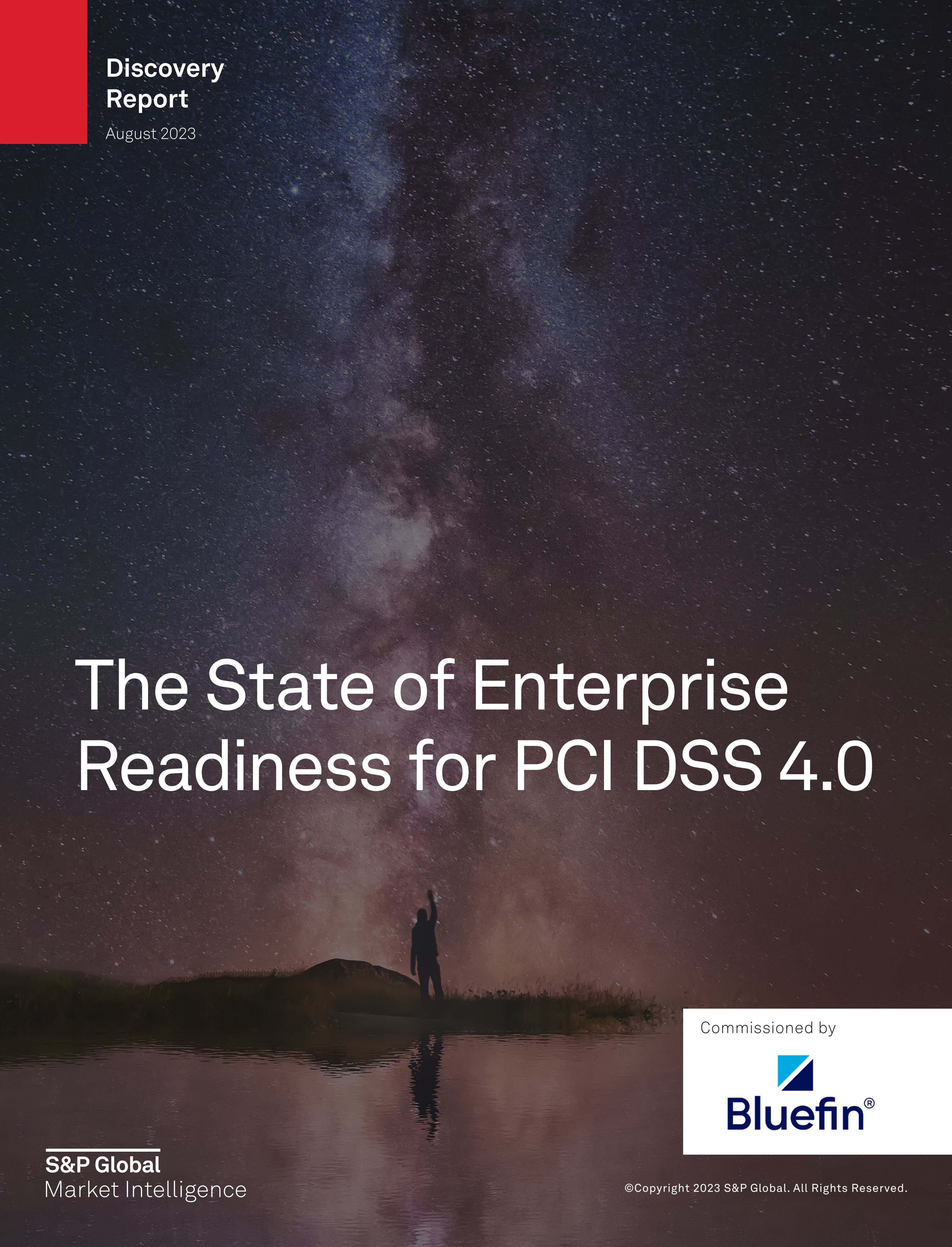
Discovery Report

August 2023



The State of Enterprise Readiness for PCI DSS 4.0

Commissioned by

Bluefin®

S&P Global
Market Intelligence

Executive Summary

Introduction

Payments are the lifeblood of any enterprise, with direct implications for revenue, profitability and operational performance. Given this level of strategic importance, businesses are continuously adapting their payments stacks to keep pace with evolving customer needs and expectations. The pace of change creates bountiful opportunity for cybercriminals to exploit emerging points of vulnerability and capture critical customer data. Maintaining a resilient cybersecurity posture in this environment is a constant battle for chief information security officers (CISOs).

For nearly two decades, enterprises and their payments partners have turned to the Payment Card Industry Data Security Standards (PCI DSS) for guidelines on how to mitigate payment data risks. These guidelines have evolved with the industry, introducing new requirements to help businesses ward off emerging payment data threats. The latest iteration, PCI DSS 4.0, introduces significant changes that enterprises must adapt to before the March 2025 deadline.

While PCI DSS 4.0 presents an array of operational and resource hurdles for enterprises, there are clear benefits for the industry. Those that approach it with a strategic mindset stand to differentiate themselves in the marketplace and deliver a superior customer experience. Backed by data from payment data security professionals at enterprises across nearly a dozen industry verticals, this report provides a view into the current state of payment data security and establishes a baseline for PCI DSS 4.0 readiness.

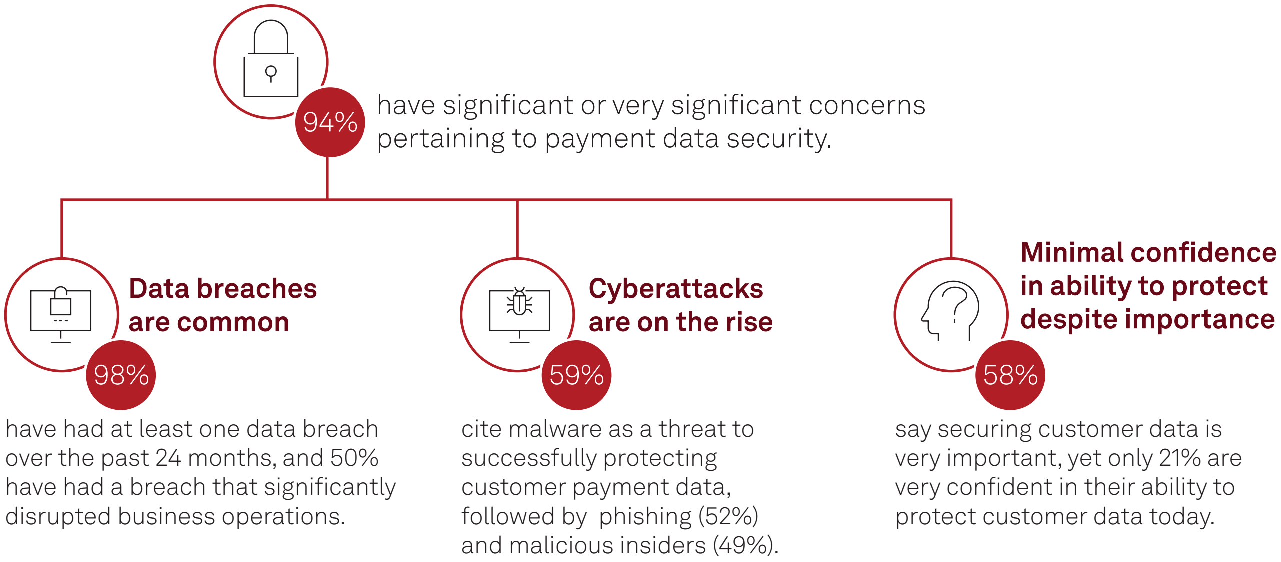
Key findings

- **Payment data security concerns are widespread and significant.** Ninety-four percent of respondents have significant or very significant concerns pertaining to payment data security, and only 21% say they are very confident in their ability to protect customer data today.
- **PCI DSS 4.0 necessitates a significant lift, and meeting the deadline is a growing concern.** Ninety-three percent of respondents indicate the changes required by PCI DSS 4.0 are significant. Further, 90% are concerned about meeting the timeline, and 64% say they would be likely or very likely to accept a timeline extension.
- **PCI DSS 4.0 education and execution remain low.** Fewer than a third (31%) of surveyed payment data security professionals have a strong understanding of all requirements associated with PCI DSS 4.0, and nearly half (49%) indicate their organizations have yet to begin executing on PCI DSS 4.0 changes.
- **Despite the challenges, enterprises overwhelmingly view PCI DSS 4.0 in a positive light.** Four in five respondents (80%) agree or strongly agree that PCI DSS 4.0 is fair, necessary and for the betterment of the industry and consumers.
- **Partnerships will play a critical role.** Eighty-six percent of respondents indicate their organization will solely or mostly rely on third-party vendors for PCI DSS 4.0 compliance in some capacity.

The state of payment data security

Enterprises are under pressure to deliver payment experiences that let their customers transact wherever and however they prefer. Diversification of payment channels and methods is expanding the attack surface, attracting growing attention from hackers and fraudsters. This has put payment and risk professionals on high alert: 94% of our survey respondents say they have significant or very significant concerns pertaining to payment data security.

Figure 1: State of payment data security



94% have significant or very significant concerns pertaining to payment data security.

Data breaches are common

98% have had at least one data breach over the past 24 months, and 50% have had a breach that significantly disrupted business operations.

Cyberattacks are on the rise

59% cite malware as a threat to successfully protecting customer payment data, followed by phishing (52%) and malicious insiders (49%).

Minimal confidence in ability to protect despite importance

58% say securing customer data is very important, yet only 21% are very confident in their ability to protect customer data today.

Q. How significant are your organization's concerns pertaining to payments data security?
Q. Has your organization had a data breach resulting in a loss of customers' payments data in the past 24 months?
Q. Has your organization caught/prevented an attempted breach targeting customers' payments data in the past 24 months?
Base: All respondents (n=250).
Source: S&P Global Market Intelligence state of PCI DSS survey, 2023.

Cyberattacks are increasingly sophisticated and come in a variety of formats. Malware (59%) is the top-cited threat to protecting customers' payment data. Malware is software designed to exploit vulnerabilities by gaining access to computer systems and wreaking havoc, such as by stealing data and disrupting operations. This includes banking trojan horse malware designed to steal financial information such as logins and credit card numbers from users. Phishing attacks (52%) can be a low-cost, high-impact method to carry malware via email or texts targeting employees at financial institutions, payment service providers, merchants or end users themselves. Malicious insiders (49%) are also a growing threat; obtaining sensitive financial data can be a lucrative option for disgruntled employees. Also on the list of threats are denial of service (45%), delays in patching/updates (40%), skimming (38%), man-in-the-middle attacks (25%) and crypto-jacking (16%).

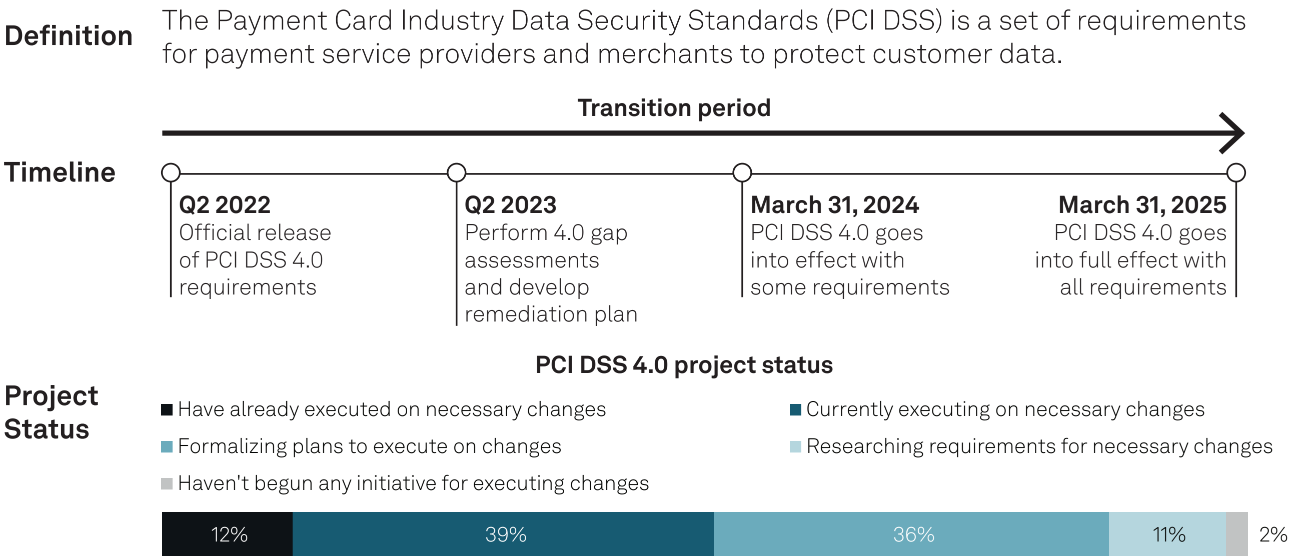
The frequency and complexity of cyberattacks is exacerbated by organizations' data management and governance challenges. In fact, only 21% of respondents say they are very confident in their ability to protect customer data. As a result, breaches of financial data have become all too common: 98% of respondents indicate their organization has had at least one data breach over the past 24 months, and 51% have experienced a breach that created a significant disruption to business operations. A seemingly minor breach jeopardizing the security of customer data can quickly snowball into a major IT issue, as well as a risk to business operations, customer trust and brand perception.

While the majority of enterprises (58%) place high importance on securing customer data, it is evident that the challenges to doing so remain both significant and persistent. For nearly two decades, organizations have turned to PCI DSS for best practices in combating payment data threats, and they can continue to do so with the latest updates in version 4.0.

Understanding the PCI DSS 4.0 challenge

PCI DSS is a set of standards established by the PCI Security Standards Council (SSC) for payment service providers and merchants to protect customer payment data. The PCI SSC formed the first set of standards in 2004, and it put forth the current iteration, PCI DSS 3.0, 10 years ago. While there have been various adjustments to requirements in 3.0, they are smaller and more short-term-focused compared to the overhaul that 4.0 will require. The standards are not required by law or regulatory mandate but self-governed and imposed by the global card networks on merchants, payment processors, service providers and others in the payments ecosystem.

Figure 2: What is the PCI DSS 4.0 mandate?



Definition

The Payment Card Industry Data Security Standards (PCI DSS) is a set of requirements for payment service providers and merchants to protect customer data.

Timeline

Transition period

Q2 2022
Official release of PCI DSS 4.0 requirements

Q2 2023
Perform 4.0 gap assessments and develop remediation plan

March 31, 2024
PCI DSS 4.0 goes into effect with some requirements

March 31, 2025
PCI DSS 4.0 goes into full effect with all requirements

Project Status

PCI DSS 4.0 project status

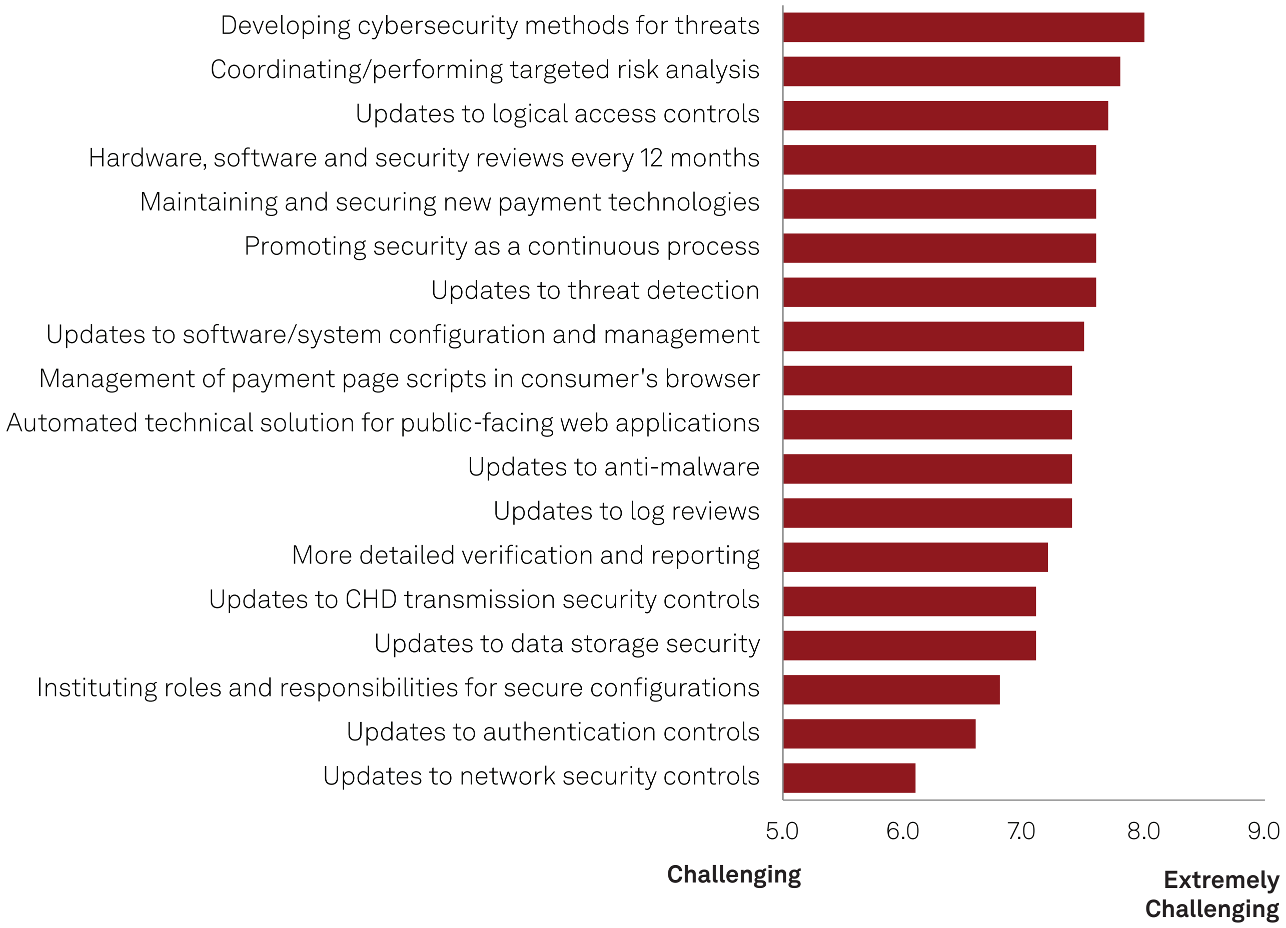
■ Have already executed on necessary changes
■ Currently executing on necessary changes
■ Formalizing plans to execute on changes
■ Researching requirements for necessary changes
■ Haven't begun any initiative for executing changes
12%
39%
36%
11%
2%

Q. What stage best describes where your organization is at for implementing changes required by PCI DSS 4.0?
Base: All respondents (n=250).
Source: S&P Global Market Intelligence state of PCI DSS survey, 2023.

A lot has changed in the 10 years since PCI DSS 3.0 was introduced: physical and digital payment innovations have widened the scope for potential vulnerabilities, and the threat landscape has only presented more complex and pressing cybersecurity challenges. While PCI DSS 4.0 has implications for nearly every payment channel, enterprises expect card-not-present channels to be most heavily affected. Respondents cite online/web as the payment channel most significantly impacted by PCI DSS compliance frameworks (56%), followed by call centers (48%), in-person/in-store (40%) and invoicing/billing (20%).

PCI DSS 4.0 brings forth new requirements designed to combat emerging threats and to ensure the protection of sensitive customer financial data from cyberattacks. The list of requirements, ranked by the perceived challenge of implementation, is illustrated in Figure 3. Top-cited challenges include developing cybersecurity methods for threats, coordinating and performing targeted risk analyses, and updating logical access controls.

Figure 3: PCI DSS 4.0 requirements ranked by reported level of challenge



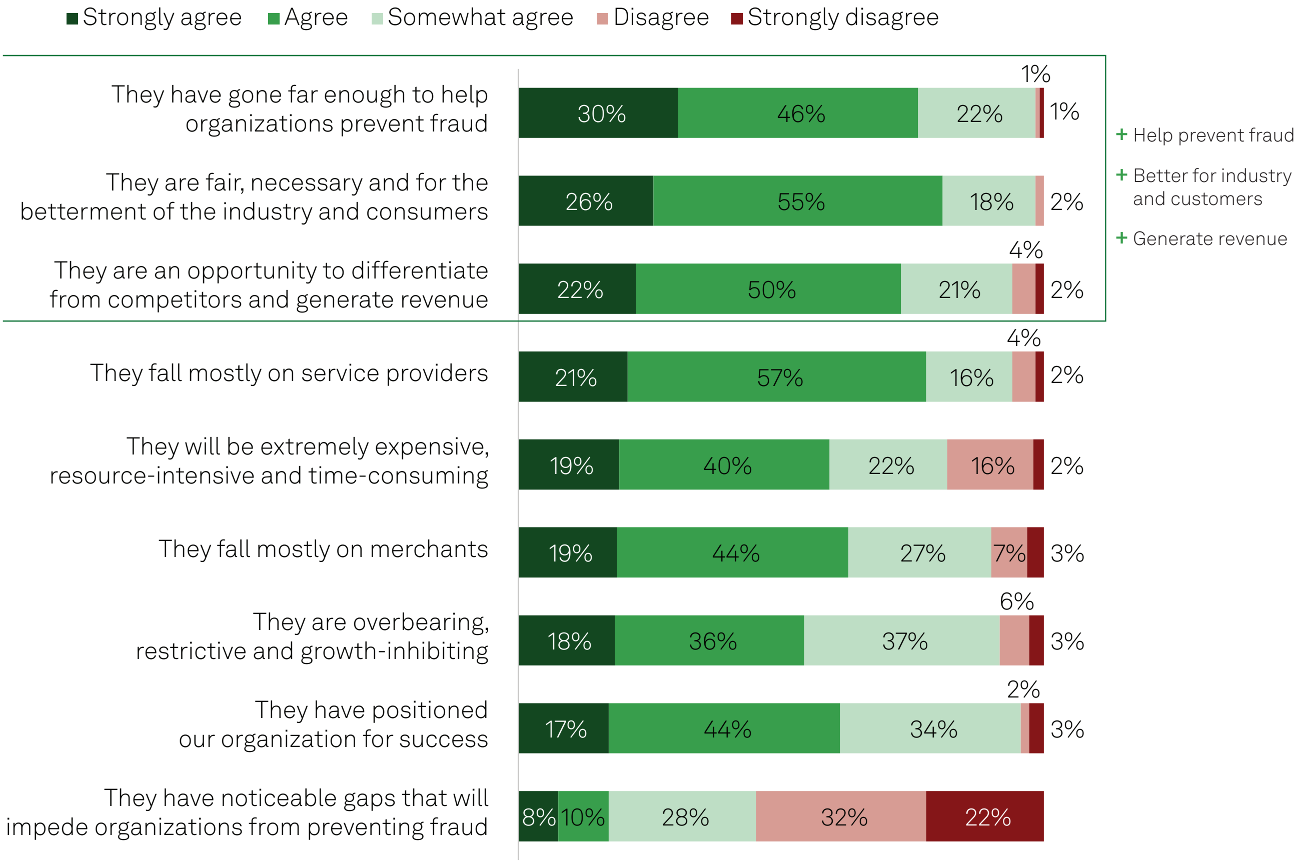
Q. On a scale of 0-10, with 0 being "not at all challenging" and 10 being "extremely challenging," how challenging will the following PCI DSS 4.0 requirements be to implement for your organization?
Base: All respondents (n=250).
Source: S&P Global Market Intelligence state of PCI DSS survey, 2023.

PCI DSS 4.0 brings forth an extensive list of new requirements, as well as updates to existing ones, each likely to require significant resources and time to address. The lift is not lost on enterprises. Ninety-three percent of respondents indicate that the changes required are significant. Further, 90% are concerned with meeting the PCI DSS 4.0 timeline, and 64% say they would be likely or very likely to accept a timeline extension.

With the deadline for updates drawing nearer, PCI DSS 4.0 education and knowledge remains low. Fewer than a third (31%) of payment data security professionals say they have a strong understanding of all requirements associated with PCI DSS 4.0, further calling into question enterprise readiness. Despite the shortening runway to 4.0 implementation and the sizable updates required, nearly half (49%) of respondents indicate their organizations have yet to begin executing on PCI DSS 4.0-related changes.

While this may paint a bleak picture for the state of PCI DSS 4.0 preparedness, payment data security professionals show cautious optimism regarding the mandate; many view it as an opportunity for strategic differentiation. In fact, overall, respondents are more likely to agree with favorable characterizations of the mandate than negative ones (see Figure 4). Consider that four in five respondents agree or strongly agree that PCI DSS 4.0 is fair, necessary and for the betterment of the industry and consumers, while just 17% agree or strongly agree that it has noticeable gaps that will impede their organization from preventing fraud.

Figure 4: Despite the lift, most businesses have positive sentiments toward PCI DSS 4.0



Q. To what extent do you agree/disagree with the following statements regarding PCI DSS 4.0?
Base: All respondents (n=250).
Source: S&P Global Market Intelligence state of PCI DSS survey, 2023.

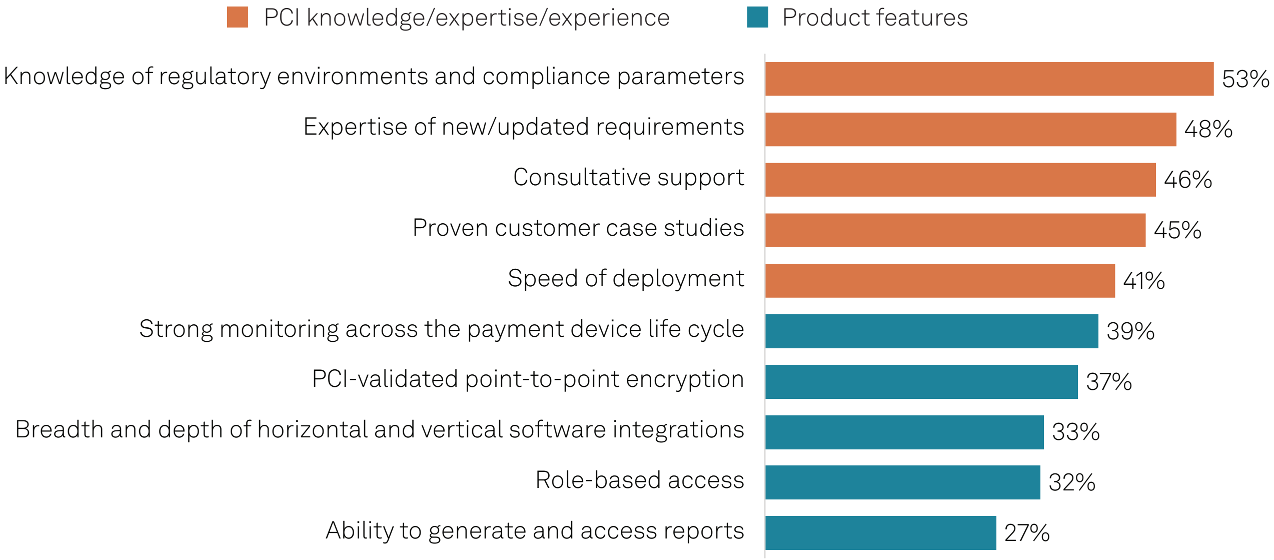
Actions to take for PCI DSS 4.0

With a lengthy list of new and updated requirements, PCI DSS 4.0 impacts a variety of business functions and operations. Internal alignment is a logical starting point, considering the extent to which the requirements impact multiple business functions. Getting the right stakeholders to formulate and execute on changes of this magnitude will require in-house orchestration.

Logical stakeholders include executive roles that are technology-focused (CIO, CISO, CTO), compliance-oriented (chief compliance officer, chief risk officer, head of legal), in relevant functions (VPs of finance, IT, procurement, governance/risk/compliance), and overseeing payments strategy (head/VP of payments) and execution (software developer/engineer, PCI coordinator). Enterprises need employees who can conduct self-assessments, create plans and implement playbooks to reach minimum requirements, as well as determine strategic opportunities to differentiate, such as by streamlining steps that may result in customer friction.

However, given the extent of the requirements and correlating changes, most enterprises are ill-suited to take on PCI DSS 4.0 alone. Partners are needed to abstract complexity and provide supporting technology. Respondents broadly acknowledge the strategic role of partners: 86% indicate their organization will solely or mostly rely on third-party vendors for PCI DSS 4.0 in some capacity.

Figure 5: Businesses want a trusted advisor for PCI DSS 4.0



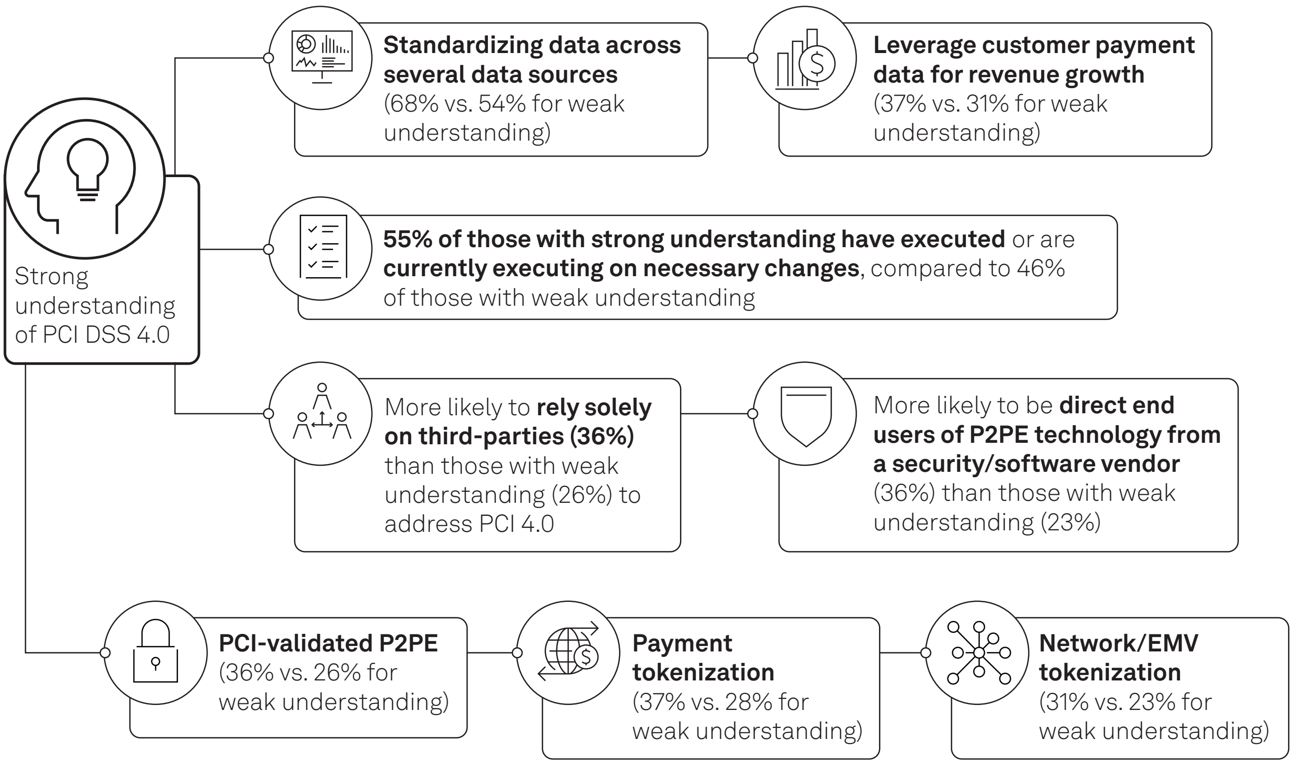
Q. What do you prioritize in a payments data security vendor when it comes to PCI DSS 4.0?
Base: All respondents (n=250).
Source: S&P Global Market Intelligence payment data security survey, 2023.

Interestingly, respondents prioritize payment data security vendors with intimate knowledge of regulatory environments and PCI DSS compliance parameters, including expertise on 4.0 updates (see Figure 5). This illustrates the PCI DSS 4.0 information gap that exists for many enterprises, and the need for partners to play the role of trusted advisor. Partners that are well-versed in the requirements, have the ability to provide consultative support and can move efficiently are well positioned to deliver on enterprises' PCI DSS 4.0 needs.

The small cohort who strongly understand PCI DSS 4.0 provide some useful direction about what enterprises should prioritize (see Figure 6). After all, they report being furthest along in the PCI DSS 4.0 maturity journey, with the majority (55%) currently executing or already having executed on necessary changes. These enterprises stand out in two key areas:

- **Importance of payment data security technologies:** Thirty-six percent of those who strongly understand PCI DSS cite PCI-validated point-to-point encryption (P2PE) as important to protecting customer data, compared to 26% of those with weak understanding, underscoring an emphasis on purpose-built and battle-tested security technology. Similarly, 37% with strong understanding cite payment tokenization (compared to 28% of those with weak understanding) and 31% cite network/EMV tokenization (compared to 23% with weak understanding), illustrating an appetite to reduce the storage of sensitive payment data.
- **Use of partners:** Despite their stated strong understanding of the requirements, most of these respondents point to their major reliance on external partners to carry the brunt of PCI DSS 4.0 compliance, with more than one-third (36%) saying they solely use third parties and over half (51%) mostly relying on third-party vendors. In other words, the more organizations know about PCI DSS 4.0, the more they value partners that can abstract the operational and technical complexities.

Figure 6: What do those with a strong understanding of PCI DSS 4.0 say?



Strong understanding of PCI DSS 4.0

Standardizing data across several data sources (68% vs. 54% for weak understanding)

Leverage customer payment data for revenue growth (37% vs. 31% for weak understanding)

55% of those with strong understanding have executed or are **currently executing on necessary changes**, compared to 46% of those with weak understanding

More likely to **rely solely on third-parties (36%)** than those with weak understanding (26%) to address PCI 4.0

More likely to be **direct end users of P2PE technology from a security/software vendor** (36%) than those with weak understanding (23%)

PCI-validated P2PE (36% vs. 26% for weak understanding)

Payment tokenization (37% vs. 28% for weak understanding)

Network/EMV tokenization (31% vs. 23% for weak understanding)

Q. How would you describe your organization's overall understanding of the new requirements of PCI DSS 4.0?
Base: All respondents (n=250).
Source: S&P Global Market Intelligence payment data security survey, 2023.

Enterprises expect to enlist a wide range of partners to meet the requirements of PCI DSS 4.0, including payment processors/acquirers (64%), cybersecurity vendors (62%), payment data security vendors (60%), IT services/consultants (59%) and point-of-sale providers (55%). While nearly two-thirds (62%) feel confident in their primary payment data security provider's ability to support their organization in meeting PCI DSS 4.0 requirements, just a quarter indicate they are very confident. Given the proximity of the deadline, enterprises should be assessing the competency of their partners and evaluating the need to address capability gaps in the near term.

Conclusion

Payment data security concerns are widespread, elevated and highly prioritized in enterprises. This creates a fitting backdrop for PCI DSS 4.0, which puts forth new guidelines to help enterprises address the evolution of payment data security threats. While PCI DSS 4.0 is generally viewed positively by payment data security professionals, understanding is limited, the changes required are significant and much of the market is at risk of falling short of the deadline. Developing an internal strategy with cross-functional stakeholders and leveraging the support of trusted partners will be fundamental to addressing required changes, abstracting the complexity of the migration and leveraging PCI DSS 4.0 as an opportunity for competitive differentiation.

Research methodology

The findings presented in this report draw on a survey fielded in North America in Q2 2023. The survey targeted 250 PCI DSS decision-makers/influencers in companies with more than 500 employees and over $100 million in annual revenue. The study prioritized respondents with intimate knowledge of the PCI DSS guidelines and requirements across the following industries: banking, commercial airlines, education, energy/oil and gas, government (state, federal), healthcare, IT (software/services), non-profits, retail (e-commerce, brick-and-mortar), transportation/logistics and utilities. The job descriptions of respondents were a mix of executives (CISO, CIO, chief compliance officer, chief risk officer), VPs and other PCI-focused roles (risk manager, governance, risk and compliance officer, head of payments, etc.) This report also draws on contextual knowledge of additional research conducted by S&P Global Market Intelligence.

Bluefin®

To learn more about Bluefin or PCI DSS 4.0 readiness, contact us at https://www.bluefin.com/contact/

About the author

Jordan McKee

Research Director, Fintech

Jordan McKee leads the newly formed fintech research and advisory group within S&P Global Market Intelligence. As an analyst, his research focuses on digital payments and enterprise payments strategies. For nearly a decade Jordan's research agenda has provided guidance on emerging technologies and disruptive forces impacting the end-to-end payments value chain. His research and analysis helps enterprises, investors, payment networks, issuing and acquiring banks, payment processors, and other payments industry stakeholders navigate change and market disruption.

David Immerman

Consulting Analyst

Internet of Things, Fintech

David Immerman is a Consulting Analyst for the TMT Consulting team based in Boston, Massachusetts. Prior to joining S&P Global Market Intelligence, David ran competitive intelligence for a supply chain risk management software startup. He spent nearly four years at PTC providing thought leadership and market research on technologies and trends in manufacturing. Previously, David was an industry analyst in 451 Research's Internet of Things channel for three years, primarily covering the smart transportation and automotive technology markets. He holds a bachelor's degree in Business Administration from Marist College.

About this report

A Discovery report is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners — what they are doing, and why they are doing it.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.