



# Simplify PCI DSS Compliance and Protect Customer Payment Data

**Are you doing enough to protect your customers' credit card information?**

Struggling to comply with payment card companies' data security rules? Fewer than 30% of companies fully comply with the Payment Card Industry Data Security Standard (PCI DSS). Learn about PCI DSS and how the PaperVision® product suite helps with compliance, minimizes the risk of costly data breaches and improves overall business efficiency. Compliance doesn't have to be so hard and cost so much!



## PCI Security Standards:

Major credit card companies put in place the first cardholder data security standards in 2004. Of the 15 PCI Security Standards in place today, nine of them apply directly to merchants. The remaining standards apply to the cardholder's and merchant's banks.

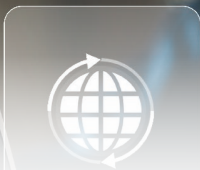
The detailed requirements are complex and, recognizing this, the PCI Security Standards Council offers a simpler list of "Six Milestones for Prioritizing PCI DSS Compliance Efforts":

1. Do not store sensitive authentication data, and limit cardholder data retention.
2. Protect systems and networks and be prepared to respond to a system breach.
3. Secure payment applications.
4. Monitor and control access to your systems.
5. Protect stored cardholder data.
6. Complete remaining compliance efforts and ensure all controls are in place.

"A concerning issue has arisen for the payment processing industry in recent years, one that could have serious ramifications for both consumers and businesses alike. The amount of security threats facing users is increasing by the day, yet the number of organizations complying with industry security standards continues to fall."

-Mark Vojtko, Contributor, Hashed Out





# Improve Overall Business Operations with PaperVision®

What if you could comply with payment card data security standards while reducing the amount of time and money you spend to securely store, share and manage your customers' important information. The PaperVision product suite secures data, simplifies information management and improves the productivity of your business.

## Enable PCI DSS Compliance

Noncompliance with PCI data security standards puts your company at risk of fines and recurring audits.

The PaperVision product suite offers data encryption and other advanced security features to help you comply with all government, legal and industry regulations that govern customers' personal information, including credit card data.

## Improve Customer Experience

When customers know a company keeps their card data and other personal information safe, they are inclined to purchase from that company, which in turn strengthens the company's reputation. The PaperVision product suite safeguards customer information and lets you retrieve customer data fast to respond quickly to customer questions.

## Protect Information Using Advanced Security

Key elements of PCI DSS compliance include data encryption, hidden account numbers and secure information transmission and storage, which the PaperVision product suite provides. In addition, access rights to information are verified each time a request is made to prevent unauthorized access and disclosures of sensitive information.

## Avoid Costly Noncompliance Penalties

Credit card issuers can impose severe penalties for noncompliance with PCI DSS. Penalties can include hefty fines and loss of the ability to process any card payments. The PaperVision product suite improves your compliance reporting with enhanced 24x7 user tracking, user activity logs and audit trails.

## Save Time and Money

Looking to be a good steward of your company's operating funds? The money-saving benefits of the PaperVision product suite include minimal to no capital investment and IT costs. In addition, you'll enjoy ironclad document and data security, and save on staff time, file storage and regulatory penalties.

"No one wants to use a credit card at an organization where the customer thinks they cannot protect their data, and it all mushrooms from that initial security breach."

-John Ramsey, Senior Product Manager, MegaPath

