2020 PSR

Payment Security Report

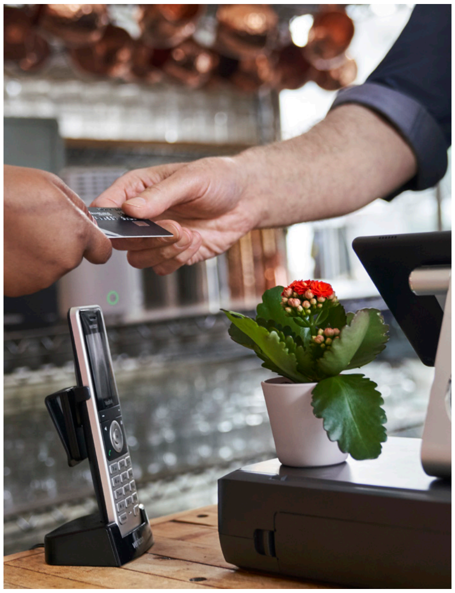
Hospitality

verizon

Hospitality sector: Better security compliance, but still lagging

Get detailed recommendations in the Verizon 2020 Payment Security Report (PSR).

The hospitality industry is a labyrinth of interconnected companies, owners, franchisors and suppliers. This makes hospitality payment and data security particularly challenging. In addition to complex payment security, the structure requires handling significant amounts of personal data on multiple databases and devices, which increases cyberattack vulnerability.



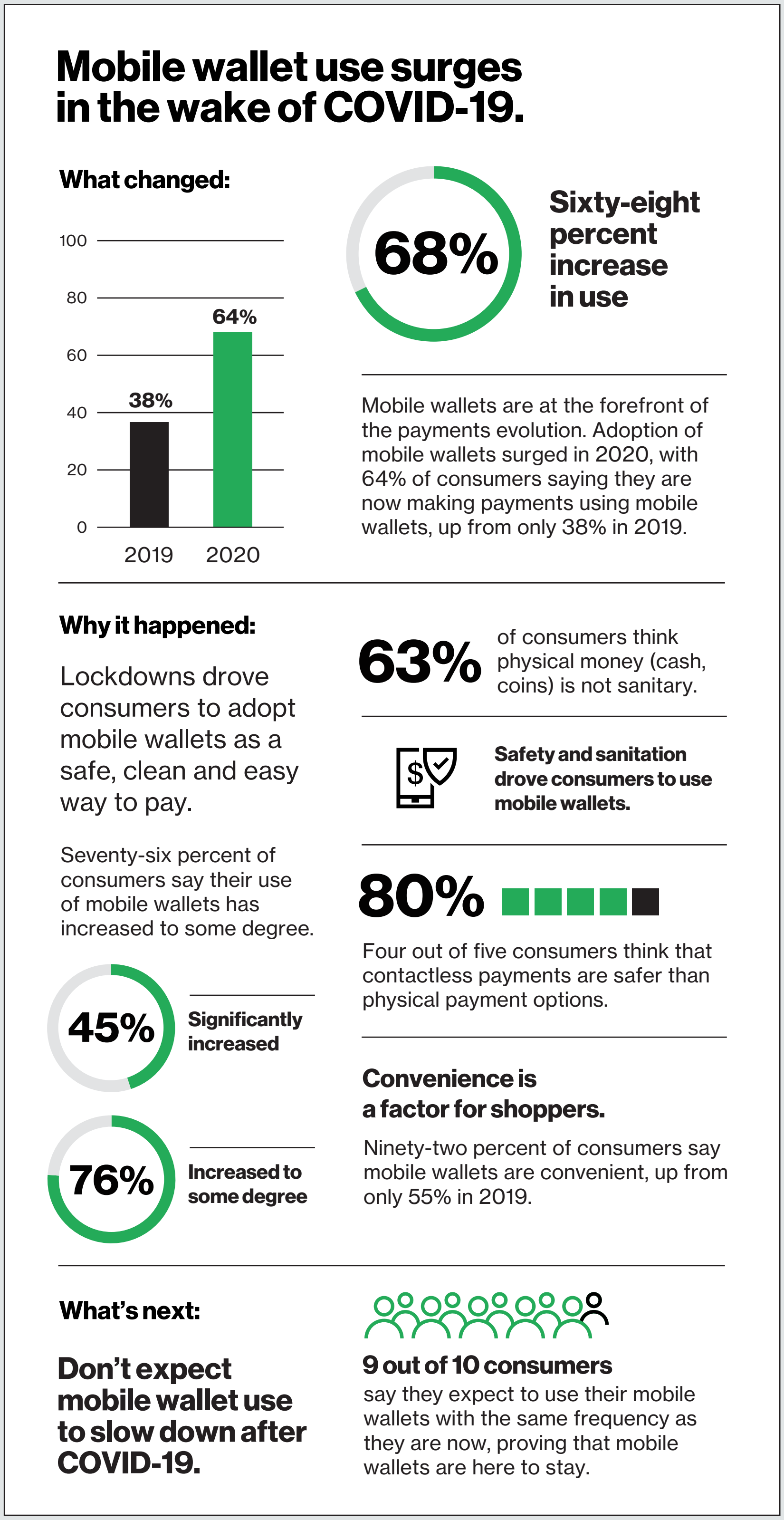
This complexity may explain why hospitality has ranked among the lowest in payment card data security sustainability over the last decade when compared with other ranked industries such as retail, financial and IT services, according to Verizon's Payment Security Report (PSR) research. However, 2019 was a breakthrough year for the hospitality industry, with improvements in this sector based on the Verizon 2020 PSR analysis of 2019 data.[1]

The hospitality industry has been in flux, with multiple new challenges due to ongoing digital transformation, increased mobile device payments, a surge in ransomware attacks and the rapid adoption of contactless payments driven by the COVID-19 pandemic.

Additionally, the industry needed to adjust to new security threats. Security is fast becoming less about defending against malware in the machine, such as point-of-sale (POS) device attacks, and more about defending infrastructure. Attackers now can easily search for known vulnerabilities on cloud-based payment platforms. They look for unpatched organization servers. When secure protocols are not in place and enforced, breaches can be easily achieved by someone with even marginal attack skills, according to the 2020 Verizon Data Breach Investigations Report (DBIR).[2] Add in the recent surge in digital payments driven by the COVID-19 pandemic, such as contactless tap-and-go payment cards and mobile wallets. Digital check-ins and room keys also suddenly are part of the new norm.

In an already complex industry with multiple interlinking enterprises, such rapid transitions require strategy rather than a wash-rinse-repeat security cycle. Intelligently negotiating new and evolving risk is particularly important as consumers and industries quickly adapt to new practices and processes. Take, for example, the significant shift to mobile wallets driven by COVID-19 concerns. This safe and popular contactless payment method could permanently change the landscape of payment security in the hospitality industry (see Figure 1). Now, how is this change impacting mobile device security and payment infrastructures?

Verizon's PSR provides the in-depth answers your industry needs in order to respond to such evolving payment security concerns, as well as a comprehensive birds-eye view on the regulatory landscape of the payment card industry (PCI). The PSR measures annual compliance through interim reports on compliance (IROCs) and reports on compliance (ROCs). It highlights risks associated with noncompliance and the PCI Data Security Standard (DSS) in a range of industries worldwide.



Mobile wallet use surges in the wake of COVID-19.

What changed:

68% **Sixty-eight percent increase in use**

Mobile wallets are at the forefront of the payments evolution. Adoption of mobile wallets surged in 2020, with 64% of consumers saying they are now making payments using mobile wallets, up from only 38% in 2019.

Why it happened:

Lockdowns drove consumers to adopt mobile wallets as a safe, clean and easy way to pay.

Seventy-six percent of consumers say their use of mobile wallets has increased to some degree.

45% **Significantly increased**

76% **Increased to some degree**

63% of consumers think physical money (cash, coins) is not sanitary.

Safety and sanitation drove consumers to use mobile wallets.

80% 🟩🟩🟩🟩■

Four out of five consumers think that contactless payments are safer than physical payment options.

Convenience is a factor for shoppers.

Ninety-two percent of consumers say mobile wallets are convenient, up from only 55% in 2019.

What's next:

Don't expect mobile wallet use to slow down after COVID-19.

9 out of 10 consumers say they expect to use their mobile wallets with the same frequency as they are now, proving that mobile wallets are here to stay.

Figure 1. Mobile wallet use surges in the wake of Covid-19.[3]

In the 2020 PSR, Verizon and several third-party contributors assessed four key industries – hospitality, retail, financial and IT services – on their levels of compliance to the PCI DSS 12 Key Requirements. The 2020 PSR reported that, of the total population of organizations assessed on PCI DSS compliance in 2019, compliance fell to 27.9%, a drop of 8.8 percentage points (pp) from the previous year and a huge 27.5 pp (50.3%) decline from 2016, when compliance peaked at 55.4%.[4]

Straw or brick? How is payment security built in hospitality?

Of the four industries, hospitality ranked lowest in full compliance in Verizon's PSR assessments from 2015 to 2018. However, this negative cycle broke in 2019, when hospitality ranked second after IT services for full compliance at 28.6%, a 2.3 pp improvement from 2018. In 2019, hospitality showed the most significant reduction in control gap of the four industries assessed, from 12.6% to 7.1%, or 5.5 pp. A reduction in control gap is a positive outcome. The smaller the control gap, the fewer controls are found to be not in place during validation, which narrows the noncompliance gap.

Building compliance with straw

Requirement 2: Do not use vendor-supplied defaults, 42.9%: Reported the lowest levels of full compliance across all industry sectors for this requirement, at 42.9%. This was very similar to this industry's 2018 figures, with just a 0.8 pp increase for 2019.

Requirement 3: Protect stored cardholder data, 64.3%: Lagged behind the other sectors in full compliance, yet showed a 7.2 pp improvement in control gap, reducing it to 3.9% in 2019.

What is PCI DSS?

Leading card brands set up the Payment Card Industry Data Security Standard (PCI DSS) to help businesses protect stored, processed or transmitted payment card data. 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 such as retention policies, encryption, physical security, authentication and access control. We've correlated PCI DSS compliance with organizations that experienced payment card data breaches since 2008, and we've never seen any organization suffering a confirmed payment card data breach while compliant across all 12 PCI DSS Key Requirements at the time of the data compromise. For more information, visit pcisecuritystandards.org

Building compliance with brick

The hospitality industry showed the highest compliance levels in several requirements in 2019, resulting in significantly better performance overall for full compliance for the year.

Requirement 1: Install and maintain a firewall configuration, 71.4%: Outperformed the other three industries in 2019, with 71.4% of organizations reporting full compliance. This was an improvement of 13.5 pp over 2018.

Requirement 6: Develop and maintain secure systems, 64.3%: Outperformed other sectors with full compliance at 64.3%, a 16.9 pp increase over 2018 findings. Hospitality reduced its control gap by the largest margin as compared with other industries—by 8.0 pp, to 4.7%.

Requirement 7: Restrict access, 85.7%: Reported the largest increase in full compliance, improving 22.6 pp to 85.7% in 2019 and again reducing its control gap.

Requirement 9: Control physical access, 85.7%: Achieved the highest full compliance, with 85.7%, a significant performance increase of over 22.6 pp since 2018. Its control gap was also the second lowest, at 4.3%, with a year-over-year decrease of almost 5 pp.

Requirement 11: Test security systems and processes, 78.6%: Had the largest rate of full compliance, at 78.6%. This share represents an improvement of 31.2 pp over 2018. Hospitality was the only industry that improved in control gap performance by shrinking it 10.9 pp to 13.5%.

Industry best practices

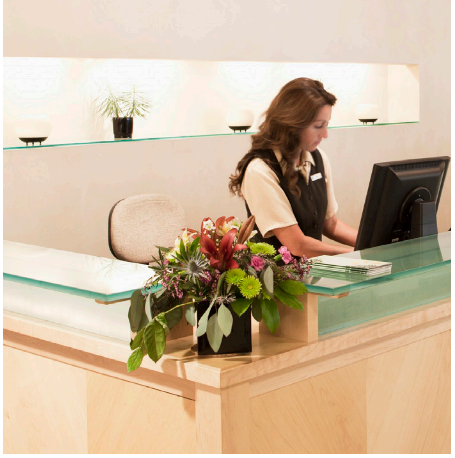
Digital transformation is generating a different approach to payment security that is less about defending POS and more about defending infrastructure and connections to the cloud. Data security is required by PCI DSS to be an ongoing 24/7 activity. To be effective, multiple components of the control environment must work together in a series of control systems in order to achieve sustainable compliance. Organizations should not allow any third-party service involved with payment security data storage, transmission or processing, or any services that impact the security of card data, to be in noncompliance with PCI DSS, as specified in Requirement 12. Devices can connect to hundreds of services a day, and organizations cannot allow any significant weaknesses to persist within the environment and expect sensitive data to be effectively protected. All systems need to consistently meet their control objectives.

The hospitality industry needs a thoughtfully designed security strategy, security business model and security operating model integrated into all aspects of its interlinking structure. Chief information security officers (CISOs) need to think strategically about the entire security framework (see the 2020 PSR, "The CISO hot seat," page 20)[5] while implementing best practices, such as:

- Following PCI DSS key requirements guidelines, and making sure they are integrated into the entire system
- Recording and reporting the exact locations of all payment card data storage, processing and transmission throughout the interlinking system, and enforcing least privileges
- Implementing zero trust when applicable (see below) and device-centric cryptography
- Encrypting all sensitive payment card information
- Consistently using multifactor authentication (MFA) for access to components in the cardholder data environment
- Regularly conducting penetration testing—at least once per year and after any significant infrastructure changes
- Maintaining annual comprehensive security training programs
- Protecting and restricting employee access on bring-your-own-device (BYOD) hardware

Contactless payments trends

Contactless payment methods are rapidly being integrated into payment systems due to COVID-19 safety concerns. This form of payment does not require physical contact between a consumer's payment device and a POS terminal, and functions in the same capacity as traditional swipe and insert payment devices. The cardholder holds the payment card (a contactless or dual-interface chip card) or payment device (such as a mobile phone) in close proximity to the terminal, and payment account information is transmitted wirelessly, over radio frequency.



As merchants migrate to the EMV standard for chip cards (EMV originally stood for Europay, Visa and Mastercard), their new POS equipment often already comes with the ability to perform contactless EMV transactions. If merchants choose to enable contactless functionality (in conjunction with their payments processor), the POS infrastructure will be ready to accept contactless payments using either dual-interface chip cards or Near Field Communication (NFC)-enabled mobile devices provisioned with a mobile EMV payment application. Contactless EMV transactions are faster; they only require tapping on the terminal rather than swiping or inserting. Cardholders do not have to hand over a device or account information during such transactions.

While these payment methods are raising some mobile security and data privacy concerns among consumers and organizations, in reality, they provide about the same level of security as – and greater convenience than – EMV chip cards. Contactless cards use the same NFC technology as mobile wallets. NFC technology in a contactless payment card can keep your card data safe when making in-store purchases. Mobile devices can also provide an additional level of security through tokenization and other types of cardholder verification. When payment data is tokenized, each transaction is anonymized to a random string of characters that cannot be reused to make additional purchases using the same information. This means that if a fraudster steals your transaction data, it can't be used again to make an unauthorized purchase. It also can't be reverse engineered to extract your card number.

Data from a contactless payment transaction that can be intercepted or stolen is insufficient to create a fraudulent card or conduct a fraudulent payment transaction. For fraudulent card-not-present transactions (internet and telephone purchases), almost all merchants require the security code from the back of the card and/or the ZIP code, neither of which is available in a contactless payment transaction.

Additionally, with the ongoing shift to cloud-based software in the hospitality industry, companies need to be familiar with their cloud service providers' track records and reputations. They need to consider all of the different connections and where the potential breach entry points exist. (See page 30 of the Verizon Mobile Security Index 2020 for additional information on device breach points.[6])

Some cloud applications can run on smartphones. They can be exposed to data outside a trusted network, which means that mobile device protocols should be included in the security framework. Many organizations are implementing zero trust models for cloud security management. Zero trust is a set of security measures that make sure that organizations do not automatically trust anything inside or outside of defined perimeters designed to protect sensitive data. In a zero trust environment, an organization must continuously verify users and devices while providing conditional access on an as-needed basis to digital resources such as email, applications, documents and information. Creating a zero trust environment around the mobile workforce requires creating an interlinking system that integrates unified endpoint management (UEM),

Common data security mistakes

CISOs need to deal with unproductive practices in their organizations that don't promote effective and sustainable data protection, such as:

- Lacking an effective security strategy; continuing to operate in a reactive mode
- Not understanding the scope of their risks; operating with poor risk assessment and management practices
- Viewing data protection as a technology problem; not managing data protection as an operational business process and cultural problem
- Failing to get real buy-in from board members and senior business management; not communicating a compelling narrative about the need for security investments
- Not knowing what to address first; inability to balance quick wins with long-term strategic initiatives
- Being unaware of data and IT assets; operating with many blind spots, not knowing where data exists and its sensitivity level, and failing to map data flow and stop shadow IT channels
- Security functioning as an island; not addressing security as a cross-functional issue that affects other parts of the organization
- Not testing their security; failing to test whether controls are effective (process and capability) and continuously testing for vulnerabilities
- Insufficient security awareness training; having ongoing education throughout the year
- Denying that they're a target; people and departments not believing they're at risk, or thinking they are too insignificant to become a target[7]

identity access management (IAM) and mobile threat defense (MTD) tools. (For more details on zero trust, see the 2020 PSR "Mobile security" appendix on page 123.[8])

Hospitality establishments need to make sure BYOD policies effectively maintain control over employee devices and include updated acceptable-use policies. Employee devices should not be allowed to connect to unauthorized applications. Security policies should be strictly enforced to automate and actively manage business-critical content and applications. These are just a few of the many considerations organizations need to think about as COVID-19 and other threats impact the way we do business.

The Payment Security Report: An exceptional guide

The Verizon 2020 Payment Security Report provides a wellspring of ideas on security practices for practitioners, CISOs and organizational leaders. For example, the challenges CISOs face in designing, implementing and executing a sound data security compliance program require strategic thinking. A lack of data security sustainability and effectiveness is largely the result of poor business, strategic and operational architecture design and execution. That's why the 2020 PSR includes clear guidance on five elements of a high-performance data security environment, as well as how to avoid the following seven strategic data security management traps:[9]

- Inadequate leadership
- Failing to secure strategic support
- Lack of resourcing capabilities
- Falling short on sound strategic design
- Deficient strategy execution
- Low capability and process maturity with lack of continuous improvement
- Communication and culture constraints

In previous editions of the PSR, we reviewed in detail the concepts of control effectiveness and sustainability. We introduced the 9-5-4 Compliance Program Performance Evaluation Framework (the 9 Factors of Control Effectiveness and Sustainability, the 5 Constraints of Organizational Proficiency and the 4 Lines of Assurance), valuable tools to help implement, maintain and measure control effectiveness. We covered how organizations can address constraints and develop data security compliance management proficiencies to become more efficient. We also discussed the application of metrics and maturity models for improving the sustainability and effectiveness of the control environment.

In addition to maintaining compliance efforts in line with the PCI DSS 12 Key Requirements, what next steps should your organization take during these disruptive times in the hospitality industry?

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. The Verizon 9-5-4 Compliance Program Performance Evaluation Framework is 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.

Hospitality's challenges in PCI DSS compliance do not need to define your response to payment security. Despite hospitality's overall lackluster compliance performance over the last decade, we saw marked improvement in 2019. Building a mature compliance program can allow you to join 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.

[1] Verizon 2020 Payment Security Report, 2020. https://www.verizon.com/business/resources/reports/payment-security-report/

[2] 2020 Verizon Data Breach Investigations Report, 2020. https://enterprise.verizon.com/resources/reports/dbir/

[3] Marqeta, Part One of Marqeta's 2020 State of Payments Report, "Mobile wallet use surges in the wake of COVID-19," Oct 15, 2020. https://blog.marqeta.com/2020/10/15/mobile-wallet-adoption-surges-among-seniors-boomers-in-wake-of-pandemic/

[4] Verizon 2020 Payment Security Report, 2020. https://www.verizon.com/business/resources/reports/payment-security-report/

[5] Ibid

[6] Verizon Mobile Security Index 2020, page 30, 2020. https://enterprise.verizon.com/resources/reports/mobile-security-index/

[7] Verizon 2020 Payment Security Report, 2020. https://www.verizon.com/business/resources/reports/payment-security-report/

[8] Ibid

[9] Ibid