This is Canada 2022

The State of Security through the Eyes of Canadian Consumers Today

Contents

In December 2021, PCI Pal commissioned AYTM, a market research organization, to survey 1,100 consumers resident in Canada.

This latest survey follows on from PCI Pal's earlier report, *This is Canada: The State of Security in the Eyes of Canadian Consumers 2019*. In 2019, our aim was to uncover Canadian's sentiments towards and behaviors around data security. Our latest survey and report revisit the theme in a commercial and societal environment that has been transformed by the COVID-19 pandemic.

Our findings reveal that trust in the ability of brands and companies to protect personal information and ensure secure payments processes is still a precious commodity. Our research highlights that all payment channels, including both real world and digital, face a trust deficit, and that businesses will need to address this as consumer shopping patterns change in the wake of the pandemic.

What's clear is that the trust Canadians have in a company and its approach to information security directly impacts the likelihood they will shop with that company, and also the amount of money they would be willing to spend. The report provides a clear call to action to businesses in Canada to mitigate the concerns of consumers around information security and to communicate the steps they are taking to protect personal data.

This e-book provides the full findings of our latest research and commentary on what these trends mean for businesses as they look to implement secure and compliant payment systems.

If our research findings pose any further questions, or you'd simply like to discuss your specific requirements in more detail, please get in touch.

GET IN TOUCH

☎ USA **+1 866 645 2903**

✉ **marketing@pcipal.com**

www.pcipal.com

CHAPTER 1

Consumer privacy in Canada: the state of play

In Canada, consumer privacy online is for the most part protected through the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2018. PIPEDA mandates that supervised entities obtain an individual's consent when they collect, use, or disclose that individual's personal information. The Act also states that organizations must protect consumers' personal data with appropriate safeguards.

PIPEDA is not the only piece of applicable privacy legislation in Canada. In addition, local private sector privacy laws apply in Alberta, British Colombia, and Québec. These local laws have in the past been substantially similar to PIPEDA, but they are now diverging and becoming more influential to the overall direction of Canadian privacy policy.

Until now, Canadian regulators have acted as ombudsmen of privacy regulations, helping mediate between individuals and organizations and providing recommendations to enterprises around how they can achieve compliance. However, the trend now appears to be toward a much more robust enforcement role.

For instance, Québec's Bill 64, An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information, which received assent in September 2021, empowers the Commission d'accès à l'information (CAI) to issue penalties of up to $50,000 CAD for individuals. The act also provides for penalties of either $10 million CAD or 2% of worldwide turnover of the previous year for businesses. This is a significant step up from PIPEDA, which mandates just $100,000 CAD fines for single instances of a breach.

2022 promises to be a packed year for privacy regulation in Canada, and changes come as security breaches continue to make headlines. In the year up to March 2021, the federal privacy commissioner had received 782 breach reports, affecting around nine million Canadian accounts. Meanwhile the Canadian Centre for Cyber Security reported 235 incidents of ransomware attacks against businesses.

Sensitive consumer data is more exposed than ever because people are more reliant on digital services due to the impact of COVID-19. For example, according to one study, 50% of Canadians report making online purchases for items that they would typically have bought in-store. Fifty-three percent of North Americans report that they have changed the way they shop, suggesting that changes made because of the pandemic will last long-term.

53%

report that they have changed the way they shop since the start of the pandemic

Canadians have been shaken by the pandemic and the many changes it has wrought. What people crave now is a degree of certainty, and relationships with brands and service providers they can trust. Delivering secure and compliant payment and communications services is therefore more vital than ever for organizations, caught as they are in the grips of both tightening regulations and consumer demand for trustworthy services.

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.

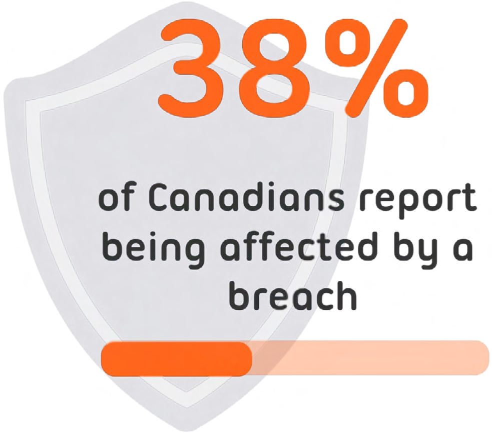
> *"...Delivering secure and compliant payment and communications services is more vital than ever for organizations, caught as they are in the grips of both tightening regulations and consumer demand for trustworthy services."*

CHAPTER 2

Consumer security concerns in the age of COVID

Canadian citizens are well aware of the security threats they face regarding their data, with 38% having personally been affected by a breach. That this number is slightly higher than the 37% recorded in 2019 may reflect the increased number of Canadians using digital services rather than a lack of investment in compliance and security solutions by businesses.

When it comes to spending behavior, Canadians are increasingly moving online. A quarter of Canadians say they now purchase almost everything online, and three quarters say that their spending habits have changed in some way. And these new habits are likely to last. While only 3% of people believe they will continue to shop exclusively online, 40% anticipate using a hybrid approach in the future, with purchases split between digital and in-store channels.

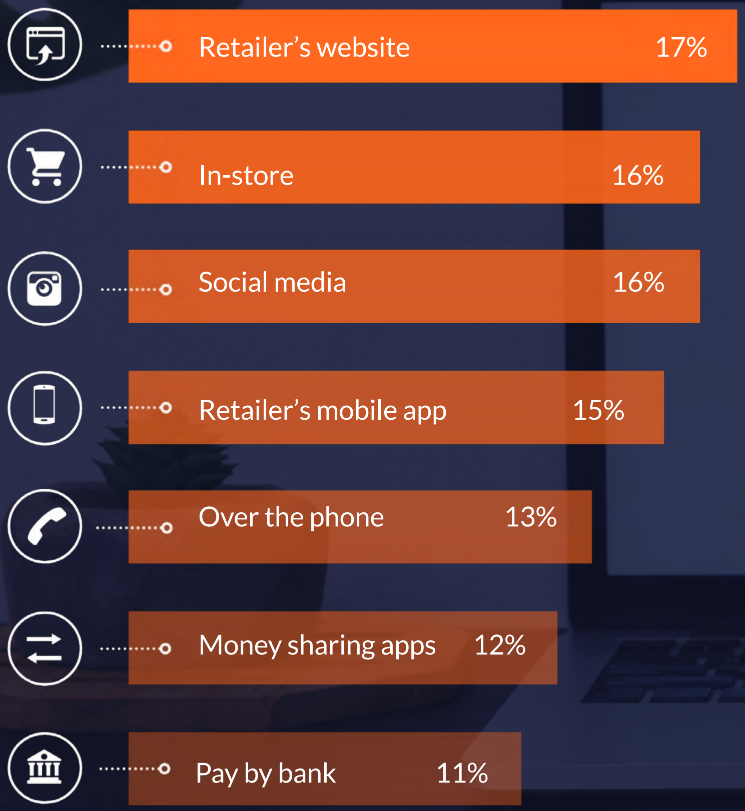


38%

of Canadians report being affected by a breach

As the ‘new normal’ for purchasing plays out, consumer confidence in payment mechanisms will be crucial. Presently, there is no clear favorite. When asked to identify their least trusted payment channel, consumer opinion was divided (see figure 1).

Figure 1: least trusted channels for shopping



These findings are remarkable for several reasons. First, there is practically speaking no difference in levels of trust between paying for something in-store vs. over a website – and that these channels (along with social media) are the least trusted by consumers.

Second, relatively novel money-sharing apps like PayPal, Venmo, and Zelle are counterintuitively more trusted than better established channels (such as in-store and web). Yet novelty does not account for this trend, as is seen by the 16% of people who distrust social media the most.

Finally, despite phone-based scams being on the rise in Canada, payment over the phone is more trusted than ostensibly more secure channels such as in-store. That is not to say they are trusted implicitly. If asked to provide personal information over the phone to complete a transaction, 56% of people say they would hang up and look for an alternative or ask for an online option. Twenty-seven percent would feel uncomfortable and ask about how the information is being taken down and whether it is safe.

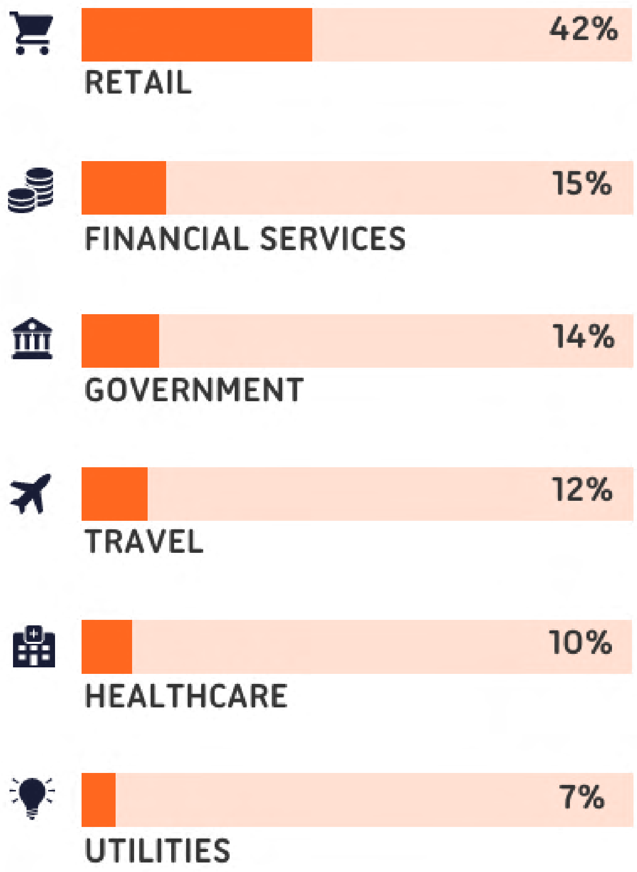
> *“Shoppers today have more payment options than ever. Clearly, there are also a greater range of factors that come into play when selecting which to trust.”*

Who to trust? An industry analysis.

Inclusive of payments, but also more broadly, businesses need to keep a finger on the pulse of consumer sentiment when it comes to trust in their ability to secure data. This varies widely between industries.

As in the 2019 PCI Pal report, a majority of survey respondents believe that retail is the least secure sector when it comes to protecting personal data, although this number has reduced somewhat (42% in 2021 vs. 65% in 2019) it is still in the majority. It is good news that retailers are catching up with other industries in terms of consumer confidence, especially given that adoption of data-heavy digital retail accelerated through the pandemic. However, the trust gap between retail and other sectors remains significant, with the gap between retail and the second least trusted sector, financial services, coming in at 27% (see figure 2).

Figure 2: Industry sectors consumers believe to be least secure when it comes to protecting their personal information



Retailers and, to a lesser extent, financial services firms and government agencies therefore need to both ensure their data is protected in line with relevant legislation (see Chapter 1), and, importantly, that relevant investments and process improvements are communicated to their consumer base.

Interestingly, the sectors most trusted by Canadians are utilities and healthcare – services that have been in high demand over the past two years. When it comes to payments, it is worth noting that businesses in these sectors typically use a blend of online portals in addition to more traditional means such as phone payments. Potentially this choice helps consumers feel in control and helps build trust.

> *"... businesses typically use a blend of online portals in addition to more traditional means such as phone payments. Potentially this choice helps consumers feel in control and helps build trust."*

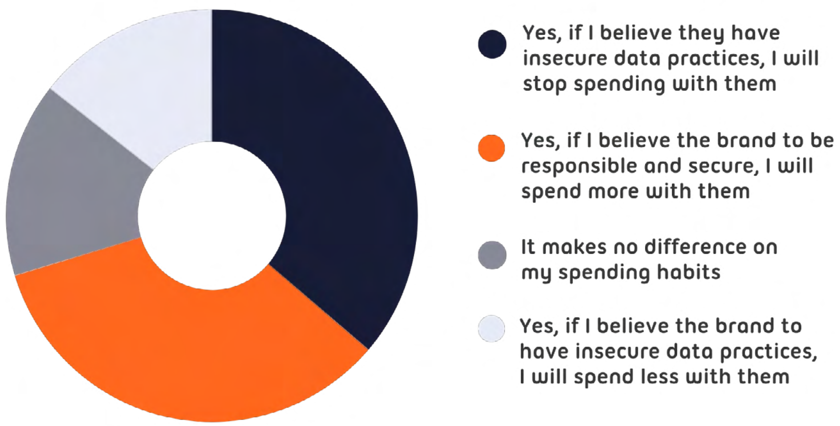
CHAPTER 3

The bottom line: security concerns affect consumer behavior

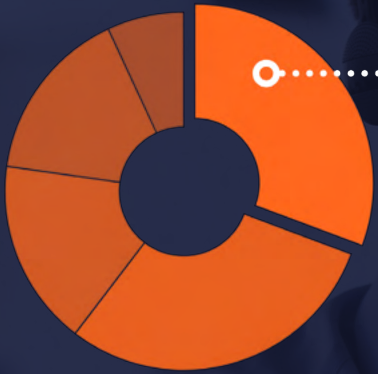
It is common sense that the levels of trust people have in brands to protect their data, and that brands purchasing channels are secure, influences how people spend and with whom. The research bears this out. Seventy-eight percent of Canadian shoppers say that they will stop spending with a brand that has experienced a hack, either forever (23%) or for a few months at least (55%).

There is also a link for many Canadians between how much they trust a brand's security and the amount of money they are willing to spend with that brand (see Figure 3). There is therefore a clear financial incentive for companies to invest in robust online, and voice-based security measures across their customer touchpoints and contact centres.

Figure 3: Consumer trust in corporate security affects spending patterns



The payment process is a key element of this mix. In fact, a “sketchy” payment process (31%) is the factor that would put off most survey respondents from following through with a purchase, ahead of unjustifiable shipping costs (30%), slow delivery (17%), the expense of the product (16%) or an inadequate returns policy (7%).



31%

of Canadian consumers state that a sketchy payment process is the greatest factor when making a purchase

The good news for brands is that Canadian consumers do not carry a grudge and will be willing to return to a brand that had suffered a security breach – but only if that company can demonstrate that it has taken remediation measures. Such measures include admitting responsibility and investing to improve security (42%), announcing PCI compliance / PIPEDA compliance (25%), or engaging a third party to confirm that the company’s payment system is safe (25%).

Meeting the needs of empowered consumers

Aware of the threats they face, consumers are becoming more proactive in assessing the capabilities of the companies available to them. Over a third (36%) of the Canadians we surveyed say they vet a company’s security practices before sharing personal data with them, either by asking them directly or carrying our research. A further 51% say that they don’t currently vet in this way but realize that they probably should – perhaps indicating that a greater number of consumers will carry out checks soon.

The good news is that there are a clear range of measures that brands can take to give peace of mind to consumers. Implementing these measures and communicating them to customers is vital to building confidence in today’s payment systems. It will also be important to ensuring that future payment innovations meet with a receptive audience. It is telling that a number of respondents (40%) will only feel comfortable trying new forms of payment if they’re deemed to be from a reputable source.

CHAPTER 4

Enhancing trust in your organization

It is evident that issues around data security are already important to Canadian consumers, and that these concerns are only going to increase over time. The business impact is clear: Lose the trust of customers and lose their business. But the regulatory risk is also clear and growing. As Canadian privacy regulations are amended and given more teeth, and as regulators are empowered to enforce these regulations with stiffer penalties, data security is going to become a significant element of enterprise risk mitigation.

Payment card data is an important part of this mix as arguably the most sensitive personal information that a company holds on its customers, and certainly the most readily open to abuse if stolen by criminals. Compliance with the Payment Card Industry Data Security Standard (PCI DSS), an information security standard for organizations to ensure the protection of sensitive cardholder data, is a top priority in that respect.

So, what practical steps can businesses in Canada – particularly those that consumers trust least to protect their data – take to put themselves on the best possible footing? PCI Pal provides organizations in Canada and elsewhere with secure cloud payment and data protection solutions for any business communications environment including voice, chat, social, email, and contact centre. Through that lens, and based on the findings of our latest survey, we believe there are three key recommendations:

- Reputation is everything, so protect it
- Invest in technology
- Admit to missteps and find a solution

1. Reputation is everything, so protect it

Even with the recent increase in security data breaches, consumers are not lightening up on companies that fall victim to cybercriminals. Organizations need to take every precaution to protect against breaches and safeguard data. As we have seen, consumers are taking fraud prevention into their own hands, which will put a heavier emphasis on companies to provide explicit information regarding security practices. Moving forward, transparency will be paramount for companies to maintain consumer trust and a positive reputation.

2. Invest in technology

It appears that at some point a security breach is inevitable, and although it's hard to cover all your bases, investing in technology can help improve company security and achieve PCI compliance. For example, technology like PCI Pal Agent Assist allows agents to securely capture a customer's payment information while maintaining the conversation. In today's increasingly digital environment, PCI Pal also offers technology such as PCI Pal Digital. Adopting technology like this is critical to improving the performance of a business and maintaining a trusting relationship with customers.

3. Admit to missteps and find a solution

Security breaches are damaging to a company financially, but they can also lead to distrust and an overall loss in loyal customers. For those companies who do make the unfortunate misstep that results in a security breach, being open and admitting to those mistakes will go a long way to repairing a relationship with the affected parties. Even going a step further to adopt and explain a solution to the problem, so it never happens again, can help rebuild consumer trust.

CHAPTER 6

Your Annual PCI Checklist

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

The Payment Card Industry Data Security Standard (PCI DSS) is the information security standard for 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 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.

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

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

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

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

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

IDS – Intrusion detection system.

IPS – Intrusion prevention system.

IVR – Interactive Voice Response – An automated system that allows a computer to 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

☎ CAN +1 866 645 2903

✉ marketing@pcipal.com

www.pcipal.com

Safeguarding reputations and trust

pcipal®

Safeguarding reputations and trust

www.pcipal.com