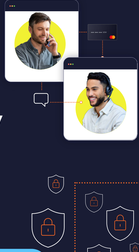
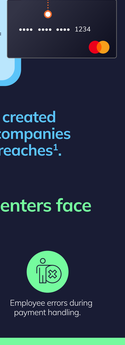
PCI DSS 101: What your contact center needs to know today



1. What is PCI DSS?

PCI DSS sets the global security standard for protecting payment card data. Compliance is mandatory for all organizations handling cardholder information.



Key facts:

12 requirements for data security.

Focus: protect data during storage, transmission, and processing.

Non-compliance = fines up to **$500k/month**

The PCI DSS standard was created in 2004 by major credit card companies to combat fraud and data breaches[1].

2. Challenges that contact centers face

Common compliance challenges:

Multi-channel complexity (e.g. voice, chat, email).

Legacy systems lacking security features.

Employee errors during payment handling.

Impact of non-compliance:

Data breaches result in loss of trust and revenue.

Operational downtime from system fixes.

Regulatory fines of up to $500,000 per month.

60% of customers avoid working with the company after a data breach[2].

3. The 12 PCI DSS requirements

The requirements are grouped into **six key areas**:

1. Build and maintain a secure network
- Install and maintain a firewall
- Avoid using vendor-supplied passwords

2. Protect cardholder data
- Encrypt stored data
- Encrypt data during transmission

6. Maintain a security policy
- Maintain an information security policy

3. Maintain vulnerability management
- Use and regularly update anti-virus software
- Develop secure systems and applications

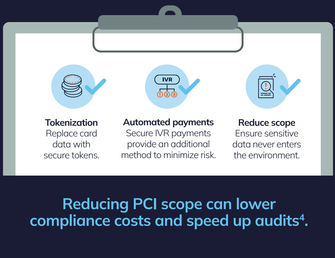
5. Regularly monitor and test networks
- Track and monitor access to network resources
- Regularly test security systems

4. Implement strong access control
- Restrict access to cardholder data
- Assign unique IDs for access
- Restrict physical access to data

New PCI DSS V4.0.1 updates introduce stronger authentication requirements and expanded encryption guidelines[3].

4. Simplifying compliance

Top strategies for simplification:



Tokenization
Replace card data with secure tokens.

Automated payments
Secure IVR payments provide an additional method to minimize risk.

Reduce scope
Ensure sensitive data never enters the environment.

Reducing PCI scope can lower compliance costs and speed up audits[4].

5. The cost of non-compliance

Ignoring compliance can lead to:

Reputation damage:
60% of customers avoid brands that suffer a breach. Trust is hard to earn, and easy to lose.

Legal and regulatory fallout:
Non-compliance can trigger audits, fines and even litigation, particularly under PCI DSS and GDPR.

Long-term impact:
Recovery isn't just about patching systems. Businesses face costly infrastructure overhauls, prolonged reputational repair, investor distrust and potential stock price dips.



The most common cause of a payment data breach is human error[5].

6. How PCI Pal helps

PCI Pal makes compliance easy with:

Secure payment solutions for all channels.

Real-time data protection.

Seamless integration with your existing systems.



PCI Pal's cloud-based solutions allow contact centers to remain compliant without storing sensitive card data[6].

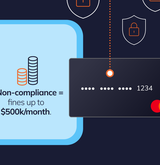
Get started today

Ready to secure your contact center?

Partner with PCI Pal for expert guidance and the right tools for a superior payment experience.

Get in touch

For more information on how to master PCI DSS compliance in your contact center, check out our handy guide.



Sources: [1] A Quick Intro to PCI DSS (Payment Card Industry Data Security Standard). [2] 60 Percent of Small Companies Close Within 6 Months of Being Hacked. [3] What's New in PCI DSS 4.0? Key Updates Explained. [4] Instilling trust and ensuring full PCI DSS compliance. [5] 95% of Data Breaches Tied to Human Error in 2024. [6] Instilling trust and ensuring full PCI DSS compliance.