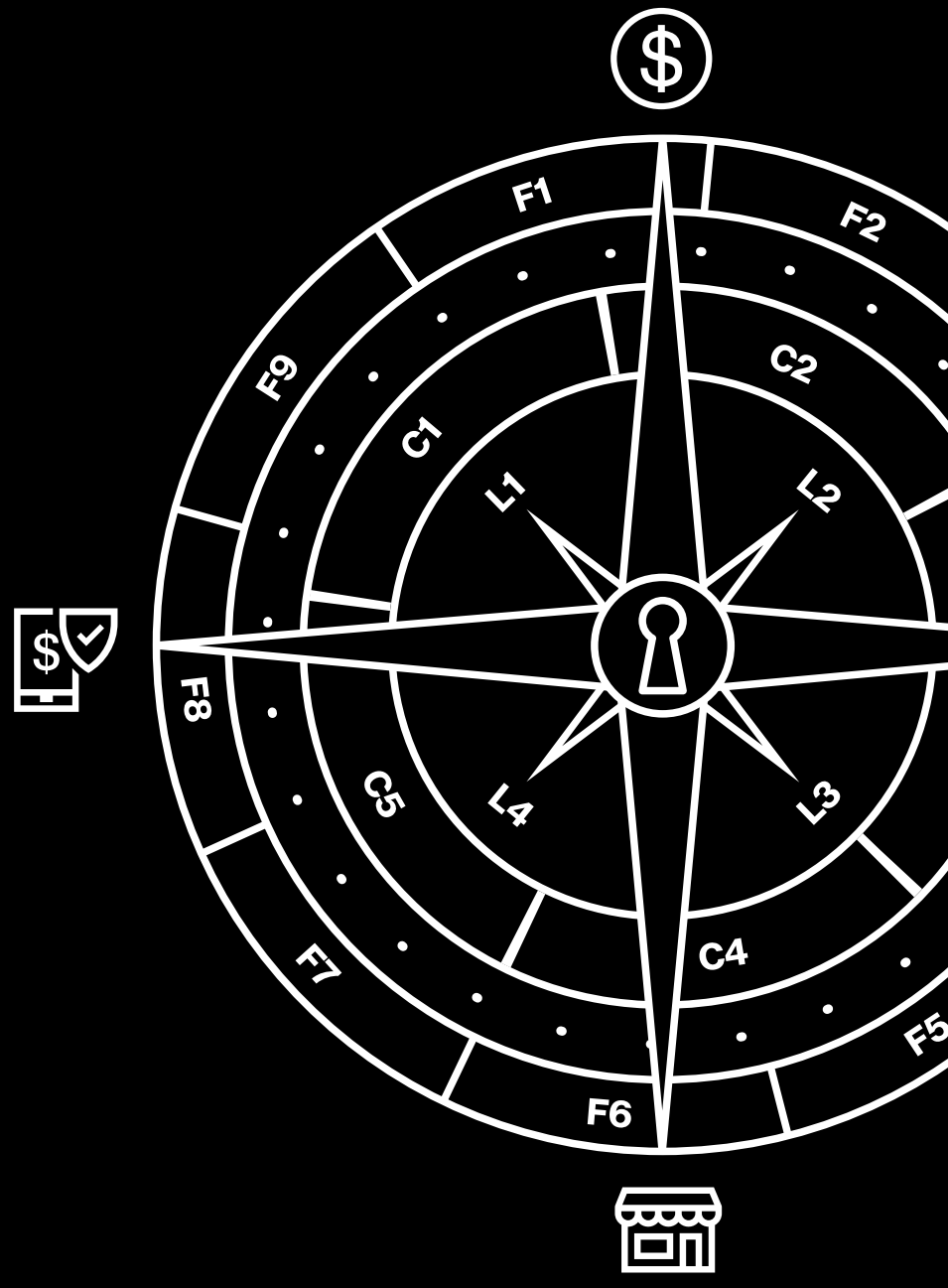
2019 Payment Security Report

Financial services snapshot



verizon business ready

The financial services industry is facing a rapidly changing landscape. Customers are demanding new ways to engage and conduct personalized transactions—particularly over mobile devices. Meanwhile, the industry continues to see entrants from other industries offer financial products.

In this competitive and highly regulated environment, the ability to protect payment card data can be a crucial differentiator. Customers have high expectations that financial service providers understand the need for payment security better than other kinds of businesses.

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.

A portfolio providing decreasing returns

Consistently maintaining effective security controls to protect payment card data and meet Payment Card Industry Data Security Standard (PCI DSS) requirements can help financial services organizations earn customer trust and win a competitive advantage. Yet our findings in the Verizon 2019 PSR show that financial service providers need assistance with maintaining payment card security.

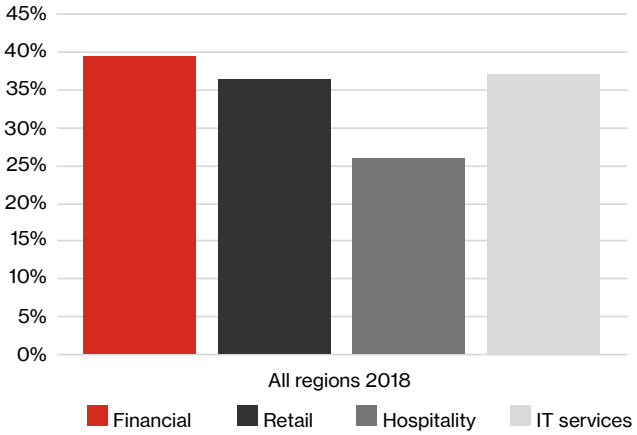


Figure 1. Global compliance by industry

While finance has the highest rate (39.0%) of full compliance with PCI DSS among the industries examined (retail, hospitality and IT services), its overall compliance rate dropped each year for the past two years. Finance's compliance rate fell from 59.1% in our 2017 PSR to 47.9% in the 2018 PSR and down to 39.0% this year.

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.

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

Finance's decline is not an outlier. In the nine years that Verizon has been producing the PSR, we've seen full compliance with PCI DSS requirements improve annually across all industries until 2017, when our assessments measured a downturn in compliance two years in a row for all industries studied. Assessments from other Qualified Security Assessor (QSA) companies show a similar decline in full compliance with the standards.

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 positive direction by decreasing 6.2 percentage points from last year to 10.2% in the 2019 PSR.

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 unfortunately, fewer than one-quarter of all organizations in the Americas (20.4%) maintained full compliance.

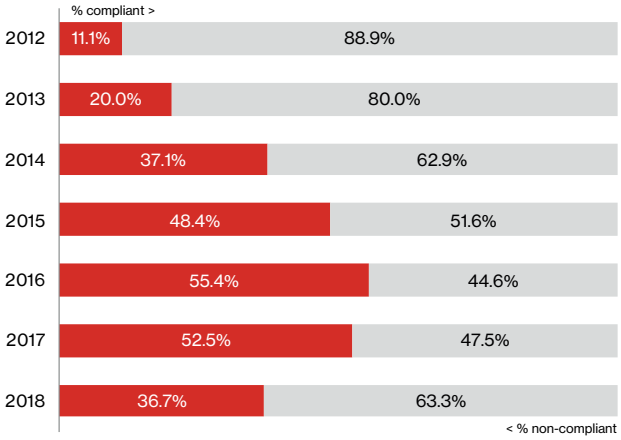


Figure 2. Full compliance by year

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.

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 (DPCP). None rate their DPCP maturity as optimized. This indicates that organizations can get better at developing and maintaining a mature PCI DSS compliance program, which will in turn help improve payment security.

18%

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

Financial services can't bank on existing DPCPs to maintain payment card security.

The good

According to the 2019 PSR, the financial services industry did better than any other industry on the following PCI DSS requirements:

- Maintain a firewall configuration (Requirement 1)
- Change vendor-supplied defaults (Requirement 2)
- Control physical access (Requirement 9)
- Security management (Requirement 12)

Finance's performance on maintaining firewalls even represented a 2.2 percentage point (pp) improvement from the 2018 PSR, a bright light in a year when overall performance for all industries showed a downward trend. Finance was also the closest to full compliance with this requirement, with the best control gap (7.3%) in this area.

Finance was the only industry to improve in protecting stored cardholder data (Requirement 3) compared to the 2018 PSR, and it showed the largest improvement in control gap in this area as well, moving from 14.1% to 5.9%.

The bad

A large portion of what some financial services providers do is transfer financial data, yet it appears that they can do a better job of encrypting data in transit (Requirement 4). The industry experienced the largest drop of any other industry (17.1 pp) in meeting this requirement.

Finance also struggled to protect against malicious software (Requirement 5), with the lowest overall compliance (at 82.9%) and the biggest control gap (8.5%) of the industries examined.

Finance had the second lowest level of compliance with PCI DSS incident preparedness requirements. In particular, financial organizations did not consistently track and monitor access (Requirement 10) and had difficulty with the ability to reconstruct security breach events through proper audit trails.

The interesting

In the 2019 PSR, we've included more detailed data breach investigation correlations from the PCI forensic investigations (PFIs) conducted by the Verizon Threat Research Advisory Center (VTRAC) | Investigative Response Team. The long-term trends show that of confirmed data breaches, 11.5% occurred in finance. That's not bad, although emulating IT services' rate of 2.7% is certainly a worthy goal.

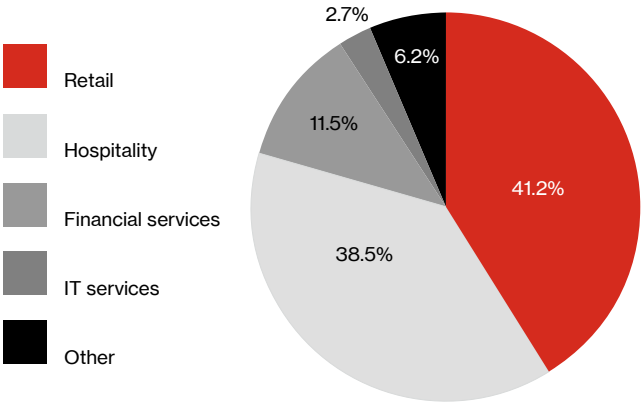


Figure 3. Confirmed data breaches by industry, six-year trend, Verizon PFI global caseload 2010–2016

Recommendations

Boost incident preparedness.

Incidents do happen. How an organization responds can make all the difference. A strong incident response (IR) plan is well worth the investment in time. Being able to provide a proper audit trail is also vital—cybersecurity and compliance experts can only help you if they know what happened. For more on the benefits of IR and how to implement it, see the Verizon Incident Preparedness and Response (VIPR) Report.

Look into mobile security.

As global mobile usage and data traffic increase—including mobile banking—it's well worth the effort to get ahead of security challenges involving employee devices, including personal devices that employees use at work. The 2019 Verizon Mobile Security Index (MSI) found that compromises involving a mobile device are a growing problem in financial services, with a rise in companies reporting a breach from 25% in the 2018 report to 42% in the 2019 MSI.[1] The 2019 PSR and MSI can both provide guidance on today's threats and how to protect data while enabling mobility.

Developing program maturity

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 be the navigational aid that organizations need 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 for PCI DSS compliance success.

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

It's time to take the lead.

The financial services industry strives to excel in meeting financial regulations and implementing technological innovations. Artificial intelligence–powered fraud detection, for instance, is just one area where many finance organizations have advanced. It's time to pair this kind of innovation with robust and sustainable PCI DSS compliance programs. Improving payment security and PCI DSS compliance could truly set an organization apart from its competition—and help pay healthy dividends in increased customer trust.

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 "Cybercriminals are banking on mobile devices being unsecured. Are you ready?," Verizon Mobile Security Index 2019—Financial services. https://enterprise.verizon.com/resources/reports/mobile-security-index/