MASTER SMALL BUSINESS SECURITY

PROTECT YOUR BUSINESS AGAINST PAYMENT CARD FRAUD

Fraud Protection & PCI compliance is more important than ever. Attackers are increasingly going after small businesses, trolling for loopholes and 'quick wins' where systems or individual employees haven't kept up with the technology. Mastercard and other payment card networks see firsthand how fraud is perpetrated and they've developed the best practices to guide businesses in beating payment card fraud. It's important to become PCI compliant and remain in compliance to reduce your likelihood of a costly compromise.

The PCI Data Security Standard (PCI DSS) is the primary security standard put forth by the PCI Security Standards Council (PCI SSC), a global forum made up of five payment card brands to ensure the security of cardholder data. PCI Compliance means being compliant with the PCI DSS and applies to any entity, regardless of size, that stores, processes or transmits cardholder data.

Benefits of PCI Compliance

- Safeguard your business reputation
- Avoid costly assessments from banks and card brands
- Increase customer confidence
- Reduce risk of account data compromise

Technology and expertise provide practical and immediate solutions. When small businesses fail to correctly configure the remote access technologies used in their point-of-sale (POS) applications, they provide the most common opening fraudsters are looking for. To reduce your risk of a costly Account Data Compromise (ADC)[1], you should:

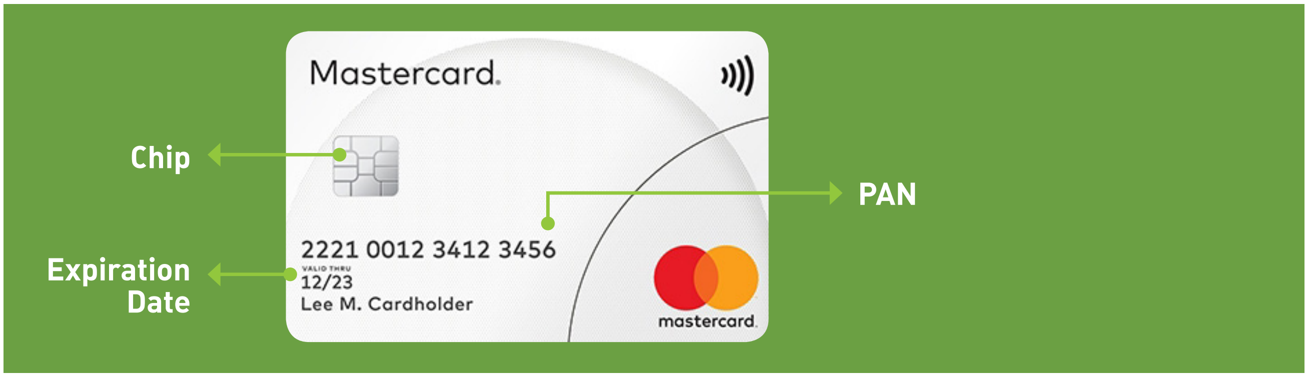
- Follow the PCI standard.
- Only use approved PIN entry devices and validated payment software at your POS and/or website shopping cart.
- Set strong passwords and be sure to change default passwords on hardware and software—most are unsafe!
- Use a firewall on your network and PCs.
- Never store ANY sensitive cardholder data after authorization.
- Make sure your wireless router is password-protected and uses strong encryption.
- Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or "skimming" devices.
- Teach your employees about security and protecting cardholder data.
- Use two-factor authentication for remote access, in accordance with PCI DSS requirements.

[1] An Account Data Compromise (ADC) event is an occurrence that results—either directly or indirectly—in the unauthorized access to, or disclosure of, cardholder data.

WHAT CARDHOLDER DATA CAN I STORE?

	Data Element	Storage Permitted	Render Stored Account Data Unreadable per Req. 3.4
CARDHOLDER DATA	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	Yes
	Service Code	Yes	Yes
	Expiration Date	Yes	Yes
SENSITIVE AUTHENTICATION DATA	Full Magnetic Stripe Data	No	Cannot store per Req. 3.2
	CAV2/CVC2/CVV2/CID	No	Cannot store per Req. 3.2
	PIN/PIN Block	No	Cannot store per Req. 3.2

TYPES OF DATA ON A PAYMENT CARD



HOW CAN I FIND OUT MORE ABOUT PCI?

PCI Security Standards Council:
www.pcisecuritystandards.org

- Attestation of Compliance (AOC)
- Self Assessment Questionnaire (SAQ)
- PCI Security Standards
- List of Qualified Security Assessors (QSA)
- List of Approved Scanning Vendors (ASV)
- List of Payment Application Qualified Security Assessors (PA-QSA)
- Lists of Approved Payment Applications and Approved POS devices

PCI Education Opportunities:
www.mastercard.com/pci360

- Complimentary PCI webinars, podcasts and white papers
- Email questions to: pci_education@mastercard.com

SDP Program Resources and Compliance Information: www.mastercard.com/sdp

- Merchant and service provider levels defined
- When to contact your acquiring bank
- Access to SDP forms and education resources
- PCI Compliant Service Provider List
- Email questions to: sdp@mastercard.com

Other: www.mastercard.com/arm

- Access to Mastercard Academy of Risk Management conferences and educational resources