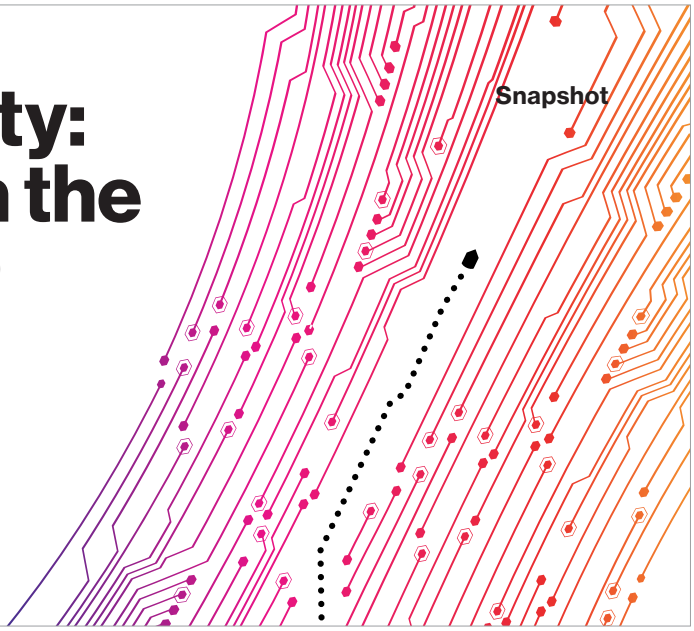
Travel and hospitality: Payment security in the era of PCI DSS v4.0



The travel and hospitality sector has always been a target for cybercriminals looking to carry out credit card fraud and identity theft. Those concerns escalated during the COVID-19 pandemic when payment practices shifted quickly to contactless and online.

Adding to the challenge is the complex ownership structure, which involves management companies as well as separate owners and franchises that are often interlinked but at the same time siloed. That structure can make personally identifiable information (PII) easier to steal because data can be stored in and transferred to multiple places. The sector is particularly vulnerable to stolen credentials, ransomware and phishing.

In response to these and other payment security changes and challenges, the Payment Card Industry Security Standards Council (PCI SSC) instituted a major rewrite of the PCI Data Security Standard (DSS). PCI DSS v4.0 is designed to help organizations better protect data, create flexible security methods and effectively navigate complex compliance environments.

It is the most significant update to the DSS since its initial release in 2004. The card brands (Visa, Mastercard, American Express, Discover and JCB) created the PCI DSS to ensure that businesses storing, processing or transmitting payment card data meet a baseline of security control requirements. Fines for noncompliance can be costly, ranging from $5,000 to $500,000 a month.

Travel and hospitality businesses need to strictly implement security defenses to avoid becoming data breach victims. Additionally, they should have a management strategy that includes a vision for the industry's special concerns and a toolbox with a clear instruction manual. Past privacy breaches in this industry have accentuated the need for a vision that addresses goals, requirements and constraints.

Security tips specific for the travel and hospitality sector

- High turnover rates due to seasonal work create more challenges, so limit access to sensitive data with multifactor authentication accessible only to trusted employees
- Have a continuous cybersecurity training program that instructs all relevant employees on securely handling sensitive data
- Add strict permissioning to lock down sensitive data sharing, which is particularly important with exported data from internal systems and reservations data accessible by many employees
- Restrict information on customer preferences and behavior—lucrative data in the right markets
- Many applications run on smartphones and tablets that access data outside a trusted network, so put processes in place beyond traditional firewalls to address the shift to cloud-based software
- Create an easily accessible, detailed response plan in the event of a data breach
- Do not share internal data through insecure channels, such as email or unsanctioned cloud software

verizon

What is new in PCI DSS v4.0

PCI DSS v4.0 still has the familiar Control Objectives and 12 Key Requirements introduced in 2006. The two most significant updates are 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 include an objective-based, customized-approach option.

The defined approach simply means that organizations follow the traditional requirements and testing procedures as written in the PCI DSS. The new, customized approach allows organizations to follow a tailored process, where they can custom design security controls or adopt other controls outside 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.

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. Even within these highly sensitive environments, organizations are slow to implement strategies that result in sustainable control effectiveness.

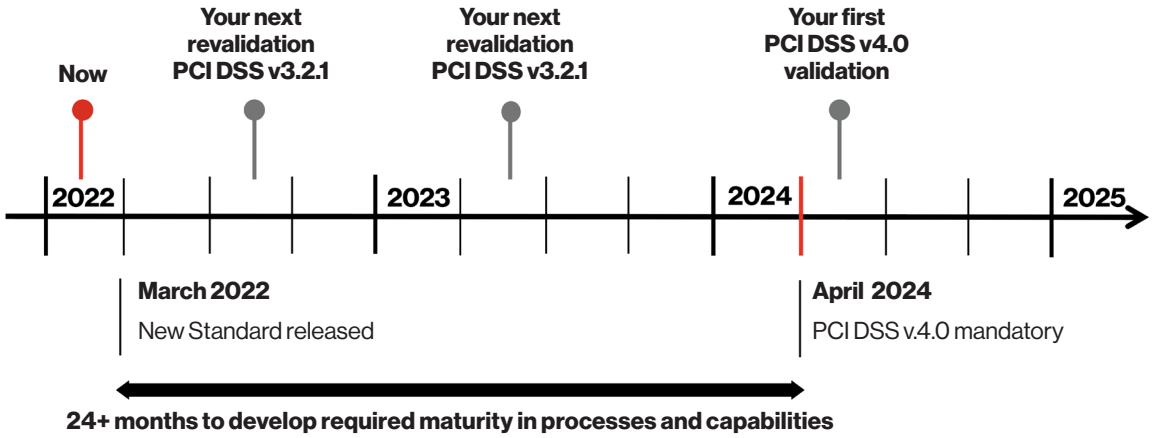
Travel and hospitality sector PCI DSS compliance challenges

Long-term PCI DSS compliance trends for this industry indicate that its main challenges are hardening and testing the security control environment. This requires travel and hospitality businesses to develop the organizational capabilities to design, implement, maintain and improve security testing, system hardening, protection of data in transit and physical security—all as integrated processes within the larger security control environment.

Compliance with PCI DSS v4.0 will not be required until March 2024. PCI DSS v3.2.1 will be active for 18 months after all PCI DSS v4.0 materials are released. 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.[1]

PCI DSS v4.0



Our toolbox for the travel and hospitality sector's transition to PCI DSS v4.0

Many approaches exist for designing the management of a compliance program. The key question is: "Which is the most effective and efficient?" Verizon explained a method for reaching that goal in the "2021 Payment Security Report insights: PCI DSS v4.0" white paper.[2]

Verizon has an exceptional track record for helping clients implement sustainable payment security frameworks. Our recently released 2022 Payment Security Report (PSR) is about preparing to successfully negotiate PCI DSS v4.0. It discusses how to find the tools 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 toolbox of management methods, models and frameworks to help your organization simplify the complexities of payment security while adapting to the new requirements.

Ten significant PCI DSS v4.0 requirement 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 integrity controls for payment page scripts are required
- No hardcoded passwords for applications
- Authenticated vulnerability scans are required
- Application/System account passwords must expire

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. Each service helps organizations become more proactive instead of reactive to the new compliance requirements.

Service 1: Interpretation of 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, including front-line staff, risk and compliance teams, internal audit teams and senior management, and external parties and vendors.

Service 2: PCI DSS v4.0 Resource Requirement Assessment

This assessment provides an integrated analysis of the scope, requirements and constraints. The analysis focuses on: (1) formalization, (2) process, (3) configuration, (4) architecture, (5) culture and (6) business model change. The service is delivered in about two weeks through a series of interviews with security and compliance teams and allows the customer to calculate work hours required to comply with PCI DSS v4.0 objectives.

Service 3: DSS v4.0 Gap Assessment

This service pinpoints the gap between your current PCI DSS v3.2.1 and PCI DSS v4.0 requirements. It results in a report that details the PCI DSS requirements and controls that need remediation, with a focus on the type and quality of evidence needed during the formal compliance validation.

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 and pinpoints any adjustments or corrections needed.

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

This 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 acclaimed Verizon Payment Security Report, a report dedicated to payment security issues and the only one of its kind to offer unique insights into the current state of PCI DSS compliance. Verizon has one of the largest PCI Security Qualified Security Assessor (QSA) teams in the world with deep experience and has conducted more than 19,000 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. And, 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 PCI DSS v4.0 insights" 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

1 Verizon 2022 Payment Security Report, 2022. verizon.com/business/resources/reports/2022-payment-security-report.pdf

2 Verizon 2021 Payment Security Report insights: PCI DSS 4.0 white paper, 2021. verizon.com/business/verizonpartnersolutions/business/resources/whitepapers/payment-security-report-insights.pdf