PAYMENTS ORCHESTRATION PLAYBOOK

Reducing The Regulatory Burden Edition

APRIL 2022

PYMNTS.com | Spreedly

PAYMENTS ORCHESTRATION

PLAYBOOK

Read the previous edition

■ FEBRUARY 2022

Payments Orchestration Playbook

PYMNTS.com | Spreedly

ACKNOWLEDGMENT

Payments Orchestration Playbook was produced in collaboration with Spreedly, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

EDITOR'S LETTER

In-store sales made a comeback in 2021, but online spending continues to grow in the wake of the global health crisis. The value of digital payments worldwide is expected to increase at a compound annual growth rate (CAGR) of 15% between 2021 and 2028. This growth includes business-to-business (B2B) and consumer-facing transactions, with 25% of United States B2B payments now conducted virtually.

The growing prevalence of digital payments has brought data security and privacy matters to the fore as lawmakers have stepped up efforts to keep transactions secure from the threat of malicious actors online. Some regulations go back more than a decade, such as the Payment Card Industry Data Security Standard (PCI DSS), launched in September 2006, which set security and privacy requirements for all entities processing or storing credit card information. Other rules have taken shape more recently as online fraud and privacy concerns escalate. Regulators in the European Union and the United Kingdom boosted customer verification and cybersecurity protections with the 2018 Payment Services Directive (PSD2). EU card networks, including Visa, Mastercard and Europay, have also developed a messaging protocol known as 3D Secure, aimed at allowing card issuers to authenticate cardholders making online or card-not-present (CNP) transactions. Strong Customer Authentication (SCA), a key PSD2 component requiring additional factors for authenticating online customers, just went into effect in the U.K. on March 14.

The increasing complexity and rising costs of regulatory compliance can significantly strain businesses, especially companies looking to establish operations in multiple markets where they may need to comply with a wide array of unique regulations. Compliance with PCI DSS requirements alone can cost companies upward of $50,000, and regulatory challenges can keep companies from innovating. A recent PYMNTS study found that 47% of merchants in the U.S. and Canada see regulatory barriers as the top reason they struggle to implement digital payments innovations.

Businesses need comprehensive regulatory compliance solutions to reduce costs and free up the capital necessary for innovation to attract and retain customers. The Payments Orchestration Playbook, a PYMNTS and Spreedly collaboration, analyzes the challenges and frictions today's businesses face in complying with PCI DSS, 3D Secure and other payments regulations. It also examines how payments orchestration can allow businesses to overcome these hurdles, minimizing costs and enabling the creation of new products to serve their markets.

Thought Leadership Team

PYMNTS.com

Feature Story

How Payments Orchestration Can Help eCommerce Merchants Offer **Seamless Payments In The Face Of Shifting Regulatory Requirements**

CONSUMERS HAVE COME TO EXPECT EASY, PERSONALIZED PAYMENT EXPERIENCES, ESPECIALLY WHEN SHOPPING ONLINE.

This means eCommerce merchants must find ways to stand apart in an increasingly saturated market by providing a diverse selection of swift payment solutions, said Yulia Drummond, CEO of eCommerce swimwear brand Voda Swim. The company currently supports a range of payment methods at checkout to meet its customers' needs, including mobile wallets such as Google Pay and Facebook Pay.

"More and more customers want conveniences," she said in a recent PYMNTS interview. "They want an easy checkout process that is seamless, and they want to pay with a payment method that is simple and that they [have come to trust] over the years."

Matching consumers' changing payment needs while ensuring that payments are secure can be tricky for merchants as their users continue to ask for a rising number of diverse payment solutions. This is especially the case as governments enact digital payment regulations aimed at protecting transactions and users' personal and financial information, such as PCI DSS and the EU's PSD2 law.

BALANCING SEAMLESS PAYMENTS WITH COMPLIANCE REQUIREMENTS

Offering consumers access to their preferred payment solutions means that merchants must work with an ever-growing list of payment service providers to ensure they can support multiple tools. eCommerce merchants must also be sure these transactions remain compliant with digital payment regulations, however, as lawmakers within the U.S. and the EU look to increase consumer protections while also making way for digital growth. Voda Swim's partnership with Shopify helps the company navigate these changing compliance requirements, Drummond explained, but meeting the compliance and seamless payment balance is becoming more critical for today's merchants.

"I do see the challenges for some companies of making sure the payments are processed securely from beginning to end while handling different payment service providers," Drummond said.

Finding technologies or industry partners that can help merchants easily manage their relationships with disparate payment service providers is key to remaining competitive as online payment regulations take shape across multiple markets. Solutions such as payments orchestration could play a key role in supporting these efforts by enabling companies to connect to their different payment partners more easily while also allowing them to manage the payment process on one platform.

"I do see how implementing payment orchestration helps ensure that the process is complete and without any issues for the consumer or the company," she said.

Implementing payments orchestration or similar systems that easily support diverse options for customers while ensuring transactions can be processed smoothly and in compliance with changing regulations is set to become more important for merchants in the coming years. This is the case for eCommerce entities especially, as a higher volume of transactions is sure to take place through digital channels, making the ability to support easy, secure payments essential for online businesses as they seek to optimize customer conversion.

MEETING NEXT-GEN PAYMENT NEEDS

Payment regulations will likely continue to shift in the next few years, especially as more consumers and businesses move online to conduct their daily transactions or meet other financial needs. This also means cybersecurity needs are likely to intensify, with lawmakers keeping a close eye on how information and payments data is shared, stored and protected.

"The bottom line is consumers need to be protected, and payments need to be secured," Drummond said. "The payments process will continue to evolve in that direction, and the lawmakers will create laws to ensure this is done properly."

Keeping pace with these regulations as well as consumers' payment wants and needs must be top of mind for today's merchants. Considering how payments orchestration could help them meet these needs more easily while remaining compliant with shifting laws is a must for businesses looking to keep customers engaged and protected.

© 2022 PYMNTS.com All Rights Reserved

Q&A

JENNIFER ROSARIO
Chief information security officer
Spreedly

How can payments orchestration help businesses achieve and maintain compliance with these regulations?

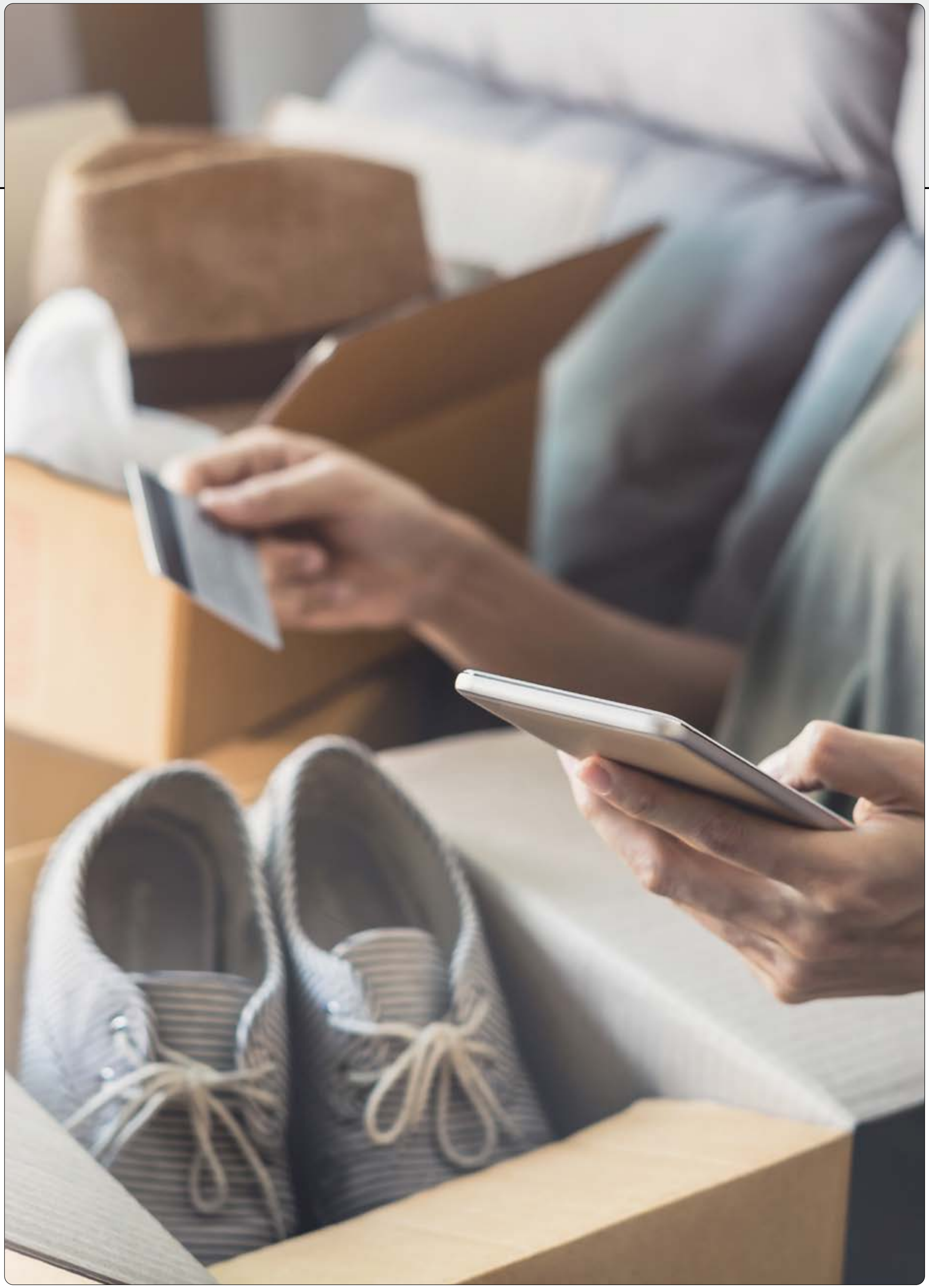
Staying on top of constantly changing payments regulations is difficult — and keeps organizations from focusing on their core value. Failing to adhere to mandates can lead to costly audits or even a shutdown of the ability to transact.

Payments orchestration is an important tool to help minimize the effort and risk that comes with regulatory burdens. A good orchestration partner will stay on top of the latest requirements and build support into the platform, [which] lets you focus on delivering a great customer experience and meeting revenue goals.

At the core of an orchestration solution is the storing, or vaulting, of customer payment details. This can help streamline the checkout for returning customers or make subscription transactions smooth each renewal period, but stored cards must be protected to avoid the crisis of a breach or PCI audit.

By leveraging the power of an agnostic vault and "universal tokens," organizations can transact with virtually any payments service while keeping data protected. This approach to storing payment details also significantly reduces PCI scope and helps avoid a costly, time-intensive, on-site data security assessment.

By implementing an orchestration layer into the payments stack, organizations can much more easily turn on (and even rapidly test) new payments service providers and other technologies. This mix and match approach offers true flexibility as needs change — including rapidly evolving regulatory requirements.



© 2022 PYMNTS.com All Rights Reserved

PYMNTS Intelligence

How Payments Orchestration Can Help Merchants Navigate **Changing Regulatory Requirements**

DESPITE IN-STORE SALES MAKING A COMEBACK IN 2021, ONLINE SPENDING SINCE THE PANDEMIC'S ONSET IN 2020 CONTINUES TO GROW.

eCommerce sales in the U.S. alone rose 14% year over year to reach $871 billion in 2021. Moreover, a surge in online and mobile payments adoption throughout the Asia-Pacific region and Europe is expected to help drive 18% annual growth in cashless transactions worldwide through 2025.

As digital payments become more prevalent, lawmakers have moved to develop regulations to keep transactions secure from fraudsters, money launderers and other malicious actors. Businesses seeking to accept an expanding variety of digital payment methods must keep pace with these rules, including PCI and 3D Secure requirements for credit and debit data as well as the SCA standard taking shape in the EU and the U.K.

Compliance with an ever-increasing number of payments regulations can prove costly, however. The cost of achieving Level 1 PCI DSS compliance, for example, can range from $50,000 to $70,000 for larger entities, threatening to place an increasing strain on companies as they attempt to recover from the pandemic's economic impacts as well as putting a strain on development teams as they look to refocus on core values. This month, PYMNTS Intelligence analyzes the growing regulatory burden that eCommerce businesses face and how merchants can reduce the cost of compliance by implementing a payments orchestration layer.

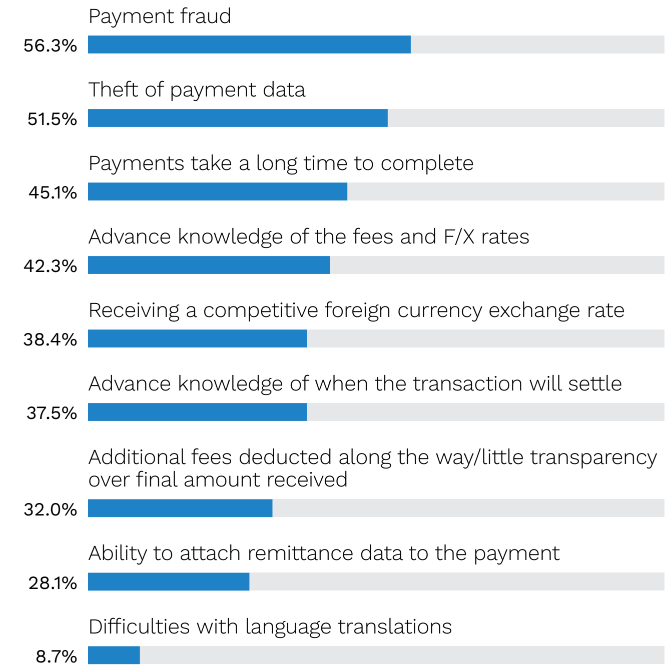
UNDERSTANDING COMPLIANCE'S COMPLEXITY

As digital becomes the preferred transaction channel for a growing number of consumers and companies, lawmakers worldwide have subjected companies' practices for the sharing and storage of online data to greater scrutiny. The PCI DSS data security standards came into place in 2006 in response to expanding online credit card sales. EU regulators soon followed by drafting the SCA standards as part of the PSD2 regulation, rules designed to provide another layer of authentication to digital transactions exceeding a specific limit.

Navigating this shifting regulatory environment can be difficult for eCommerce merchants, as it means maintaining compliance with complex, often overlapping security and privacy rules and keeping payments seamless and convenient for customers. April 2021 PYMNTS research revealed that up to 58% of consumers would abandon online purchases if their payments were declined, making it clear that swift, convenient transactions are necessary for today's digital shoppers. Another recent PYMNTS study found that regulatory barriers were one of the major challenges preventing migration to digital B2B payment solutions for 47% of U.S. and Canadian merchants. The April 2021 PYMNTS report also found that 56% of companies said payments fraud was the top worry in cross-border transactions. As online customers continue to do more shopping outside their native countries, businesses looking to support easy, convenient cross-border payments will need to maintain regulatory compliance in multiple markets.

FIGURE 1:

Businesses' top concerns in cross-border transactions
Share of businesses identifying select top pain points



Implementing a payments orchestration layer is one way for companies to remain compliant with multiple regulations without introducing undue customer friction into the payments process. Payments orchestration can offer businesses a competitive edge by aggregating all payment relationships in one place, simplifying the overall payments process and reducing the confusion caused by diverse compliance needs.

Payments orchestration has many advantages for eCommerce merchants seeking to expand into new markets or target new customer bases to benefit from the ongoing digital boom. Finding the right payments orchestration partner could substantially reduce businesses' regulatory burdens, allowing them to reserve valuable resources to create innovative products and services for customers.

NEWS & TRENDS

REGULATORY **FRICTIONS AND CHALLENGES**

TECH FIRMS FACE BIG FINES OVER PERSONAL DATA STORAGE VIOLATIONS

Online financial regulations have shifted rapidly in the EU, where lawmakers are moving swiftly to enforce General Data Protection Regulation (GDPR) requirements for data sharing and storage. Three years after ratification, failure to comply with GDPR is proving costly, with Big Tech players such as Facebook and Google facing hefty fines for violating rules regarding the storage of personal information.

Regulators in Luxembourg issued the largest GDPR penalty on record to eCommerce platform Amazon last year, a fine of approximately €746 million ($811 million USD).

Implementing technology such as tokenization to protect users' data is one way these companies could ensure compliance with the regulations. The technology secures users' personally identifiable information (PII) and payments data by encrypting it and storing it with a trusted third-party provider for protection. It then initiates transactions with secure tokens that disappear after a single use. Companies seeking to remain competitive in these markets must remain vigilant about data privacy rules as the regulatory landscape continues to shift.

FRENCH COURT UPHOLDS GOOGLE GDPR FINE

Search engine and technology provider Google is one firm facing significant penalties for failure to comply with GDPR in its storage of European consumers' sensitive information. France's highest administrative court, the Conseil d'État, recently upheld a January 2022 fine issued by the country's data privacy watchdog, the Commission nationale de l'informatique et des libertés (CNIL), for the tech giant's cookie-storing policy.

CNIL fined Google approximately €100 million ($109 million USD) for how it stored website cookies, citing that its policy made it challenging for EU consumers to avoid online trackers of such data or to opt out of sharing it — rights protected under GDPR. The court's ruling to uphold the penalty indicates the rising need for companies of all sizes to ensure they can remain compliant with GDPR and other regulations for sharing and storing online data.

UK MERCHANTS STRUGGLE TO OVERCOME SCA TRANSACTION BARRIER

Merchants must also find ways to ensure they can provide the seamless payment experiences customers expect while remaining compliant with emerging payment regulations. U.K. merchants, for example, are currently bracing for SCA requirements to become mandatory by the end of the month, potentially adding undue frictions to customers' purchases if mishandled.

SCA, a tenet of the EU's PSD2 regulation, requires transactions above a specific limit to be verified using two-factor authentication (2FA), and one recent report found that European customers abandon 29% of the transactions requiring it. This cart abandonment causes merchants to miss out on a collective €90 billion ($98 billion USD) in annual sales, so reducing this point of friction is key for businesses. Adding a payments orchestration layer that can consolidate payment options and smooth transactions on the back end is one way merchants can do so.

PAYMENTS ORCHESTRATION DEVELOPMENTS

WHY PAYMENTS ORCHESTRATION IS KEY TO CONSOLIDATING PAYMENT COMPLEXITY

As the payments ecosystem grows more complex, merchants must find ways to support a rising variety of payment tools and channels to meet customers' needs. These shifts mean that partnering with just one or two payment service providers (PSPs) is no longer enough to allow businesses to remain competitive — a change pushing PSPs themselves to team up to offer diverse services to merchants.

Justin Benson, CEO of payments orchestration provider Spreedly, told PYMNTS in a recent interview that payments orchestration tools can enable PSPs to more easily consolidate offerings, providing more seamless solutions to merchants looking to enable easy, convenient sales via multiple channels and payment methods. This can help businesses optimize payments, he continued, to increase customer conversion and revenue. Integrating payments orchestration is likely to grow more critical for businesses across multiple industries as commerce becomes increasingly digital.

FRAUD AND PAYMENT CHALLENGES

BUSINESSES CITE RISING CONCERNS OVER CROSS-BORDER PAYMENT FRAUD

Commerce is also growing increasingly global, with more and more businesses in various industries now offering products and services in international markets. This makes it critical that companies can send and accept cross-border payments safely and seamlessly. Still, recent PYMNTS research noted that many firms report fraud concerns related to these payments. The report found that 56% of companies were worried about cross-border payments fraud, while 52% of respondents admitted concerns about the potential theft of payment data.

Protecting against such fraud requires companies to rethink overall payments strategies and means companies must work to remain compliant with a diverse set of financial regulations aimed at warding against these attacks. Implementing a payments orchestration layer could help international firms remain compliant with the unique financial regulations of multiple markets without placing undue friction on the cross-border payments process. Implementing such tools can offer companies access to a broad range of key solutions and tools to help create greater transparency surrounding potential fraud attempts, explained Spreedly's head of product Andy McHale in an October 2021 PYMNTS interview. This can help them dismantle more sophisticated forms of fraud, an increasing necessity for companies as commerce becomes more global.

PAYMENTS ORCHESTRATION PLAYBOOK

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Spreedly

Spreedly's Payments Orchestration platform enables and optimizes digital transactions with the world's most complete payment services marketplace. Global enterprises and hyper-growth companies grow their digital businesses more quickly by relying on our payments platform. Hundreds of customers worldwide secure card data in our PCI-compliant vault and use tokenized card data to enable and optimize more than $30 billion of annual transaction volumes with any payment service. www.spreedly.com

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at feedback@pymnts.com.

DISCLAIMER