Snapshot

Securing payments with PCI DSS v4.0 in an evolving retail industry

How to overcome the complexity of updated compliance requirements

Use of stolen credentials, ransomware and phishing continues to challenge the retail sector, with no clear relief in sight. Organizations that keep data security controls in place in accordance with industry security standards are more likely to prevent data breaches. Yet staying ahead of the latest threat-actor exploits is a constant challenge that already-overwhelmed chief information security officers (CISOs) and security managers face daily. Security professionals in the retail industry also must juggle the complexity of evolving payment technology, cloud computing, the increasing adoption of omnichannels, a rising number of payment card transactions and a widening attack surface. In the retail industry, a breach can be particularly damaging, resulting in lost customer confidence, bad press and declining profits.

Security trends in the retail industry

Social engineering attacks in the retail industry increased from 7% in 2016 to 29% in 2021, according to the 2022 Verizon Data Breach Investigations Report (DBIR).[1] Credentials, often used to hack into servers and load ransomware, are the top data type compromised in this industry, the DBIR found. Thieves are leveraging a range of new phishing tactics and "app data" malware that can capture credit cards being processed by web forms. The prevalence of "capture app data" as a malware enumeration is seven times higher in retail than in other industries, which explains why the 2022 DBIR ranks the System Intrusion Pattern as #1 in the industry.

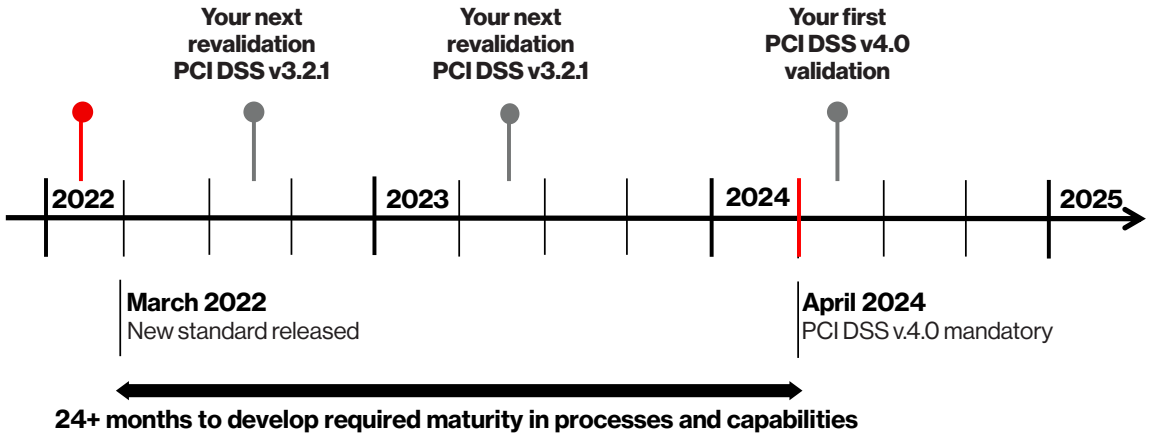
In response to these and other payment security changes, the Payment Card Industry Security Standards Council (PCI SSC) instituted a major rewrite of the PCI Data Security Standard (PCI DSS). The shift from PCI DSS v3.2.1 to PCI DSS v4.0 provides new navigation points to help organizations achieve sustainable effectiveness across control and compliance environments. It's the most significant update to the PCI DSS since its initial release in 2004.

The retail sector needs to pivot and adapt to the new PCI DSS v4.0 requirements just as quickly as other industries; the PCI DSS is applicable to all organizations. Retailers need to strictly implement security defenses to avoid becoming payment card data-breach victims. Additionally, retail needs a management strategy—a pragmatic "toolbox" of data security compliance management methods, with a clear instruction manual for building PCI DSS v4.0 success.

PCI DSS v4.0 still has the familiar six Control Objectives and 12 Key Requirements introduced in 2006. Its changes reflect the PCI SSC's goals for evolving objectives and requirements. The two most significant updates in PCI DSS v4.0 are an increased emphasis on continuous compliance and a new customized approach for compliance control design and validation. Enhanced validation methods and procedures have evolved from a defined-only approach to security control design, implementation and validation to also include an objective-based, customized approach option.

verizon business

PCI DSS v4.0



Payment card data is one of the most sought-after data types by external and internal threat actors, because it's one of the easiest types to monetize.

The defined approach simply means that organizations follow the familiar (traditional) requirements and testing procedures, as written in the PCI DSS. The new customized approach of validating controls allows organizations to follow a tailored process, where they can custom design security controls or adopt other controls outside of the list of defined controls. This is an outcome-based approach rather than a must-implement-based approach. All customized controls must still meet the stated security objective of the requirement.

Compliance with PCI DSS v4.0 will not be required until March 2024. PCI DSS v3.2.1 will remain active for 18 months after all PCI DSS v4.0 materials are released. When this transition period ends, PCI DSS v3.2.1 will be retired, and PCI DSS v4.0 will become the only active version against which compliance can be formally validated. In addition to the 18-month period when PCI DSS v3.2.1 and PCI DSS v4.0 will both be active, there will be an extra period of time for phasing in new requirements that are identified as "future dated" in PCI DSS v4.0. Organizations working to upgrade their compliance environments may think they have ample time to resituate their controls. But with significant changes, including the customized approach option, they can't start to prepare soon enough.[2]

A Verizon management toolbox to help the retail sector transition to PCI DSS v4.0

Many approaches exist for designing and executing the management of a compliance program. The key question is: Which is the most effective and efficient? In 2021, Verizon explained a method for reaching that goal in the 2021 Payment Security Report insights: PCI DSS v4.0 white paper.[3]

Verizon has an exceptional track record of helping clients implement sustainable payment security frameworks. The theme of the recently released 2022 Payment Security Report (PSR) is about preparing to successfully navigate PCI DSS v4.0: how to apply the methods you'll need to identify and solve potential challenges, and how to choose the best path forward to determine and accomplish your goals. It explores a collection of management methods, models and frameworks to help your organization simplify the complexities of payment security while adapting to the new requirements.

Verizon services

Verizon also offers many services designed to help you focus on and navigate the transition to PCI DSS v4.0. This sequence of services offers a structured roadmap to achieving compliance. It helps organizations reduce uncertainty and is particularly valuable for those that don't have a high level of maturity with their security and compliance management processes. Each service helps organizations become more proactive instead of reactive to the new compliance requirements.

Significant PCI DSS v4.0 requirement changes

Number of new requirements: 74

New requirements for service providers: 12

New requirements for merchants: 62

Changes in Requirements 1, 3, 5, 8, 9, 12

Among the changes:

- **Disk- or partition-level encryption is no longer enough**
- **An anti-phishing solution is required**
- **A web application firewall (WAF) is required**
- **Multifactor authentication (MFA) is required**
- **A cryptographic key is required for stored hash values**
- **Certificates protecting cardholder data (CHD) need to be signed by a valid certificate authority (CA)**
- **Enforced intregrity controls for payment page scripts are required**
- **No hardcoded passwords are allowed for applications**
- **Authenticated vulnerability scans are required**
- **Application/System account passwords must expire**

Service 1: Interpretation of the PCI DSS v4.0

This service is designed to help clients develop a structured approach to understanding the PCI DSS. It includes a framework to help clients communicate the Standard to their organizations across teams, including:

- Frontline staff
- Risk and compliance teams
- Internal audit teams and senior management
- External parties and vendors

It includes presentations and guidance on:

Why: Goals and objectives, outcomes, and expectations of PCI DSS v4.0

How: Guidance (hard-copy workbooks or support for developing e-learning/online)

Who: Targeted messaging for each of the stakeholder groups (internal and external)

When: Recommendations on the steps and order of when to start each communication and its duration

Service 2: PCI DSS v4.0 Resource Requirements Assessment

The Resource Requirements Assessment service provides an integrated analysis of the scope, requirements and constraints imposed on the customer by the new PCI DSS standard. The analysis focuses on identification and classification of the impact that PCI DSS requirements have on the organization and the main remediation action for each new or updated requirement. It includes (1) formalization/documentation, (2) process changes, (3) configuration changes, (4) architecture changes, (5) culture changes and (6) business model changes. The service is delivered in about two weeks in a series of interviews with security and compliance teams. It results in an analysis that allows for the calculation of work hours required to achieve PCI DSS v4.0 project objectives.

Service 3: PCI DSS v4.0 Gap Assessment

The Gap Assessment pinpoints the gap between your current payment security systems and processes and PCI DSS v4.0 requirements (present vs future reality). It results in a report that details the PCI DSS requirements and controls that need remediation and includes a focus on the type and quality of evidence needed to be submitted during the formal compliance validation. Verizon also offers a differential gap assessment to identify only the gaps between PCI DSS v3.2.1 and PCI DSS v4.0 requirements.

Service 4: PCI DSS v4.0 Preassessment

The PCI DSS v4.0 Preassessment reviews a sample of compliance evidence and assessment preparedness to determine readiness for the formal assessment. It checks the readiness of security and compliance teams to participate in the formal validation assessment and includes a last-minute check to confirm the adequacy of compliance evidence, pinpointing any adjustments or corrections needed in advance of the formal assessment.

Service 5: Formal PCI DSS v4.0 Compliance Validation Assessment

This assessment is the formal, annual compliance validation against all applicable PCI DSS v4.0 requirements. It results in a Report on Compliance (ROC) and Attestation on Compliance (AOC).

Why Verizon

As an industry thought leader, we've written the book on PCI security compliance—literally. Since 2010, we've regularly published the Verizon Payment Security Report, a report dedicated to payment security issues and the only one of its kind to offer unique insights into the state of PCI DSS compliance. Verizon has one of the largest PCI Security Qualified Security Assessor (QSA) teams in the world and has conducted more than 20,000 security assessments for companies of all sizes, including many Fortune 500 and multinational organizations. We keep up with the rapidly changing nature of cyberthreats by analyzing more than 1 million security events every day at our global Network Operations Centers and Security Operations centers. For over a decade, we've offered our knowledge through thought leadership with publications such as the Verizon Data Breach Investigations Report.

Learn more:

For more information on the Verizon PCI DSS Assessment, contact your Verizon Business Account Representative or visit verizon.com/business/products/security/cyber-risk-management/governance-risk-compliance/payment-card-industry-data-security-standard-assessment/

Read the latest Payment Security Report: verizon.com/paymentsecurityreport

Read our 2021 Payment Security Report insights: PCI DSS v4.0 white paper: verizon.com/business/verizonpartnersolutions/business/resources/whitepapers/payment-security-report-insights.pdf

For more information about the other security solutions and services we offer, visit verizon.com/business/products/security/

verizon business

1 2022 Verizon Data Breach Investigations Report, 2022. https://www.verizon.com/business/solutions/secure-your-business/business-security-tips/

2 Verizon 2022 Payment Security Report, 2022. https://www.verizon.com/business/reports/payment-security-report/

3 Verizon 2021 Payment Security Report insights: PCI DSS v4.0 white paper, 2021. https://www.verizon.com/business/verizonpartnersolutions/business/resources/whitepapers/payment-security-report-insights.pdf