

The strategic importance of payments data ownership

Table of contents

The Take	3
Key findings	3
More SaaS companies and merchants are approaching payments strategically	4
Figure 1: SMBs have an appetite for embedded financial services	4
Payments technology roadmaps must not overlook data ownership	5
Figure 2: Businesses place high importance on strategic use of customer payment data	6
Multiple scenarios make payments data ownership critical	7
Impact on SaaS companies' valuation in M&A	7
PSP outage/downtime	7
De-banking of higher-risk merchants and SaaS platforms	8
Need for payment orchestration and multi-PSP relationships	8
Figure 3: Most large merchants prefer to work with multiple payment processors	9
PSP migration delays	9
The strategic role of PSP-agnostic tokenization	10
Reaching the ideal state	11
About Bluefin	12
About the authors	13

The Take

Payments have become a strategic lever for many software-as-a-service (SaaS) companies and large merchants as they look to drive growth, enhance their customer experience, and generate operational and cost efficiencies. While these organizations increasingly recognize the business value of payments, they often overlook the strategic importance of payments data ownership.

When payments data is “locked in” with a single payment service provider (PSP), merchants and SaaS companies increase their dependency risk while forgoing a certain degree of agility and adaptability. The consequences of this can manifest in multiple ways, ranging from a possible hit to a SaaS company’s valuation in an M&A scenario to revenue loss and customer churn in the event a merchant experiences an abrupt closure of its bank or payment processing account or its PSP suffers an outage or change in business direction. At the core of these concerns is the lack of complete control of payments data, which can reduce a business’s ability to pursue opportunities and act in its own best interest.

While taking data in-house can provide a path to payments autonomy, most businesses are ill-equipped to shoulder the myriad responsibilities associated with this shift. For many, using a PSP-agnostic tokenization and data devaluation provider can be the best solution. When selecting a vendor, businesses should not view tokenization solely through the prism of costs but instead focus on leveraging it to enable orchestration and operational excellence. It is also crucial to factor in individuals’ and regulators’ increasing expectations for data privacy and the need to mitigate issues related to privacy laws and data sovereignty. This holistic approach offers the benefits of true payments data autonomy while reducing the overall operational and compliance burden.

Key findings

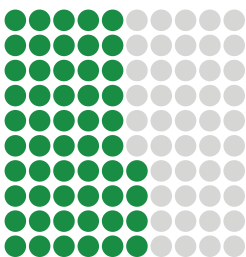
- It is common for merchants and SaaS companies to tokenize card data through PSPs, which reduces agility and compromises their ability to respond to market developments and opportunities. Gaining control over tokens is a prerequisite to gaining control over payments data.
- Opting for an agnostic tokenization provider that offers a proxy capability to orchestrate payments to any PSP alleviates the compliance burden associated with safeguarding sensitive customer data while mitigating the risk of long-term PSP vendor lock-in. This enables businesses to leverage a host of opportunities, ranging from M&A to payment orchestration to enhancing operational resilience.
- Growing businesses require multiple PSP relationships to execute various strategies, allocate resources efficiently and build redundancies in their payment processing systems. It is unsurprising that nearly two-thirds (63%) of merchants with 1,000+ employees indicate their preference is to use multiple processors, citing flexibility, reaching multiple geographies and cost optimization as key factors.

More SaaS companies and merchants are approaching payments strategically

More SaaS companies and merchants are deepening their payments strategies to elevate customer journeys, drive topline revenue growth and enhance profitability. In recent years, SaaS companies have strategically inserted themselves into the payments value chain by embedding payment processing services in their software. By taking greater ownership over payments, SaaS companies can streamline their user experience, increase product stickiness and, importantly, add a new source of revenue with zero marginal customer acquisition cost. Further, payments can be a beachhead for offering other value-added services, such as embedded lending, add-on reporting and analytics capabilities, and point-of-sale hardware.

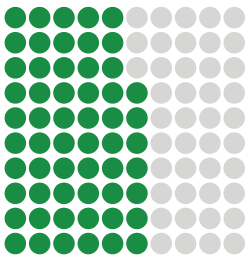
Embedded payments provide small and medium-sized businesses (SMBs) with a single pane of glass to run their business. More than half (54%) of SMBs agree they would like to see their software partners offer integrated financial products, according to a 451 Research survey. Further, 57% of SMBs indicate that their organization would run more efficiently if the financial services they used were better integrated with their business software/applications. Embedded payments are becoming commonplace in virtually every industry vertical — running the gamut from healthcare and field services to restaurants and retail — as more SaaS companies look to capitalize on this market opportunity.

Figure 1: SMBs have an appetite for embedded financial services



54%

Agree that they would like to see their software partners offer integrated financial products.



57%

Agree that their organization would run more efficiently if the financial services they used were better integrated with their business software/applications.

Q. To what extent do you agree with the following statement? - We would like to see our software partners offer us integrated financial products (e.g., payment processing, business banking).

Q. To what extent do you agree with the following statement? - Our organization would run more efficiently if the financial services we use were better integrated with our business software/applications.

Base: Respondents from businesses with fewer than 1,000 employees, excluding don't know (n=171-180).

Source: 451 Research's Voice of the Customer: Macroeconomic Outlook, SME Tech Trends, Fintech 2022.



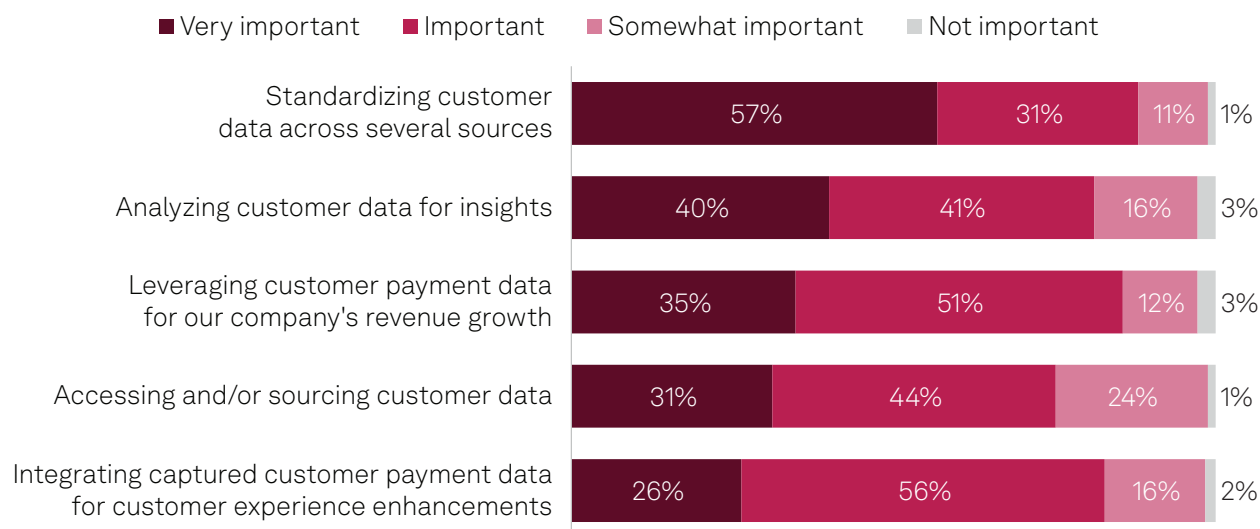
Similarly, many large merchants are approaching payments as a strategic lever for their business. Rather than dismissing payments as a “cost of doing business,” they are devising comprehensive payment strategies oriented around quantifiable business outcomes such as geographical expansion, reduction in abandonment rates and optimization of direct and indirect costs associated with acceptance. Among merchants with more than 1,000 employees, 451 Research finds that 73% view payments as a highly strategic area of focus for their organization that drives significant competitive differentiation.

We expect the trend of SaaS companies and merchants prioritizing payments will continue to accelerate as more businesses recognize the role of payments in driving growth, customer experience and operational enhancements.

Payments technology roadmaps must not overlook data ownership

As SaaS companies and merchants increase their strategic embrace of payments, the criticality of payments data cannot be overstated. The value of data goes beyond executing a transaction; payments data fuels marketing engines, bolsters risk management, powers personalization strategies and serves as a critical link between a business and its customers. Ensuring this data is readily accessible is imperative. Consider that three in four businesses agree it is very important or important to be able to access or source customer payments data. Further, 88% of businesses indicate it is very important or important to be able to standardize customer payment data across several sources (e.g., e-commerce, in-store).

Figure 2: Businesses place high importance on strategic use of customer payment data



Q. How would you rate the importance of addressing the following challenges for payments data?

Base: All respondents (n=250).

Source: 451 Research & Bluefin custom payments data security survey, 2023.

Yet, many businesses inadvertently overlook the absence of true data ownership in their contracts with PSPs. Many PSPs offer payment tokenization to absolve their customers of the various obligations related to the Payment Card Industry Data Security Standard (PCI DSS). As a result, merchants and SaaS companies commonly forgo the traditional route of storing sensitive card details and instead rely on PSP-specific tokens during transactions.

It is common for merchants and SaaS companies to find themselves in a situation where a single PSP controls all of their cardholder data, leaving them with limited means to retrieve it. We see several concerns with this approach, including:

- **Reduced agility and adaptability.** A lack of true payment data ownership may compromise the ability to respond to market developments, business opportunities and customer needs.
- **Dependency risk.** Lock-in created by a PSP owning merchants' payment tokens could threaten operational resiliency, reduce cost efficiencies and potentially impact the level of service merchants receive from their PSP.
- **Conflict of interest.** When SaaS companies or merchants attempt to move credit card and other personal cardholder data to a different PSP, the incumbent has no incentive to facilitate the data transfer. It is not uncommon for PSPs to impose high fees to export customer data to another vendor with significant lead time.

At the core of these concerns is the lack of control of payments data, stemming from an asymmetrical relationship with the PSP. As a result, many merchants and SaaS companies find their hands are tied with a single PSP relationship that might not serve their best interests. Recognizing this and taking steps to obtain true data ownership can empower businesses and SaaS companies, giving them greater control over their operations.

Multiple scenarios make payments data ownership critical

Losing control over payments data could result in adverse consequences in an unforeseen contingency, such as an outage at the PSP. It could also endanger the odds of success in a strategic event, such as M&A or a geographical expansion. Conversely, those that reclaim their ownership of payments data could be setting themselves up to better respond to market developments and opportunities. Below, we outline several scenarios where owning payments data can have significant business implications.

Impact on SaaS companies' valuation in M&A

If a SaaS company puts itself up for sale, investors will look at several points of strength and differentiation. One of the factors determining a SaaS company's valuation is churn, which measures the rate at which the company loses customers in a time frame. Operating an integrated software and payments model allows SaaS companies to reduce churn. After all, businesses will face higher switching costs in walking away from a software provider they rely on for accepting downstream payments from their customers. The payments revenue stream, on top of subscription fees, drives average revenue per user, another key metric that influences the valuation of a SaaS company.

An embedded payments model can help SaaS companies bump up their valuation multiple, but due diligence measures that reveal PSP lock-in could have an opposite impact on valuation. Limited flexibility to add or change a processor could prove to be a costly headache as growth expectations hinge on being able to seamlessly onboard a new processor for adding a new payment type or entering a new market. It could even be a deal-breaker for a strategic acquirer eyeing instant synergies by moving the target company's payments data in-house or to its existing PSPs.

PSP outage/downtime

Merchants and SaaS companies exclusively tied to a single PSP have limited redundancy and flexibility. Service disruptions such as outages and latency-related issues at payments vendors often have devastating repercussions, resulting in revenue loss and customer churn. Without control over their payments data, merchants and SaaS companies could be further hamstrung by their inability to move credit card data to another PSP seamlessly. The lack of flexibility to seamlessly switch between PSPs could deter businesses from taking decisive actions promptly to mitigate losses.

De-banking of higher-risk merchants and SaaS platforms

Data portability should be a top priority for businesses serving markets subject to high chargeback rates and regulatory attention, such as online gaming, pharmacies, cryptocurrency, non-profits and firearm retailers. Media reports point to growing instances of businesses having their accounts closed in these sectors. For example, the Financial Ombudsman Service in the UK saw a 44% jump in complaints related to de-banking during the 2023-24 financial year, according to data published by the Treasury Committee, with many claiming that their accounts were shut down on unreasonable grounds. With the prospect of sudden de-banking looming large over even medium-risk merchants, building redundancy and flexibility into the payment stack must be a high priority.

Higher-risk businesses are subject to the whims and vagaries of their payments provider, whose sudden change of policies can lead to their getting dropped with limited notice. While many high-risk merchants tend to utilize the services of PSPs specializing in their industries to avoid account suspension, placing all eggs in one basket is generally fraught with consequences. Specialized processors come with elevated pricing structures, and they may not offer all the capabilities (e.g., alternate payment methods, geographic reach) a merchant or SaaS company requires. Therefore, retaining data ownership is key for businesses to remain flexible and work with multiple PSPs to optimize costs and improve acceptance rates.

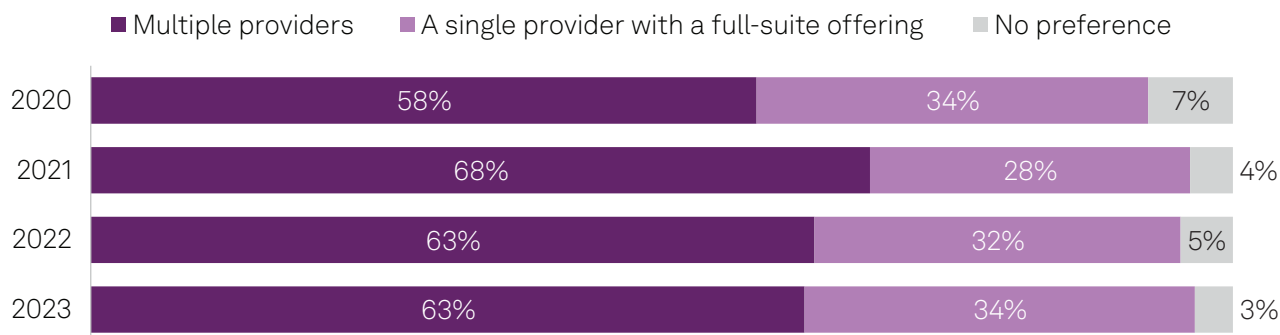
Need for payment orchestration and multi-PSP relationships

The utility of single-PSP relationships quickly runs out for businesses looking to expand into new markets, add payment methods, accept payments through multiple channels and drive optimization. As merchants and SaaS companies expand, onboarding additional PSPs becomes imperative to enable geographical and omnichannel expansion and provide local payment method coverage. Similarly, SaaS companies and large merchants may need to add more innovative PSPs into their environment to pursue new use cases and customer experiences (e.g., pay by link, tap on mobile).

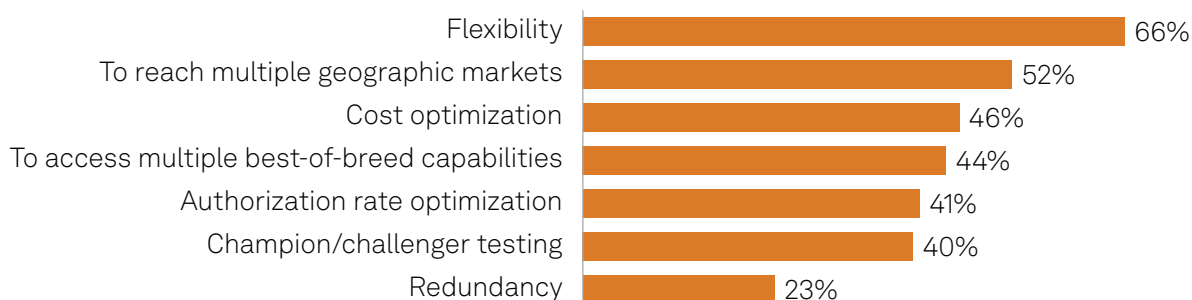
Growing businesses need multiple PSP relationships to execute multiple strategies, allocate resources efficiently and build redundancies. It is unsurprising that nearly two-thirds (63%) of merchants with 1,000+ employees indicate their preference is to use multiple processors, citing flexibility, the ability to reach multiple geographies and cost optimization as key factors.

Figure 3: Most large merchants prefer to work with multiple payment processors

1,000+ employees



Multi-processor drivers



Q. Thinking about the various components required to process a payment transaction, does your organization prefer to work with multiple providers or a single provider with a full-suite offering?

Base: All respondents (n=250).

Q. Why does your organization prefer to work with multiple providers to process payment transactions? Please select all that apply.

Base: Respondents whose organization prefers to work with multiple payment providers (n=124).

Source: 451 Research's Voice of the Enterprise: Customer Experience & Commerce, Merchant Study 2023.

As merchants' and SaaS companies' transaction volumes flow through multiple PSPs, they must orchestrate how each transaction will be routed to improve acceptance rates and costs. Using an orchestration layer allows them to direct payments to the most appropriate PSP based on various business criteria, such as cost, acceptance rate and use case. However, merchants and SaaS companies must take control of tokens before embarking on orchestration strategies. Leveraging PSP-agnostic tokenization and orchestration allows businesses to gain from the strengths of their payments providers while maintaining autonomy. Further, it enables them to solve specific business requirements, such as omnichannel processing and PIN debit routing.

PSP migration delays

Customer experience could suffer due to delays in the process of adding or changing a PSP. A critical part of PSP migration entails moving sensitive customer data, including credit card data and transaction histories, to facilitate recurring payments or one-off transactions. A business's current provider may levy an export fee or create laborious obstacles to retrieve cards tokenized with the provider. If merchants and SaaS companies require users to reenter credit card details and reauthenticate transactions to save cards on-site, it could introduce significant friction to the customer experience. Further, delays or an inability to recapture customers' credit card information could jeopardize revenue and result in significant churn.

The strategic role of PSP-agnostic tokenization

Reclaiming ownership of customer data requires an effective “decoupling” strategy that does not bind businesses to any single PSP, allowing them to increase autonomy and agility. Gaining control over tokens is a prerequisite to gaining control over payments data. While the traditional approach of tokenizing card data through PSPs has helped businesses gain compliance with PCI DSS, it has also chained them to their PSP, limiting their flexibility. There are two alternatives to using PSP-specific tokens.

One option is to invest in a card data management infrastructure. However, in-house vaulting activities require businesses to gain certifications associated with PCI DSS, shoulder significant operational complexity and take on the considerable risk related to storing payment data internally. Besides, most businesses are ill-equipped to build and handle their own tokenization processes. Consider that just 21% of businesses are “very confident” in their ability to protect customers’ payments data today, according to a 2023 survey conducted by 451 Research and commissioned by Bluefin.

The most advantageous alternative for many merchants and SaaS companies is to utilize an external tokenization service that allows them to offload the compliance burden and liability without sacrificing the control of payments data. A third-party tokenization provider enables businesses to outsource the technology to substitute sensitive card data with unique tokens. Because they are independent of PSPs, third-party tokenization providers help businesses ensure that their card data is both portable and readily accessible.

Third-party tokenization can be implemented in two ways: vaulted and vaultless. Vaulted tokenization involves storing the original data in a secure location, whereas vaultless tokenization secures the data at the source without storing the original data. When choosing between these methods, organizations should carefully consider their specific business needs and competencies.

Vaultless tokenization eliminates the need for a data vault. This is particularly important for larger and fast-growing businesses handling significant volumes of data because it can help to avoid performance issues. Additionally, it can help businesses comply with data sovereignty requirements more easily. Vaulted tokenization has traditionally been the preferred option for businesses in more heavily regulated industries such as financial services and government due to specific audit and access requirements.

We also advise merchants and SaaS companies to closely consider the total cost of ownership of each model. For many businesses, the pay-per-use pricing model typically associated with vaultless tokenization can generate greater cost efficiencies compared to the monthly “rental” model commonly associated with vaulted tokenization. This is especially the case as businesses accumulate larger numbers of tokens and as they tokenize additional types of infrequently used data (e.g., personally identifiable information, protected health information). However, businesses with relatively consistent data volumes seeking cost predictability may prefer the traditional vaulted pricing model.

Reaching the ideal state

Relying on PSP-agnostic tokenization services that offer data portability could be the first critical step to gaining autonomy from the limitations of a single PSP. Mastering control over customer payment data through the ownership of tokens helps set the stage for businesses to exploit multiple opportunities, from M&A to payment orchestration to operational resilience.

PSP-agnostic tokenization service providers vary based on capabilities and experience. Merchants and SaaS companies should seek out partners that maximize data security while supporting flexibility and scalability. Further, businesses should seek out partners that can abstract complexity, allowing them to liberate and operationalize their payments data without operational burden. Businesses should consider providers that offer tokenization in combination with a proxy capability. This enables real-time tokenization and de-tokenization of data, which can be transmitted to any PSP seamlessly. Additionally, when businesses add or modify a PSP, they do not have to pay to retrieve their tokens or generate new ones. Hence, they have complete control over their payment processes and can effectively manage payments to their preferred PSPs.

As the world is rapidly pivoting toward stringent data privacy and data sovereignty standards, SaaS companies and merchants will need to broaden the range of customer data that is subject to protection and take steps to limit the accessibility of sensitive data. For example, the General Data Protection Regulation in Europe and a potential US data privacy law could compel businesses to tokenize an increasing variety and quantity of valuable personally identifiable information or protected health information. Investing in a robust and flexible tokenization solution could be the way forward for managing payment and sensitive data securely across multiple processing platforms and navigating the growing complexity of data sovereignty and privacy requirements.



Content provided by



When evaluating tokenization providers, it is imperative to:

- Ensure you pick a service provider that can work across all payment platforms to avoid processor lock-in.
- Understand the implications to your business – start with a tokenization strategy that strengthens your current posture and considers all stakeholders. Don't forget to make internal stakeholders aware.
- Recognize that there is variation in token solutions – they are no longer a commoditized offering and some offer features and functionality that unlock real business value.

About Bluefin

Bluefin is the recognized integrated payments leader in encryption and tokenization technologies that protect payments and sensitive data. Our product suite includes solutions for contactless, face-to-face, call center, mobile, E-commerce and unattended payments and data in the healthcare, higher education, government and nonprofit industries. The company's 300 global partners serve 35,000 connected enterprise and software clients operating in 60 countries. Bluefin is a Participating Organization (PO) of the PCI Security Standards Council (SSC) and is headquartered in Atlanta, with offices in Waterford, Ireland and Vienna, Austria. www.bluefin.com

About the authors



Jordan McKee

Research Director, Fintech

Jordan McKee is research director of the 451 Research Fintech research and consulting practice within S&P Global Market Intelligence. He leads a team of analysts based in North America, Europe and Asia that provide guidance on trends at the intersection of finance and technology. As an analyst, Jordan's research focuses on digital payments and enterprise payments strategies. Jordan has been an industry analyst for more than a decade, having launched the payments coverage at 451 Research (acquired by S&P Global Market Intelligence in 2019) in 2013. Prior to this he has held research and advisory roles at Yankee Group, OnProcess Technology and FM Global.



Sampath Sharma Nariyanuri

Senior Research Analyst, Fintech

Sampath Sharma Nariyanuri, CFA, is a financial technology senior research analyst supporting 451 Research, a technology research group within S&P Global Market Intelligence. He is responsible for producing proprietary analyses of digital payments and digital banking sectors in Asia-Pacific. Additionally, he tracks global real-time payments and fintech funding trends. Sampath publishes in-depth market reports and articles, which estimate the market opportunities, evaluate the emerging business models and assess the implications of the digital transformation of financial services for industry stakeholders.

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

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

Copyright © 2024 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

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.