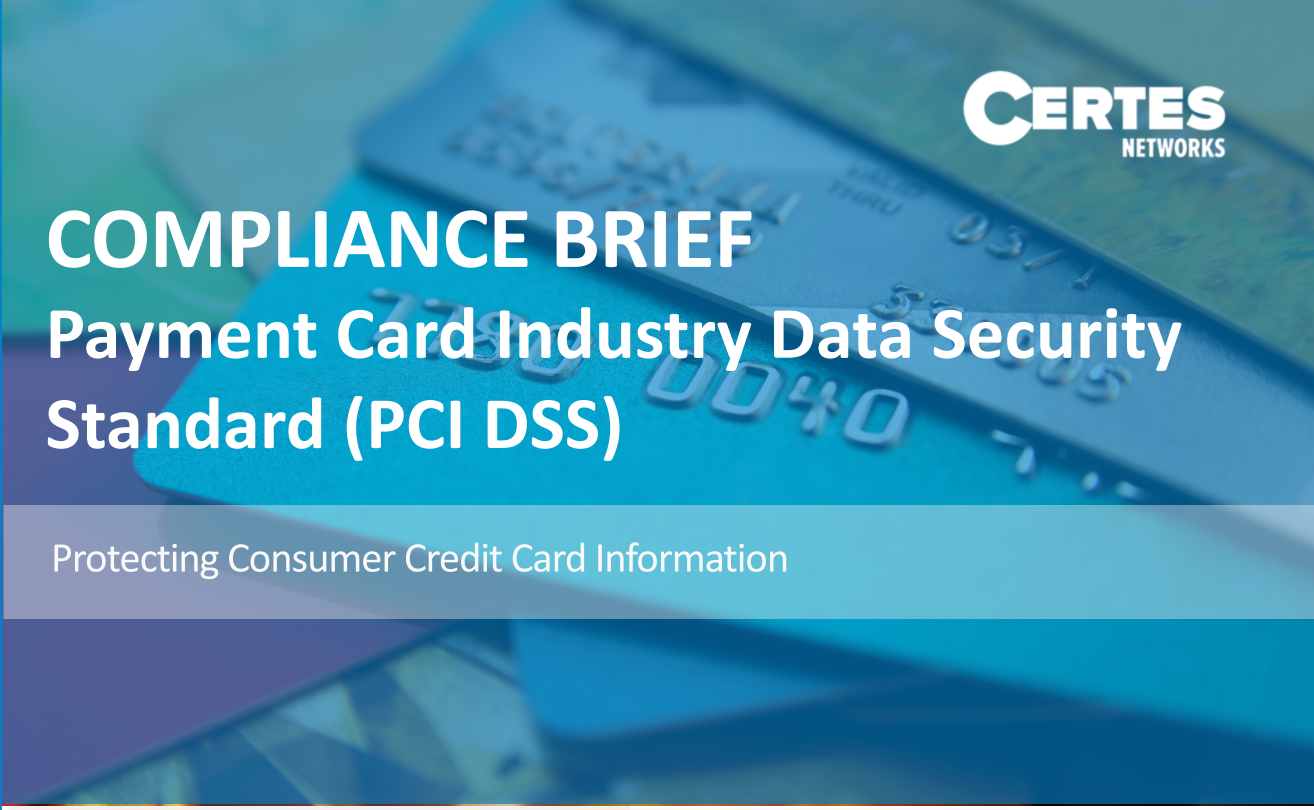

CERTES NETWORKS

COMPLIANCE BRIEF

Payment Card Industry Data Security Standard (PCI DSS)

Protecting Consumer Credit Card Information

What is the PCI and Why It's Important

Developed by the major credit card issuers, the Payment Card Industry Data Security Standard (PCI DSS) outlines best practices for credit card data storage, processing and transmission. Its intent is to protect credit card information from fraud, theft, or any other breach.

Any retailer, merchant, bank or service provider storing, processing or transmitting cardholder data must comply with PCI DSS. Compliance validation is required for major merchants and may be required for some smaller merchants. Failure to comply with PCI DSS could result in fines that are severe enough to put you out of business.

WHAT DO YOU NEED TO KNOW?

There are twelve specific requirements that can be grouped into six main categories which retailers must meet to comply with PCI DSS:

Build and maintain a secure network:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect cardholder data:

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program:

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement strong access control measures:

7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly monitor and test networks:

10. Track and monitor access to network resources and cardholder dat.
11. Regularly test security systems and processes

Maintain an information security policy:

12. Maintain a policy that addresses information security for all personnel.

CIVIL PENALTES

If a merchant experiences a security breach and is found to be non-compliant with PCI rules, they may be subject to fines. Merchants might have to pay anywhere from $5,000 to $100,000 every month until they address all compliance issues.

WHAT SHOULD YOU DO NEXT?

In order to comply with PCI DSS, companies must meet all 12 requirements mentioned above. Essentially, protecting cardholder information and processing IT infrastructure are the two main points of PCI DSS.

To protect cardholder information, companies must protect the data wherever it travels, specifically encrypting it over public networks. In addition to encryption, companies must put into place IT security controls to protect the cardholder's data from hackers and other cybercriminals who want to steal the information.

To protect IT infrastructure, merchants must protect both systems and applications. In addition, they must establish control processes and guidelines to secure computers and other electronic equipment.

A copy of the CCPA can be found here:
https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com

We offer an encryption solution that is simple, scalable and uncomplicated.