Prepare your business for new PCI DSS requirements

DON'T do business WITHOUT IT™

Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 will be retired on March 31, 2024. The PCI DSS v4.0 requirements are a best practice until March 31, 2025, after which they will be required. To help safeguard payment card data and protect you and your customers, here's what you need to know.

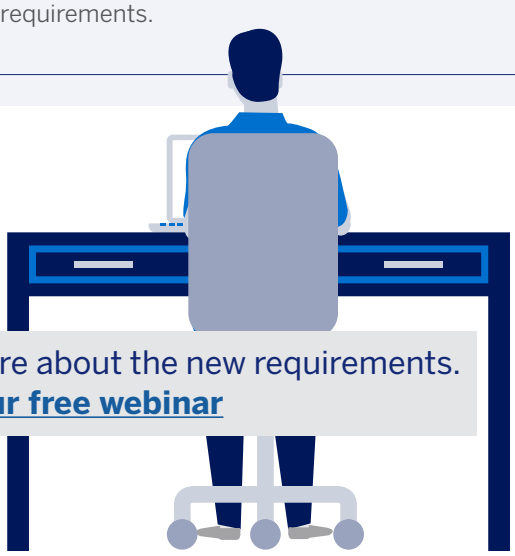
How the updated standard affect your business

REQUIREMENT/RATIONALE	WHAT YOU MUST DO	HOW YOU CAN PREPARE
Approved Scanning Vendor (ASV) Vulnerable websites create opportunities for data thieves to steal Card data from your site, even when you don't capture or save the information.	Perform and pass an external vulnerability scan on your ecommerce site at least every three months by a PCI SSC Approved Scanning Vendor.	Engage an ASV to start conducting external vulnerability scans on your ecommerce site. **Helpful resource:** PCI Security Standards Council Approved Scanning Vendors.
Page Scripts Authorization Protecting the integrity of your payment page helps to protect your customers' Card data from theft.	Inventory all payment page scripts loaded and executed in the consumer's browser.	Work with your web developer to create a baseline of scripts loaded and executed in the consumer's browser from your payment page. Be sure to document each script, its use and authorized users.
Payment Page Monitoring Systematic monitoring of changes to payment page scripts may help you to identify unauthorized changes and quickly stop data theft from occurring.	Monitor your payment page for unauthorized changes to headers and active content at least once every seven days.	Identify and evaluate the cost, appropriateness and feasibility of possible solutions used to detect and report changes to payment page content loaded into the consumer's browser upon checkout.
Scope of Compliance from Service Provider Documenting who owns, implements and verifies your data security controls helps avoid inaccurate assumptions, which is foundational to preventing data theft.	Obtain clear documentation from your Service Provider of the PCI DSS requirements your services cover.	Consult with your Service Providers to understand and document the specific PCI DSS requirements their services help you meet. **Helpful info:** Self-Assessment Questionnaire (SAQ) versions A and A-EP help you evaluate the compliance of your ecommerce site with PCI DSS technical and operational requirements.

Other ways American Express is here to help you

Download these helpful resources to learn more about how to help protect your business:

- PCI DSS v4.0 Resource Hub
- Ransomware Protection
- Zero Day Vulnerability Guidance
- Target Analysis Program (TAP)



Learn more about the new requirements.
Watch our free webinar