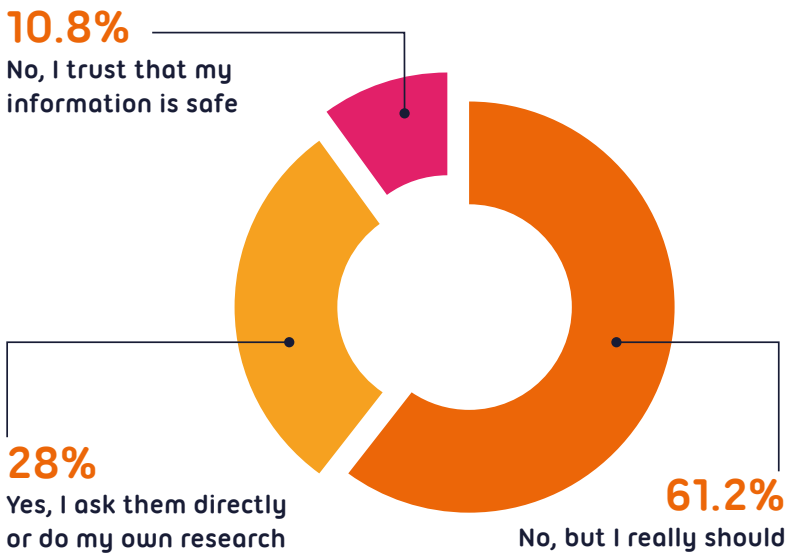
CHAPTER 3

The quiet before the storm: how consumer behavior is starting to change

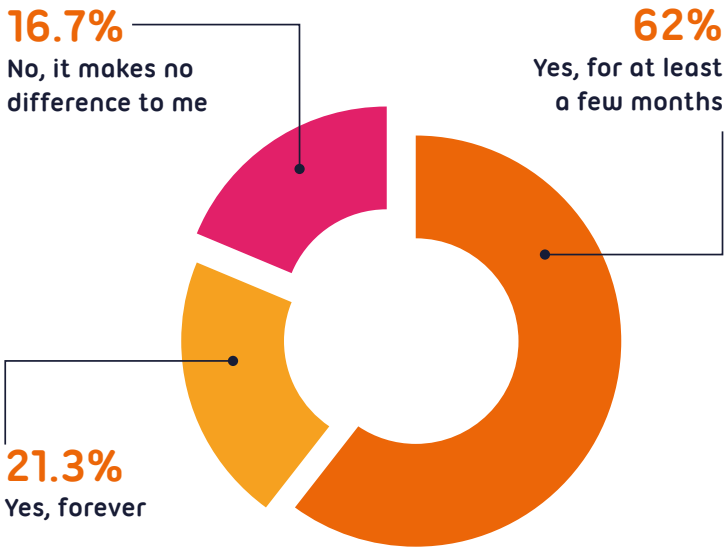
Changes in consumer perception are beginning to play a role in the way individuals engage and spend with brands. Almost 80% of consumers have changed their spending habits based on their trust in a brand's security, and a whopping 89% of consumers don't trust their information is safe with companies anymore. That 89% has started to press businesses on their security practices to assess whether they feel safe to spend, or should look elsewhere.

28% of 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 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.

Do you vet a company's security practices before giving your information?



Will you stop spending with a brand after a hack? If so, for how long?



This applies to call centers which often serve as the front line for over 60% of consumers dealing with questions about security. 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 share the work being done to protect personal data. If they can't, brands may lose business from fearful and uncertain consumers.

But what does this all mean for the company's bottom line? On top of facing massive fines (GDPR lays out up to 23.3M or four percent of annual global, whichever is highest), our research found that 83% of consumers will stop spending with a business for several months in the immediate aftermath of a security breach. Even more significantly, over a fifth (21%) of consumers will never return to a business post-breach, representing a significant potential revenue loss.

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.

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, 41% of consumers want the business to admit responsibility and invest money in improving its security efforts. But for some, that isn't enough: 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 or GDPR compliance to earn back trust. In total, 88% of consumers require businesses to make additional investments in their security after they are hacked.

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 most simple 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.

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 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- a work-around introduced to give organizations an alternative to security requirements that could not be met due to legitimate technological or business constraints. Research conducted by Verizon shows that the 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 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 the network 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 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 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.

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

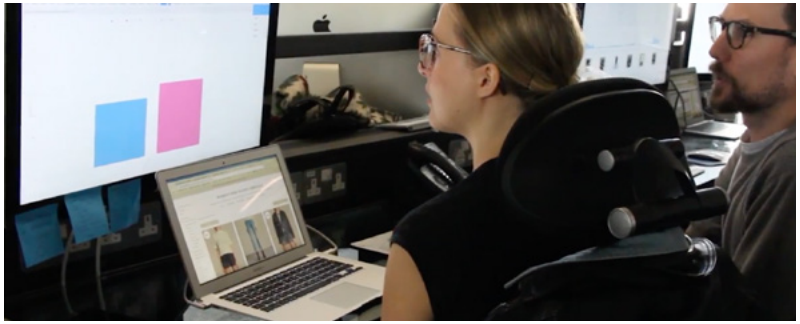
The AllSaints customer experience team were facing a number of problems in creating a seamless customer journey. Time-consuming for both agent and customer, AllSaints needed to join up their various systems and provide a payment solution that would be smooth and painless for both parties.

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

Riding the waves of change: compliance style

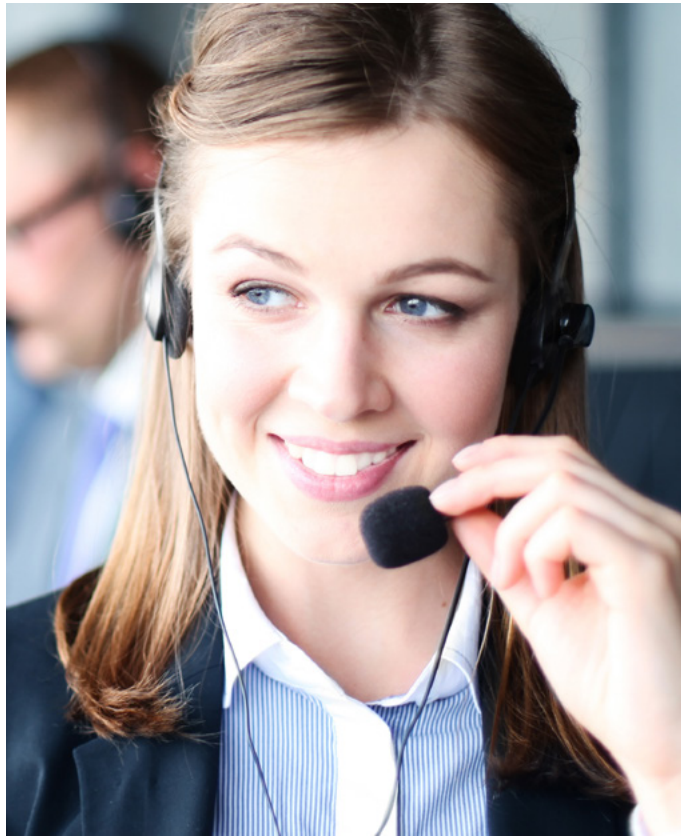
There's no doubt that this shift in consumer sentiment should be concerning for businesses, especially retailers and travel-related organizations. Hacks are at an all-time high, and trust is at an all-time low, meaning that their business revenue is at risk. Businesses need to make moves now to protect 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 21% 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. 88% of consumers require that businesses make large investments in their security after they are hacked in order to lure them back. As we mentioned before, the most simple answer to this is to make sure there isn't any information in the ecosystem 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 for 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.



21%

OF SALES REVENUE COULD BE LOST PERMANENTLY

as consumers lose trust in companies

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 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 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 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 recognises 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 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 how PCI Pal can help secure your contact center without compromising your customer service experience, 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**

info@pcipal.com

615 South College Street, Charlotte, NC 28202, USA

www.pcipal.com

Award winning secure payment technology

Award winning secure payment technology

www.pcipal.com