pixxles

WHY PCI DSS IS MORE IMPORTANT THAN EVER FOR ECOMMERCE MERCHANTS

WHAT IS PCI DSS?

The **Payment Card Industry Data Security Standard** (PCI DSS) is a set of data security standards to help combat fraud to better ensure secure card transactions and data management.

WHY HAS IT DEVELOPED?

DECEMBER 2004
Inception of PCI DSS

JUNE 2005
New requirements for merchants

- Merchants processing **20,000 transactions per year** are required to be PCI DSS-compliant.

2006
Payment Card Industry (PCI) Security Standard Council founded

- Founding members – Mastercard, Visa, American Express, JCB International and Discover Financial Services – govern and execute the Council's work.
- More than **94 million credit and debit card numbers are stolen** over the course of 18 months due to a data breach that was discovered in December 2006, later resulting in a **$40.9 million fine**.

(Source: CNN, BankInfoSecurity)

2008
PCI DSS enforced

- Credit and debit card data for more than **134 million people** is stolen due to a data breach that went undetected for 8 months.
- Record data breach results in **$140 million in fines and penalties**.

(Source: CSO Online)

OCTOBER 2010
PCI DSS 2.0 is introduced

- Further clarifications and guidance for merchants around the requirements for protecting cardholder data.

AUGUST 2012
Compliance reaches record levels

- **Visa** reports that **97% of level 1 merchants** have achieved compliance.

(Source: VISA 2012 Annual Report)

NOVEMBER 2013
PCI DSS 3.0 is introduced

- Updates and new requirements for data security, including new requirements such as mandatory penetration testing.

SEPTEMBER 2018
Full PCI DSS compliance drops for the first time in 6 years

- A drop in compliance rates in 2017 ends the annual growth in compliance seen during 2012 – 2016.

(Source: Verizon 2019 Payment Security Report)

MARCH 2019
PCI DSS v4.0 is announced

- The PCI Security Standards Council (SSC) announces that industry feedback will help shape this latest version with completion planned for **mid-2021**.

WHAT IS PCI DSS v4.0?

PCI DSS v4.0 will consist of 4 key high-level goals:

- Ensure the standard continues to meet the security needs of the payments industry.
- Add flexibility and support of additional methodologies to achieve security.
- Promote security as a continuous process.
- Enhance validation methods and procedures

(Source: PCI Security Standards Council)

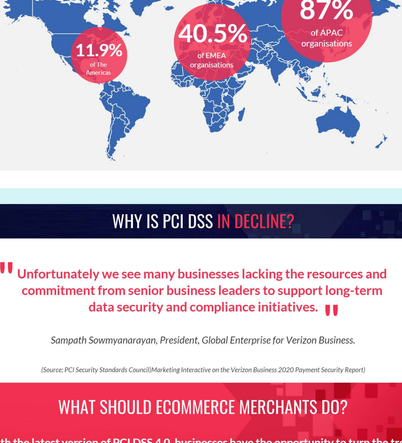
WHY IS IT SO IMPORTANT TO THE CURRENT STATE OF COMPLIANCE?

Recent years have presented a downward trend in PCI DSS compliance:

2019 saw only 27.9% of organisations globally meeting all of the PCI DSS requirements. This marks a 27.5% drop in compliance since 2016.

(Source: Verizon 2020 Payment Security Report)

Organisations that are most likely to maintain full compliance by region:



WHY IS PCI DSS IN DECLINE?

> "Unfortunately we see many businesses lacking the resources and commitment from senior business leaders to support long-term data security and compliance initiatives."

Sampath Sowmyanarayan, President, Global Enterprise for Verizon Business.

(Source: PCI Security Standards Council/Marketing Interactive on the Verizon Business 2020 Payment Security Report)

WHAT SHOULD ECOMMERCE MERCHANTS DO?

With the latest version of PCI DSS 4.0, businesses have the opportunity to turn the trend:

- Contact your payment processing partner to ensure you are PCI DSS compliant
- Get started at: https://www.pcisecuritystandards.org/pci_security/