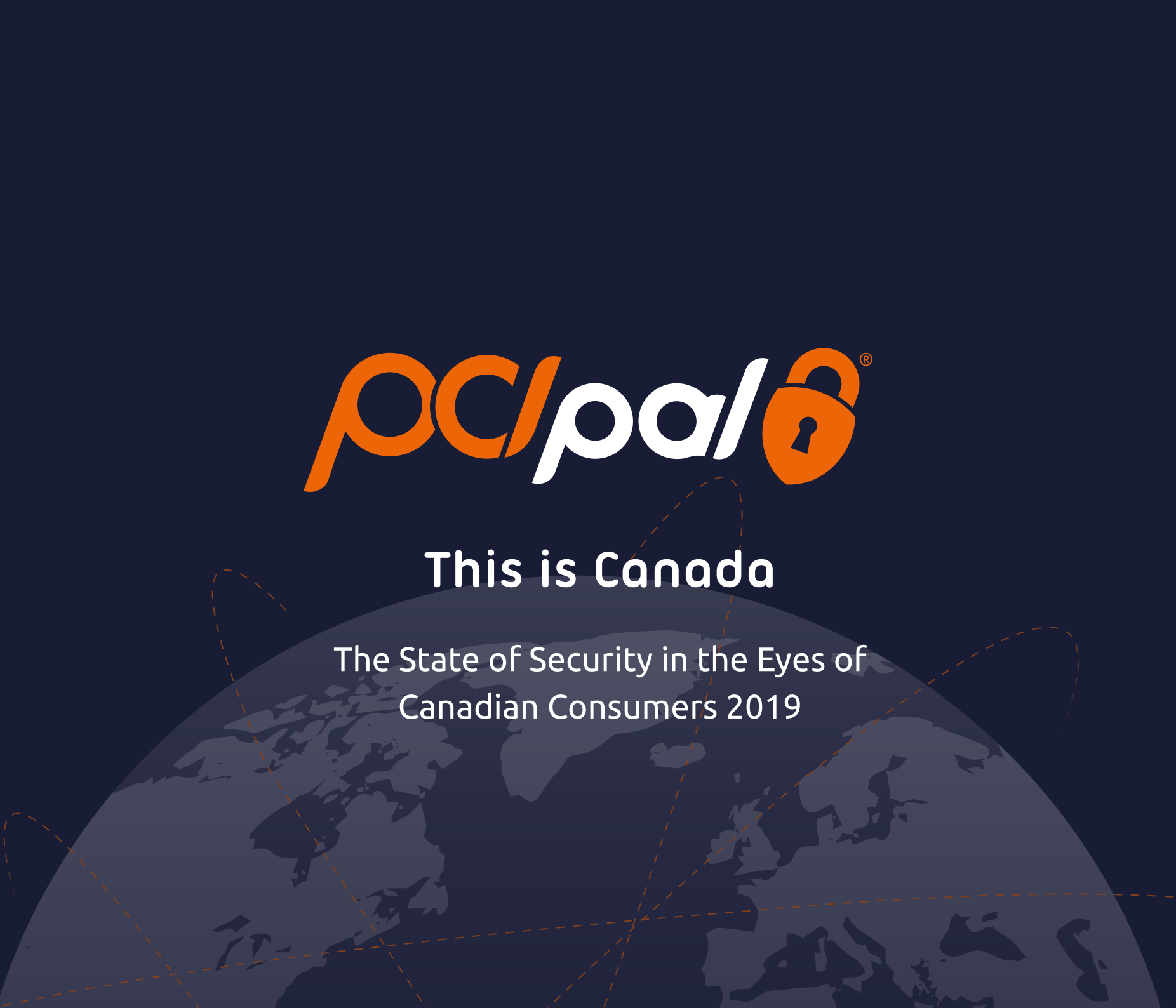


This is Canada

The State of Security in the Eyes of Canadian Consumers 2019

Contents

In May 2019, PCI Pal conducted market research via Environics Research, surveying over 2,000 consumers aged between 18 and 65 living in Canada with a household income between $30,000 CAD - $650,000 CAD.

We wanted to uncover sentiment and behavior changes when it comes to data security. Our findings suggest that the combination of recent high-profile breaches and headlines devoted to the introduction of Canada's Personal Information Protection and Electronic Documents Act 2018 (PIPEDA), and personal experience have put security concerns at the forefront for Canadians.

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

The findings suggest that it's not just online threats that consumers are concerned about, with 18% of respondents refusing to conduct financial transactions via phone and almost half (42%) 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.K. **+44 207 030 3770**

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

marketing@pcipal.com

www.pcipal.com

CHAPTER 1

A brief history of Canadian consumer privacy

As of Nov 1, 2018, Canada introduced the latest in a series of new data and related regulations. Inspired by Europe's GDPR, Canada's Personal Information Protection and Electronic Documents Act, known as PIPEDA, took effect. Similar to other privacy laws, PIPEDA decrees that organizations must obtain consent when collecting or storing personal information - and that all personal information - including identifiers, financial data, medical records and even opinions - falls under PIPEDA protection. Where there is something of a contrast to harsher laws such as the GDPR, the penalties that can be incurred for breach of PIPEDA regulations are significantly lighter. Data breaches must be reported to the Office of the Privacy Commissioner and affected customers according to the law but failure to do so will only incur fines of up to $100,000.

34k

CANADIAN USERS

had their personal data exposed from a security breach in March 2019

The lower penalties afforded by PIPEDA raised some eyebrows and were specifically targeted by the more recent ten principle Digital Charter unveiled by the federal government in May 2019. With a clear promise that the principles would make their way into future legislation and regulations, the Charter proposals would bring federal privacy private sector legislation much closer to the EU's GDPR. Promises to move in this direction are welcomed by consumers increasingly concerned about the myriad ways in which their data is being collected, used, sold and significantly, stolen but, until they become real-world regulations, security breaches and the impact on trust, revenue and reputations continue apace.

High-profile brand names such as Equifax and Hyatt dominate the headlines but they are not alone, and the problem affects industries as disparate as telecoms provider, Freedom Mobile and healthcare business, Natural Health Services whose March 2019 breach exposed the personal information of approximately 34,000 medical cannabis users.

Currently at least, Canadian businesses are compelled to come clean and pay the (small) financial price for a security lapse. But for the victims of a breach, the consequences can be far-reaching, with ruined credit scores or stolen identities impacting future financial decisions.

"...the Charter proposals would bring federal privacy private sector legislation much closer to the EU's GDPR."

CHAPTER 2

Consumers are rightfully concerned about growing security threats

To assess the level of concern and consumer sentiment around security in Canada, we conducted a 2,000-person study to understand how consumers are reacting to the growing threat of security breaches.

With just over a third (37%) of Canadians reporting being a victim of a hack or 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. In fact, the vast majority of Canadians now express concern when sharing personal data with brands both on and offline - only 15% of consumers say they have no concerns about sharing personal information with brands. Businesses need to understand this change in perception and address it head on, or risk losing valuable dollars.

37%
OF CANADIANS
reported being a victim of a hack or security breach

What industries do you think are the least secure?

This is particularly concerning to retailers - a shocking 65% of Canadians rate Retail as the least secure sector, followed closely by the Travel industry at 41%. These findings aren't necessarily surprising, with even global brands in these sectors being breached, and the numerous reports of credit card data being stolen from undisclosed big name retailers. Interestingly for Canadians though, is a significant lack of trust for financial services and even government - almost a quarter (24%) rated both as the least secure.

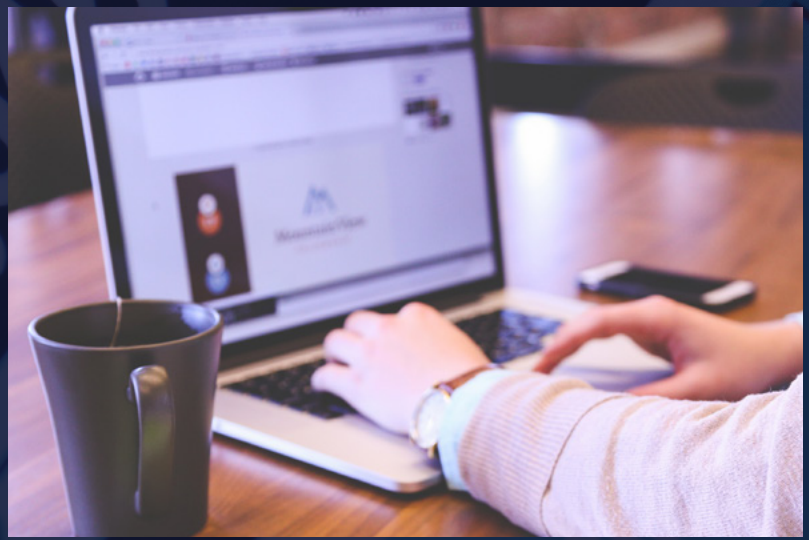
Brands in these high-target categories need to take extra measures to ensure their data is protected, and communicate the security investments made to consumers to restore their trust in the industry.

It's not only certain verticals or types of companies that alarm consumers, it's also how brands are obtaining their personal information. Almost half (42%) 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 Cardholder Not Present (CNP) transactions. Speaking the information 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.

So what would make consumers feel better about data security in general? Over half (62%) want companies to undergo regular security audits, and another half would feel more safe if sensitive personal information was not required for everything. 49% of consumers would feel better if businesses were federally mandated by stricter regulation to protect their data.

The solution for any business operating call centers is to invest in technology that prevents customers from having to speak their private information out loud. Not only will this reassure increasingly wary consumers, but it will also ensure the business is compliant with regulatory requirements.



CHAPTER 3

How Canadian consumer perception is impacting their behaviors

Changes in consumer perception are beginning to impact the way Canadians engage and spend with brands. 65% of consumers claim they will change their spending habits based on their trust in a brand's security (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 better vetting a company's security practices before giving their information. These figures show that consumers are growing increasingly uncomfortable with how businesses are managing data and presenting those security efforts - they want to know more.

65%

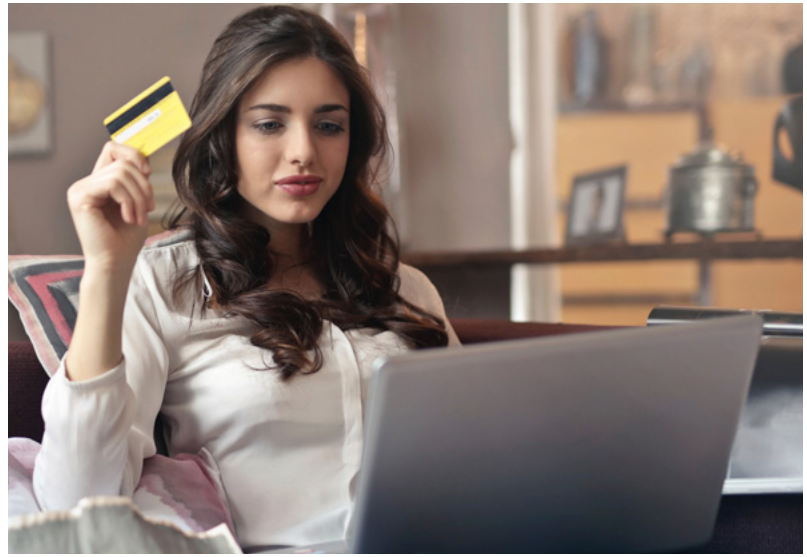
OF CONSUMERS

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

But what does this all mean for a company's bottom line? On top of facing financial penalties, our research found that a stunning 78% of consumers will stop spending with a business following a data breach, 58% for several months in the immediate aftermath of a security breach and a fifth 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.

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



78%
OF CONSUMERS
will stop spending with a business following a data breach

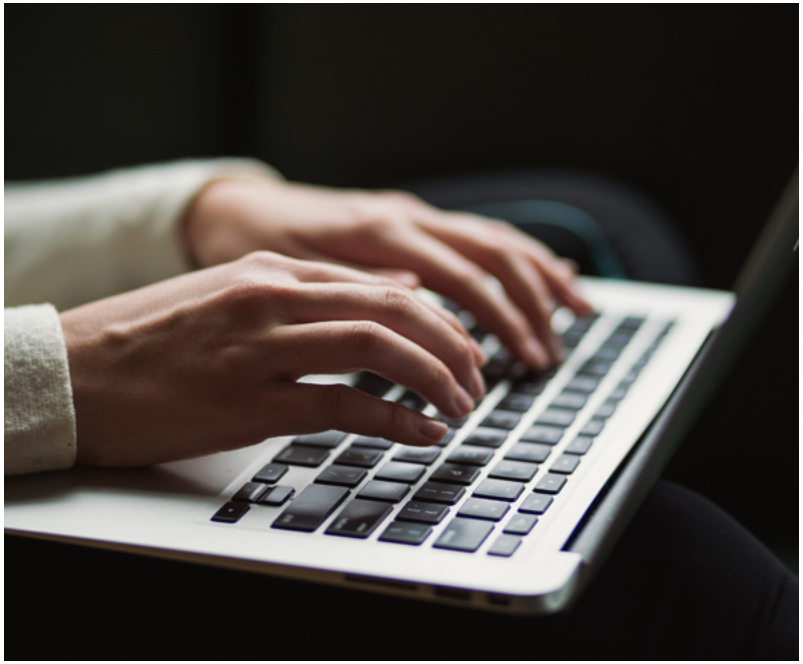
The good news for businesses is that consumers can be encouraged to forgive (if not quite forget) a security lapse, but that forgiveness comes at a price. In the event of a hack, 33% of consumers want the business to admit responsibility and invest money in improving its security efforts. But for some, that isn't enough: 26% want a third party to confirm its system is safe before spending with them again, and another 28% go even further to require the company to announce security 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 hack. 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.

CHAPTER 4

PCI compliance and how PCI Pal helps businesses

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 compliance. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations to ensure the protection of sensitive cardholder data. Founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc, PCI DSS enables companies 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 organizations an alternative to security requirements that could not be met due to legitimate technological or business constraints. Research conducted by Verizon in 2018 found that the organizations subject to a security breach were more likely to be using compensating controls. In the short-term, compensating controls, such as pause and resume, act as the intended bandage that

they are, but practically speaking, they aren't good long-term solutions for businesses. Relying on compensating controls will not prevent fraud or breaches, thus risking 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 from the requirements of PCI DSS.

Our core solution to the compliance 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 their 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. We have simple and proven telephony and API integrations minimizing the impact on business operations.

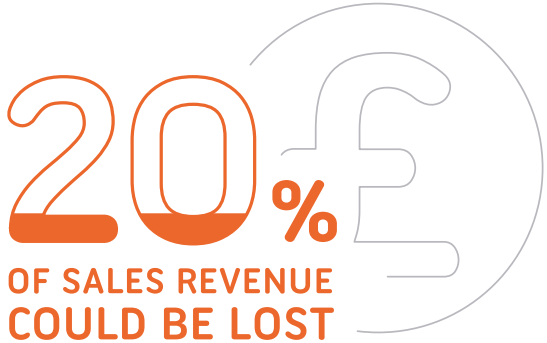
"Being fully compliant with PCI DSS takes away the bandage and stitches the problem permanently, becoming vital for the survival of businesses, both in terms of reputation and finance."

CHAPTER 5

Adapting to compliance requirements

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 revenue is at risk. Businesses need to make moves now to protect their reputation, revenue and consumer trust.

Arguably the most alarming finding in our research was that businesses stand to lose 20% of their sales revenue forever if they are hacked. That doesn't include the fines from the government, lawsuits or any other potential negative outcomes 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. Nearly half of consumers require that businesses admit responsibility and make investments in their security after they are hacked in order to lure them back. We believe the simplest answer to this is to make sure there isn't any information in the contact center environment to steal - by descoping your business from the requirements of PCI DSS.



Invest in 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 their contact centers, ensuring that valuable, hacker-attracting data isn't available to steal. Rather than investing time and money in a vault to protect valuable data from external hackers, or even internal agents, PCI Pal ensures that there is nothing in the vault to guard or steal.

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 distrust. Consumers across the board want to see businesses not only investing in technology to safeguard their data, but they also want to be kept informed. Transparency is going to be key for earning, maintaining 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 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 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 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.

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**

marketing@pcipal.com

www.pcipal.com

Award winning secure payment technology

Safeguarding reputations and trust

www.pcipal.com