PRESS RELEASE
17 September 2019

Global research shows poor data security practices have serious consequences for businesses worldwide

PCI Pal research finds a significant change in how consumers around the world are thinking about and reacting to security breaches

According to newly released research conducted by PCI Pal®, the secure payments provider to contact centres, 44% of Americans, 38% of Brits, 33% of Australians, and 37% of Canadians have been the victim of a data breach.

As a result of the influx in cybercrime, consumers are increasingly aware that they are in no way exempt from data breaches, especially as more people are forced to resolve the short and long term damages caused by an organisation's weak data privacy practices. In response, consumers around the world are prioritising security and leveraging their spending power to hold businesses accountable:

- In the UK, 44% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and 41% of consumers claim they will never return to a business post-breach.
- In the US, 83% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and over a fifth (21%) of consumers claim they will never return to a business post-breach.
- In Australia, 43% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and 43% of consumers claim they will never return to a business post-breach.
- In Canada, 58% of consumers claim they will stop spending with a business for several months in the immediate aftermath of a security breach, and a fifth of consumers claim they will never return to a business post-breach.

Whether it's adjusting how much they spend or deciding to avoid the company altogether for several months or even forever, these figures represent significant potential revenue loss that many businesses may not be able to recover from.

The findings suggest that a combination of recent high-profile data breaches in each region, the development of assorted laws and regulations to protect consumer data privacy (e.g. Europe's General Data Protection Regulations, the California Consumer Privacy Act, Canada's Personal Information Protection and Electronic Documents Act, Australia's Consumer Data Right, and others), and personal experience have made security top-of-mind for consumers around the world.

The consumer-facing consequences of a data breach have resulted in consumers reconsidering the safety of common business practices in obtaining data. Consumers in every region expressed concerns about having to read their credit card information over the phone, and many are only comfortable sharing information over the phone with certain companies that they trust:

- In the UK, 55% of consumers are uncomfortable reading their credit card information over the phone and 44% of consumers are only comfortable sharing information over the phone to select companies that have earned their explicit trust.
- In the US, over 40% of consumers are uncomfortable reading their credit card information over the phone and 58% of consumers are only comfortable sharing information over the phone to select companies that have earned their explicit trust.
- In Australia, 49% of consumers are uncomfortable reading their credit card information over the phone and 43% of consumers are only comfortable sharing information over the phone to select companies that have earned their explicit trust.
- In Canada, 42% of consumers are uncomfortable reading their credit card information over the phone and 58% of consumers are only comfortable sharing information over the phone to select companies that have earned their explicit trust.

Consumers also report that when it comes to trust in security practices, not all industries are created equal. The results showed that consumers trusted the retail and travel industries least, with 40% and 35% of UK consumers, 50% and 40% of Australian consumers, 65% and 41% of Canadian consumers , and 19% and 16.4% of US consumers rating these industries as the worst when it comes to security practices.

"With the ongoing introduction of new data privacy regulations around the world, companies face significant fines in the event of a breach," said James Barham, CEO at PCI Pal. "Our research however shows they may face an even bigger financial consequence in the aftermath of a breach, with the loss of customer loyalty and trust. To avoid such implications, companies should adequately prepare themselves for the increasing likelihood that a data breach will inevitably occur."

For more information and to learn how PCI Pal can help protect your company against data breaches, download the global eBook here.

For more information on PCI Pal visit www.pcipal.com, call +44 207 030 3770 or follow PCI Pal on Twitter.

ends

Notes to Editors:

About PCI Pal PLC
PCI Pal is the 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 card payment 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 are simple and light-touch, ensuring no degradation of service while achieving security and compliance.

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: https://twitter.com/PCIPAL

Editor's Contact:
Peppa Sheridan
Peptalk Communications
+ 44 (0)1787 313822
peppa@peptalkpr.co.uk