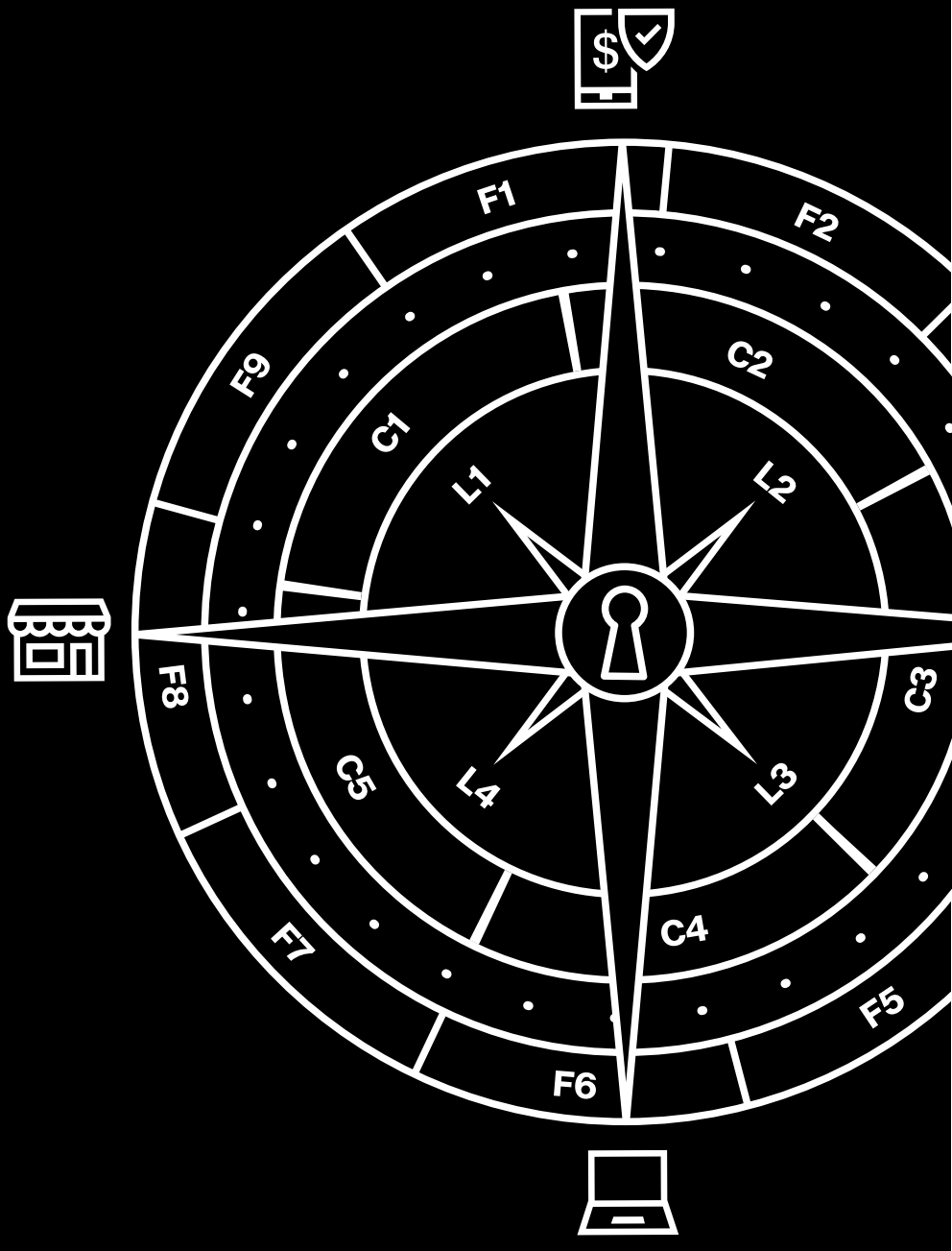
2019 Payment Security Report

Retail snapshot



verizon business ready

Retail has never been more competitive. To succeed, retail organizations must listen to their customers. And more than ever, data and privacy protection matter to retail customers.

Only 7% of customers would continue to use a company if it suffered a data breach, and 69% of customers would avoid a company that has suffered a data breach even if it offers a better deal than competitors.[1] This makes payment card security a crucial differentiator.

Consistently maintaining effective security controls to meet the Payment Card Industry Data Security Standard (PCI DSS) can help retail organizations earn customer trust and win a competitive advantage. But to accomplish this, data protection and compliance programs (DPCPs) must evolve and mature.

This is where Verizon's 2019 Payment Security Report (PSR) can help. The PSR reveals groundbreaking insights on payment card security trends to help professionals better understand their world. Our 2019 PSR also explains how new navigational tools—such as the Verizon 9-5-4 Compliance Program Performance Evaluation Framework—can help improve data protection and compliance.

Despite chip and PIN, retail data is still getting swiped.

Four years ago, retail data was most often compromised at the point of sale.[2] Since that time, Europay, Mastercard and Visa (EMV) technology has seemingly reduced the value proposition of card-present fraud, and data breaches are primarily occurring through web applications.[3] However, security breaches haven't been entirely eliminated. Retailers must still be vigilant about protecting card data.

In the 2019 PSR, we include more detailed data breach correlations from PCI forensic investigations (PFIs) performed by the Verizon Threat Research Advisory Center (VTRAC) | Investigative Response Team from 2016 to 2018. Data on long-term trends shows that retail suffered the largest percentage of confirmed data breaches compared to the other industries studied—hospitality, financial services and IT services.

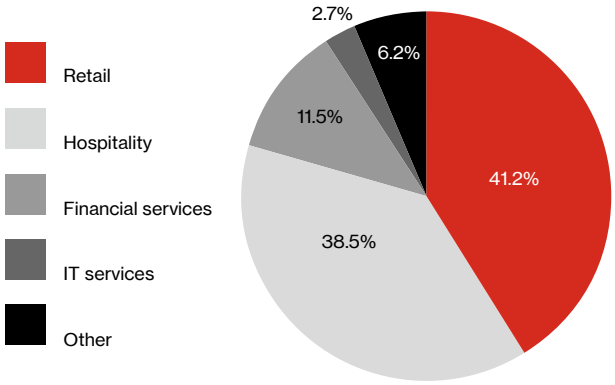


Figure 1. Confirmed data breaches by industry, six-year trend, Verizon PFI global caseload 2010–2016

Our data shows that mostly online retailers experience compromises. According to the Verizon 2019 Data Breach Investigations Report, bad actors compromise retail data for financial gain, fun and espionage. This includes personal information that can be stolen from reward programs.

Payment card security is vital—but not all businesses are in full compliance.

Fortunately, there are opportunities to strengthen payment card security. According to the approximately 55 organizations we surveyed for the 2018 PSR, 18% of organizations across all industries have no defined data protection and compliance program. None rated their DPCP maturity as optimized.

18%

of organizations across all industries have no defined data protection and compliance program. None rated their DPCP maturity as optimized.

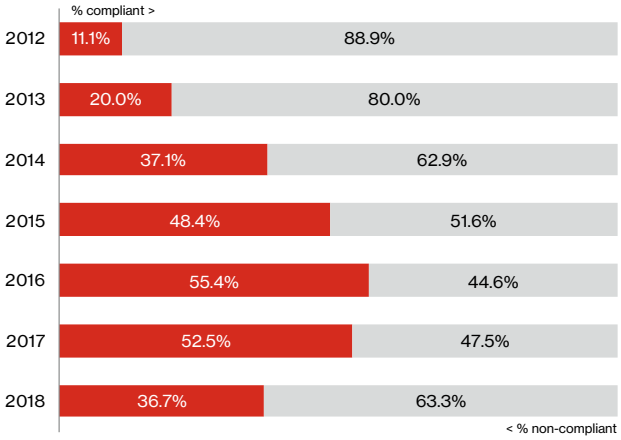


Figure 2. Full compliance by year

In the nine years that Verizon has been producing the PSR, we've seen full compliance with PCI DSS requirements improve annually until 2017, when our assessments measured a downturn in compliance two years in a row. Assessments from other Qualified Security Assessor (QSA) companies show a similar decline in full compliance with the standards.

What is PCI DSS?

Leading card brands set up the Payment Card Industry Data Security Standard to help businesses that take card payments reduce fraud. While PCI DSS is focused on protecting card data, it's built on solid security principles that apply to all kinds of data. It covers topics like retention policies, encryption, physical security, authentication and access control. For more information, visit pcisecuritystandards.org.

While the 2019 PSR shows that overall compliance fell, the control gap—representing how far organizations were from fully complying with PCI DSS requirements—remained consistent with the previous year at 7.2%. Looking at only the organizations that failed their interim compliance validation, the control gap moved in a good direction by decreasing 6.2 percentage points from last year to 10.2% in this year's report.

Organizations in the Asia-Pacific (APAC) region are showing a stronger ability to maintain full compliance with PCI DSS at 69.6%. Europe, the Middle East and Africa (EMEA) scored a 48.4% on full compliance, while fewer than one-quarter of all organizations in the Americas (20.4%) maintained full compliance.

Retail headed in the wrong direction

The 2019 PSR indicates that all industries experienced a drop in full compliance in meeting PCI DSS requirements. Retail's overall compliance with PCI DSS tumbled to 36.4% in this year's report, falling from 56.3% last year and 50.0% in the 2017 report.

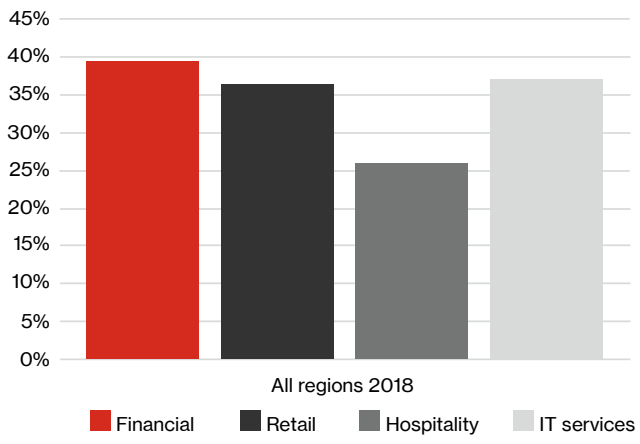


Figure 3. Global compliance by industry

Retail's compliance rate with PCI DSS this year was similar to IT services, better than hospitality (26.3% compliance) and behind financial services, which led the four industries studied at 39.0% compliance with PCI DSS.

The good

The 2019 PSR indicates that retail did a good job of encrypting data in transit (PCI DSS Requirement 4) and protecting against malicious software (Requirement 5). Retail outperformed other industries by decreasing its control gap in both cases and getting closer to complying with both requirements.

This industry also did fairly well at authenticating access (Requirement 8) to prevent data theft. Retail reduced the control gap and reported 70.5% full compliance with Requirement 8, ahead of both financial and IT services.

Retail showed marked success tracking and monitoring access to data (Requirement 10). The industry reported the highest full compliance across the four industries we examined (81.8%) in meeting this requirement.

The bad

Where retail fell short in meeting PCI DSS requirements was in using too many vendor-supplied defaults across in-scope components (Requirement 2). The control gap of how far it was from meeting full compliance was a substantial 12.4%.

Additionally, retail dropped significantly in complying with the requirement to have good security management (Requirement 12). The control gap declined 18.2 percentage points from last year's report to 56.8%.

The interesting

Retail scored the lowest of all industries studied in data breach incident preparedness. It struggled with many aspects of this, such as:

- Identifying users and ensuring that they had the right level of privileges (Control 10.2.5)
- Following due diligence when engaging service providers (Control 12.8.3)
- Detecting unauthorized wireless access points (Control 11.1.2)
- Maintaining an incident response (IR) plan (Control 12.10)

Recommendations

Change vendor defaults.

Replacing default passwords and avoiding other vendor-supplied defaults makes organizations more resistant to attacks. Organizations must make this a priority. The good news is that the skills to replace defaults are likely already in-house.

Invest in incident preparedness.

Cybersecurity incidents will likely occur. How an organization responds can make all the difference. Identifying potential security incidents, responding quickly and maintaining IR plans can give retailers a head start in investigations and damage control. For more on the benefits of IR and how to implement it, see the Verizon Incident Preparedness and Response (VIPR) Report.

Why is it important to meet PCI DSS requirements?

We've correlated PCI DSS compliance with organizations that experienced payment card data breaches since 2008, and we have never seen a record of any organization suffering a confirmed payment card data breach and being compliant across all 12 PCI DSS key requirements at the time of the data compromise.

Figure 4. A relational model of the 9 Factors of Control Effectiveness and Sustainability

Mature your compliance program.

Organizations don't deliberately fail to design good compliance programs. Developing program maturity is difficult. The right navigational guides, however, make it possible.

In the 2019 PSR, we provide the Verizon 9-5-4 Compliance Program Performance Evaluation Framework. It combines work from past PSR editions with additional guidance to create an integrated framework that can serve as a navigational aid to enhance a compliance program. The framework provides a new level of visibility and control to help businesses achieve repeatability, consistency and highly predictable outcomes that lead to data protection and compliance success.

Make payment security a part of securing your brand.

Retail's recent slide in PCI DSS compliance does not need to define your response to payment security. Despite retail's overall lackluster performance in the 2019 PSR, we still encountered compliant retail organizations. Building a mature compliance program can allow you to join these industry leaders and gain a competitive advantage by creating the trusted brand that customers seek.

Learn more:

To find out where to focus your security efforts and how to improve your compliance program, visit enterprise.verizon.com/resources/reports/payment-security/ or contact your Verizon representative.

verizon business ready

1 Data is from the 2019 Verizon report, "Winning the CX war: The risks and rewards of next-generation CX," and is based on online survey responses from 6,000 consumers in 15 countries, as well as qualitative interviews with customer experience (CX) experts. Longitude, a Financial Times Company, conducted the research. https://enterprise.verizon.com/resources/reports/2019/winning_the_cx_war.pdf

2 Verizon 2019 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/

3 Ibid.