Inadequate Data Security Practices Come with Serious Financial Consequences for Canadian Businesses

PCI Pal research found that 78 percent of Canadians will stop spending with a company following a breach

Charlotte, N.C., August X, 2019 - Over one-third of Canadian consumers have experienced the consequences of a security breach or hack, according to newly released research conducted by secure payments provider to contact centers, PCI Pal. The findings suggest that a combination of recent high-profile breaches, media coverage of new data privacy regulations such as GDPR and Canada's Personal Information Protection and Electronic Documents Act, and personal experience have made security a top concern for Canadian consumers.

"As data breaches become increasingly common, Canadian consumers are realizing that their personal data is at the mercy of the organizations they shop with. As a result, attitudes toward data security are changing significantly, with a majority of consumers now reporting a company's security practices directly influence their spending habits," says James Barham, CEO, PCI Pal.

The research found that 78 percent of consumers will stop spending with a business following a data breach, with 58 percent reporting that they would avoid a company that's been hacked for several months, and a fifth saying they would never return. This research provides a serious warning as to the implications of a breach for consumer-facing businesses operating in Canada.

Consumers also reported that simply perceiving a company as having insufficient security practices impacts their trust and spending behaviors, with 30 percent reporting they would spend more with an organization they perceive to be trusted and secure, and 35 percent claiming they would either spend less or stop spending completely with those they believe may have insecure security practices.

The findings suggest it's not just online threats that worry Canadian consumers. When it comes to obtaining data, conducting transactions via the telephone securely is also top of mind - 42 percent feel uncomfortable sharing credit card information over the phone, and 58 percent are only comfortable sharing information over the phone to select companies that they either trust or have verified their security measures. For businesses taking Cardholder Not Present (CNP) payments over the phone, these findings underscore the importance of investing in technology that prevents customers from having to share their sensitive information in an insecure way.

With consumers increasingly wary of businesses' data privacy practices, the survey also examined what would make consumers feel better about data security. Over half (62%) want companies to undergo regular security audits, another half would feel safer if sensitive personal information was not required for every transaction, and 49% of consumers would feel better if businesses were federally mandated by stricter regulation to protect their data.

Barham continues: "Given the increase in data breaches, it's unsurprising that consumers are increasingly paying attention to the data security practices of companies they buy from. Our research found that 61 percent believe it is important to vet a company's security processes before giving their information, and 24 percent will go so far as to ask a company directly about their security practices. As these concerns become top of mind for consumers, it will be wise for businesses to adopt and promote stronger security practices, or risk losing customer loyalty."

For more information, download the ebook here.

METHODOLOGY & MARKET RESEARCH
PCI Pal conducted market research through Environics Research, surveying 2000 Canadian consumers aged between 18 and 65 years with annual incomes between $30,000 CAD and $650,000 CAD to uncover customer service preferences and security concerns when sharing personal information online and over the telephone. The survey findings highlighted changing behaviours and considerations for consumers in 2018 around data privacy, brand trust and impact on spending resulting from security breaches.

ABOUT PCI PAL
PCI Pal is a specialist provider of secure payment solutions for contact centres and businesses taking Cardholder Not Present (CNP) payments. PCI Pal's globally accessible cloud platform empowers organisations to take payments securely without bringing their environments into scope of PCI DSS and other relevant data security rules and regulations.

With the entire product portfolio served from PCI Pal's cloud environment, integrations with existing telephony, payment, and desktop environments is simple and light-touch, ensuring no degradation of service while achieving security and compliance.

With extensive operations and technical experience of the contact centre sector, PCI Pal is uniquely qualified to deliver operationally efficient cloud-based payment security solutions to organisations operating on a global scale.

PCI Pal has offices in London, Ipswich (UK) and Charlotte NC (USA). For more information visit www.pcipal.com or follow the team on Twitter @PCIPAL