



This is Australia 2022

The State of Security in the Eyes of
Australian Consumers Today

Contents

A brief history of Australian consumer privacy	4
Consumer concern about cybersecurity threats	6
How Australian consumer perception is impacting their behaviours	8
PCI compliance and how PCI Pal helps businesses	10
Adapting to compliance requirements.....	12
Your Annual PCI checklist	14
A PCI glossary	16

The latest figures released within the Office of Australian Information Commissioner (OAIC) Notifiable Breach Report revealed that ‘More than 75 per cent of pandemic-related cybercrime reports involved Australians losing money or personal information.’

In January 2022, PCI Pal conducted market research with Atomik Research, surveying over 1,000 adult consumers across Australia on their attitudes to sharing payment data with brands.

We wanted to understand how the Covid pandemic might have changed consumer attitudes to personal and financial data security, particularly as many organisations’ contact centre staff now operate remotely.

Our survey findings suggest that greater awareness of data security, as a result of a growing number of consumers’ personal experiences of data breaches, have hardened consumer attitudes and behaviours towards organisations that fail to safeguard their personal and financial data.

Almost three quarters of respondents (70%) expressed concerns about sharing payment details with organisations where staff work from home or operate remotely as a result of the pandemic. Over half of people surveyed (51%) said that they had been the victim of a security breach. The majority (90%) said that they would temporarily, or permanently stop spending money with any organisation that compromised their data as a result of poor security practices.

These findings, and others that we share in this e-book, demonstrate how important it is for organisations to mitigate these concerns, particularly those that operate contact centres and take payments over the phone. 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

 **AUS +61 2 7202 0294**

 **info@pcipal.com**

 **www.pcipal.com**

CHAPTER 1

A brief history of Australian consumer privacy

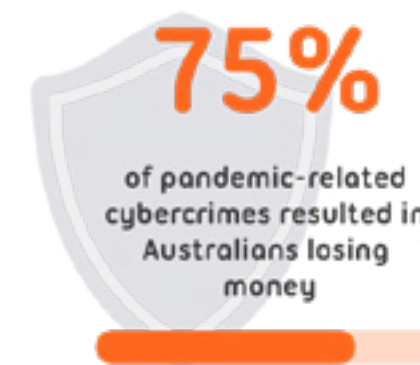
The Australian Parliament passed The Privacy Act of 1988 in order to protect individuals' personal information handled by Australian Government agencies, and to implement safeguards for the collection and use of tax information. Several amendments have been added throughout the years to regulate the handling of consumer credit reports and set standards for the secure collection, use, storage and disclosure of personal information in the federal public and private sector, as well as additions relating to data handling in specific industries, such as telecommunications, pharmaceuticals and healthcare. In November 2017, the Australian government introduced the Consumer Data Rights to empower Australians to decide how their data is used and shared in the banking sector. The government plans to expand this to cover other sectors in the future.

These increases in consumer data privacy protections are laudable, but, as the OAIC's latest Notable Breach Report shows, there is always more work to be done. Organisations across all industry sectors must prioritise security and maintain systems that protect citizens' data from the latest methods of attack. Even after enacting stricter reporting guidelines under Australia's Privacy Act, high-profile breaches and attempted hacks are still happening. The Australian Cyber Security Centre figures reveal that of the 67,500 cyber incidents reported in 2021, more than 75% of pandemic-related cybercrimes resulted in Australians losing money, or personal information, with an estimated \$33 billion (AUD) lost overall. The OAIC reported in March 2019 that a single breach affected more than 10 million Australians.

Security breaches that result in the loss of consumers' personal and payment card data can seriously impact victims' lives, including affecting individuals' credit scores, preventing them from obtaining a loan, or even being able to take out a mobile phone contract.

In response, our findings show that consumers are demanding that brands do a better job of protecting their data and are either threatening to take their money elsewhere if they feel security practices place their data at risk, or are actually voting with their wallets.

On the flipside, our survey found that when consumers feel reassured that a brand is doing everything that it can to keep their data and financial transactions safe, they are more likely to spend more with that organisation.



“... When consumers feel reassured that a brand is doing everything that it can to keep their data and financial transactions safe, they are more likely to spend more with that organisation”

CHAPTER 2

Consumer concern about cybersecurity threats

We conducted the study with 1004 Australians to understand how consumers' sentiment and behaviour might be affected by the growing number of security breaches. With 51% of our survey participants reporting being a victim of a hack or security breach, it was no surprise that the research revealed a significant change in how consumers are thinking and acting when it comes to data security. In fact, 90% of Australians surveyed said that if their data was compromised as a result of poor security they would avoid spending money with that organisation. Businesses need to understand this change in behaviour and address it head on, or risk losing valuable dollars.



Our findings revealed a substantial change in the industry sectors that consumers trust the least with their personal data. In our 2019 study, 50% cited retail as the riskiest sector, followed by travel (40%) and the financial sector (36%).

Figure 1: least secure industries



In 2022, this has switched, with 44% of consumers saying that finance is the most prone to security breaches, followed by government (39%) and retail (26%) See Figure 1. Indeed, these were all cited in the Australian Cyber Security Centre's top ten reporting sectors for cyber security incidents during the financial year 2020 – 2021.

Brands in these high-target / low-trust categories need to take extra measures to ensure their data is protected, and clearly communicate to consumers the security investments they have made, in order to regain their trust.

CHAPTER 3

How Australian consumer perception is impacting their behaviours

When asked if they would stop spending with an organisation following a reported hack or data breach, more than three quarters of respondents (78%) said they would pause spending, 40% said that they would never spend money with that brand again, 27% said that they would remove their custom for a few months, 11% said that they would avoid spending with the affected brand for at least a few weeks, 17% said that they would continue spending with a breached organisation, but would worry that it could happen again. These figures demonstrate the scale of losses in revenue, reputation, and consumer trust that can result from a breach, in addition to any financial penalties that might be incurred if the affected organisation is found to have been non-compliant with industry frameworks and data security regulations.



78%
of Australian consumers
would pause spending
with an organisation if it
suffered a data breach

When asked what it would take to coax them back to a brand that had suffered a breach, 43% of respondents said they would need to see confirmation from a regulator, or other third party, that the brand's systems have been made safe. Over a third (37%) said that they would need to see the brand admitting responsibility and investing money in improving their security, while 34% would want to see evidence that the brand had adopted strict payment security practices, such as verified compliance with the Payment Card Industry Data Security Standard.

The good news is that brands that can show that they are handling consumer data in a responsible and secure manner are likely to generate higher revenues. When our survey sample was asked whether trust in a brand's security affects their spending, 40% of consumers confirmed that they will spend more with brands that they trust to keep their personal and financial data safe.

“When our survey sample was asked whether trust in a brand's security affects their spending, 40% of consumers confirmed that they will spend more with brands they trust to keep their personal and financial data safe.”



CHAPTER 4

PCI compliance and how PCI Pal helps businesses

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations 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 organisations 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 found that the organisations subject to a security breach were more likely to be using compensating controls.”

Research conducted by Verizon in found that the organisations 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 is the storage of data in systems. In addition to investing time and money in protecting data from would-be hackers, merchant organisations can simply make sure there's no customer payment data there to steal. Reducing or removing the amount of customer data stored, lessens the risk 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, PCI Pal Agent Assist, integrates with the merchant's payment gateway via our AWS cloud infrastructure, providing companies with a solution to receive payments by phone, without storing any payment data within their systems and thus descopeing 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, minimising the impact on business operations.



90%
of Australian consumers would avoid purchasing from a business that compromised their data

CHAPTER 5

Adapting to compliance requirements

There's no doubt that this shift in consumer sentiment should be concerning for businesses, especially within verticals where consumers feel their data is at most risk, such as finance and retail. The incidence and severity of hacks are increasing, and consumer trust is declining, with a resulting risk to business revenues. Businesses need to make moves now to protect their reputation, revenue and build trust with customers.

Arguably, the most alarming finding in our research was that 90% of respondents said that they would avoid purchasing from a business that compromised their data as a result of poor data security practices: 38% said they would avoid the business for several months, 25% would avoid spending with the business for several years, and 25% said that they would never give that business their custom again.

It's clear from these findings that financial losses from a breach aren't isolated to the fines from the Government, or lawsuits from seriously unhappy customers. The damage sustained by a 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. 37% of the respondents said that they need to see organisations admit responsibility and make investments in their security after they are hacked in order to win them back. One of the most simple ways to provide this reassurance is to ensure that there isn't any sensitive payment information in the business environment to steal - by descope your business from the requirements of PCI DSS.

Invest in technology

Achieving and maintaining 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 Agent Assist exists to descope your contact centre from the requirements of PCI DSS, ensuring that valuable, hacker-attracting data never enters the contact centre ecosystem.

Own up to your mistakes as well as your solution

We've seen the headlines sounding alarm bells about the number of data hacks occurring each year. It happens so often that breaches no longer surprise anyone, and this reinforces consumer distrust. Consumers across the board want to see businesses not only investing in security, but explaining the security measures that they have taken in terms that consumers can understand. As our survey findings reveal, transparency is key for earning, keeping and, in the event of a breach, regaining 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 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 – visaurope.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 up to 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 make sure your implementation of this application is secure and compliant with PCI DSS. PA DSS compliance and configuration by a QIR may help with this
- 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 – Physically accessing a specific port that allows for administrative actions without needing network access, or

elevated access for both administrative and non-administrative actions.

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.

Descoping - keeping customers' card data out of company systems and minimizing contact areas where data is processed or stored.

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 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.

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 – Payment Card Industry Data Security Standards

PCI SSC – The PCI Security Standards Council.

PFI – PCI Forensic Investigator – The person who investigates system breaches to analyze 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

 **AUS** +61 2 7202 0294

 **info@pcipal.com**

 **www.pcipal.com**

Safeguarding reputations and trust



Safeguarding reputations and trust

www.pcipal.com