Unified Commerce

A New Opportunity for Payments

CAYAN®

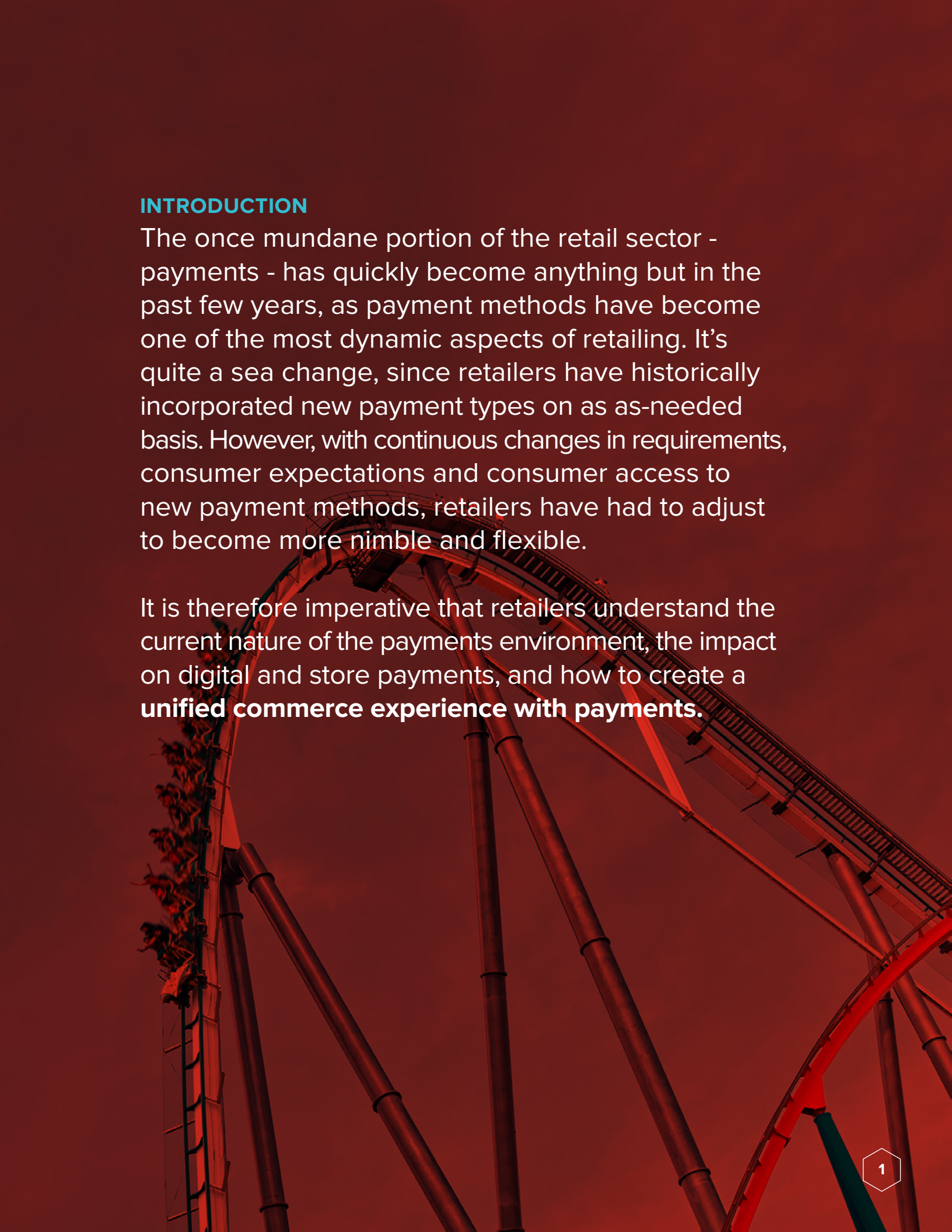
commerce cloud

TABLE OF CONTENTS

INTRODUCTION

The once mundane portion of the retail sector - payments - has quickly become anything but in the past few years, as payment methods have become one of the most dynamic aspects of retailing. It's quite a sea change, since retailers have historically incorporated new payment types on as as-needed basis. However, with continuous changes in requirements, consumer expectations and consumer access to new payment methods, retailers have had to adjust to become more nimble and flexible.

It is therefore imperative that retailers understand the current nature of the payments environment, the impact on digital and store payments, and how to create a **unified commerce experience with payments.**

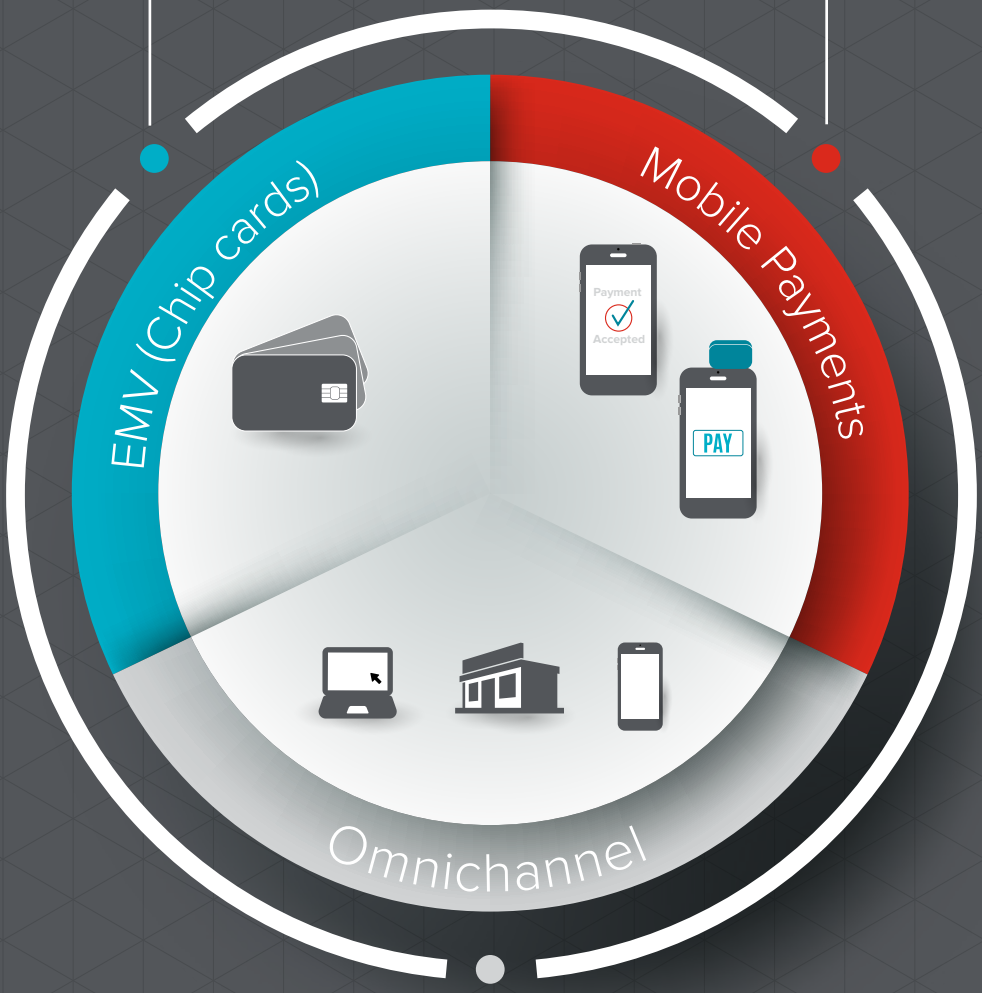


The changing state of payments

While the payment industry is seeing changes from all areas, EMV, mobile and omnichannel have seen the most significant changes over the past two years.

Europay, MasterCard, and Visa (EMV) has long been the chip-based standard in Europe and much of the world.

Fast growing mobile payments can be broken down into two distinct parts: mobile device via a card reader, and payments made with a mobile device.



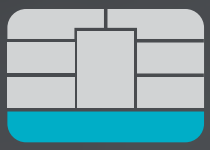
A seamless shopping experience through the entire shopping journey, online to in-store

EMV

Europay, MasterCard, and Visa (EMV) has long been the chip-based standard in Europe and much of the world. However the US, the last country within the G20 to adopt EMV, has been a laggard in implementing the technology. This all changed for the US in October 2015 when liability shifted from banks to merchants. Despite the decades of learning from the European deployment of EMV, The Strawhecker Group says only 37 percent of businesses are able to accept chip enabled cards.[1]

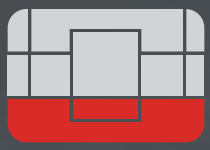
There are many reasons why the US adoption of EMV has been slow. First and foremost is the large cost associated with enabling EMV; 60 percent of POS devices still need to be upgraded to accept the newpayment type.[2] Next is the widely held belief that the chip-and-signature method adopted by the US is far less secure than the chip-and-PIN method used in Europe, thus minimizing any security gains. Chip-and-signature requires a user to sign, either on screen or paper, to authenticate a transaction whereas chip-and-PIN requires users to enter a PIN to authenticate a transaction. Thirdly, consumers are not using chip-enabled cards because they do not have them! [3]

It is estimated that only 25 percent of cards were chip-enabled at the end of 2015 and only 73 percent are expected to be enabled by the end of 2016. With the US implementing a less secure version of a 20-year-old technology, and mobile payments (Apple Pay, etc.) on the rise, the real story on EMV is that it is likely a Trojan Horse for NRF/mobile payments.



25%

of cards were chip-enabled at the end of 2015



37%

of businesses are able to accept chip enabled cards.

73%

of cards are expected to be enabled by the end of 2016

[1] "Survey: Adoption of chip-enabled credit cards falls behind," USA Today, February 17, 2016
[2] "4 Important Takeaways From Our EMV Webinar," Cayan, January 25, 2016
[3] "One of Every Four Debit Cards to be Converted to Chip by End of 2015: *Cost of Chip Cards is Double That of Magnetic Stripe*," Pulse, September 10, 2015

Mobile

In the not so distant past, mobile payments were considered a niche technology due to constantly changing players and confusion in the market. However, today consumers are more comfortable with mobile payments, driving adoption.

Mobile payments can be broken down into two distinct parts: payments accepted through a mobile device via a dongle or card reader, and payments made with a mobile device. Payments accepted through a mobile device via a dongle or card reader have been adopted more quickly, mainly because they are easier to implement. Small businesses, previously dependent on cash because they could not support a POS system, found an affordable option in payments accepted through a mobile device via a dongle or card reader.
Some examples: food trucks or independent sellers transacting at an fair.

Payments made with mobile devices are not as easy to implement, mostly because they rely on consumer technology. Even though manufacturers and developers started creating phones and software that made mobile payments possible, it took time for consumers to adopt these new devices.

Most payments made with mobile devices fall into one of the following categories:

A merchant-specific wallet, like the Starbucks app

A wallet that enables card emulation and can be used anywhere NFC is accepted—an example would be Apple Pay

Merchant-agnostic wallet based on partnerships with credit card issuers—an example would be PayPal mobile wallet

A mobile loyalty app—an example would be CVS

Omnichannel

With a focus on providing a seamless shopping experience through the entire shopping journey, online to in-store, omnichannel offers a unique opportunity when it comes to payments. The traditional siloed way of managing card transactions no longer addresses the needs of consumers. Consumers want payment services that revolve around them, and retailers must find a way to seamlessly cross channels with them. The ability to streamline POS, digital and payments will allow retailers to create a unified shopping experience.

And the benefits to omnichannel are clear[5]

71%

of consumers expect to view in-store inventory online.

50%

of consumers expect to buy online and pick-up in store.

20%

of consumers say retailers should provide a consistent experience across all devices.

3.5x

Omnichannel customers spend 3.5 times more than single-channel shoppers.

107%

For online sales with in-store pick-up and return, retailers can expect a net sale of 107%.

89%

is the average customer retention percentage for companies with extremely strong omnichannel engagement.

[5]Seizing the OmniChannel Opportunity, Cayan, April 27, 2016

Understanding Digital Payments

A digital or online payment is known as an electronic payment because it does not involve cash or a paper check.

Electronic payments fall into three categories:

One-time customer-to-vendor payment—most commonly used when shopping online at an eCommerce site

Payment used to pay a bill through a scheduled debit from a user's banking account Automatic bank-to-vendor

Payment which is offered through a banking service most commonly called online bill pay

Over the years, consumers have become increasingly comfortable with using credit and debit cards online. Forrester Research estimates that online sales will increase in the US by $51 billion from 2015 to 2017. The act of using a credit or debit card online is called a card-notpresent (CNP) transaction.

DIGITAL PAYMENT SECURITY

As online shopping continues to grow so does the risk of card-not-present fraud. CNP fraud is the unauthorized use of a credit or debit card number, security code, and/or cardholder's address to purchase products or services in a setting where a retailer is taking payment from a customer outside of a face-to-face setting. CNP fraud accounts for about 16 percent of losses. According to Cybersource, eCommerce fraud is 0.9 percent of all online revenue. CNP fraud plagues all 80 countries that use EMV. Physical transactions allow for something called the ownership factor; the merchant sees the cardholder and their verification. As this cannot happen online, merchants and issuers use a combination of processes to prove that the card is being properly used.

Forrester Research estimated that online sales would increase in the United States by

$51 billion from 2015 to 2017.

[6] "Online Merchants Are Beating Fraud, But the Gains Are Costly, CyberSource Study Reveals," Digital Transactions, April 29, 2016

BUILDING BLOCKS OF FRAUD PREVENTION

Retailers, payment processors, and eCommerce providers continue to look for techniques to authenticate online transactions. Authentication can occur through the ownership (having a card or the IP address linked to it), knowledge (PINs and addresses) or information factors (fingerprints and personal details). When authenticating a card one or more of these factors must be provided by the cardholder.

All CNP transaction types use information factors to verify the identity of the cardholder. They can also use ownership factors like an individual's IP address. Often, merchants will use multiple factors to determine whether the individual can use the card. Intermediaries, like major credit card companies, can be brought in to help retailers limit their CNP risk. These intermediaries offer such services as collecting data from multiple retailers and checking cardholder information for verification or performing risk assessments and suggesting secondary forms of authentication.

AUTHENTICATION BEST PRACTICES

There are various forms of authentication techniques used today. Some of the most popular techniques include:

Behavioral Biometrics
based on an individual's behavior patterns

End-Point Identity
like an IP address, identifying the device a customer is using

IVR Voice Authentication
based on a pre-recorded voice message or PIN

Physical Biometrics
based on an individual's physical characteristics

Random Knowledge Authentication
based on a user answering one or more secret questions

Retailers can conduct one or all of these CNP authentication techniques but they do have upfront costs, routine maintenance costs, and risk of cart abandonment. In addition, the effectiveness of any one technique varies from retailer to retailer.

Today, retailers most commonly use three approaches to authenticate CNP transactions. The three approaches, which use one or many of the authentication techniques, are alternative intermediaries, account issuance or standard intermediaries. For account issuance, a customer will set up a profile with basic information like username, telephone number, password, and address. The retailer will then send a token to the customer to ensure they received valid information—like sending an email to a new user to validate a user profile. If the customer then logs on using a different IP address they may be required to perform random knowledge authentication—like being told a site does not recognize a log-on from a new device.

With a standard intermediary, cardholder information is often re-entered for each purchase to prove possession of the card. Since this information is not stored in the magnetic stripe or chip of the card it shows the card was not part of mass fraud. The use of an alternative intermediary is done by third parties with stronger authentication capabilities. An example of this would be paying for an online purchase via PayPal.

Understanding Store Payments

The store, where more than 90 percent of all retail transactions still occur,[7] uses card-present transactions. This means the customer and their debit or credit card are physically present at the time of a purchase.

PAYMENT TERMINAL CONFIGURATIONS

There are three main types of payment terminal configurations that are used in the store to accept credit and debit card transactions.

INTEGRATED PAYMENT SOLUTIONS

An integrated payment solution communicates directly with the point of sale application. It receives needed information from the POS application, such as the tender amount, and in turn sends information such as encrypted card data back to the POS.

SEMI-INTEGRATED PAYMENT SOLUTIONS

A semi-integrated solution, while maintaining communication with the POS application, sends card data directly to a bank or payment gateway for authentication. The authorization is then communicated back to the POS application via the payment terminal.

NON-INTEGRATED PAYMENT SOLUTIONS

A non-integrated solution has no communication with the POS application. All card authorization and processing is done in isolation on the payment terminal.

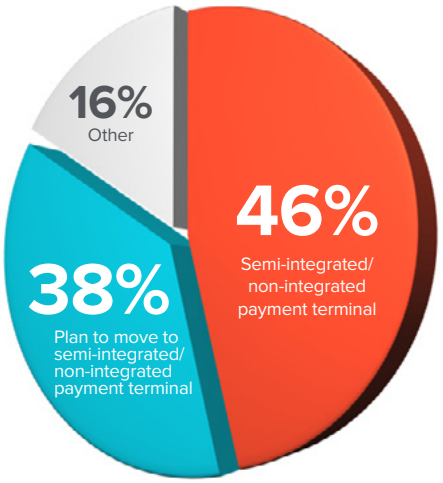
STORE PAYMENTS SECURITY

The adoption of EMV may somewhat deter card-present fraud, as it requires the chip-based card to be present, it does not protect against all card-present fraud. With the implementation of chip and signature the possibility of fraud still exists as no PIN is required, only a signature. However, the bigger threat for retailers centers on security breaches. Therefore retailers must rely on other best practices for security payment card data such as end-to-end encryption (E2EE) and tokenization.

CARD-PRESENT BEST PRACTICES

End-to-end encryption allows retailers to remove encrypted data at rest. Tokenization enables retailers to eliminate sensitive information from the network. Retailers are trending toward removing sensitive data from their own environment by using semi-integrated or non-integrated payment solutions with a direct to bank or vendor hosted gateway.

Based on Boston Retail Partners' special report "Payment/Data Security in an Omnichannel World," 46 percent of retailers are using a direct configuration from a semi-integrated or non-integrated payment terminal to bank or vendor-hosted gateway. An additional 38 percent, based on the same report, are planning to move to semi-integrated or non-integrated payment terminal to bank or vendor-hosted gateway in the next three years.[8]



[7] "Quarterly Retail E-Commerce Sales: 1st Quarter 2016," U.S. Census Bureau News, U.S. Department of Commerce, May 17, 2016
[8] "Special Report: Payment/Data Security in an Omnichannel World," Boston Retail Partners, 2016

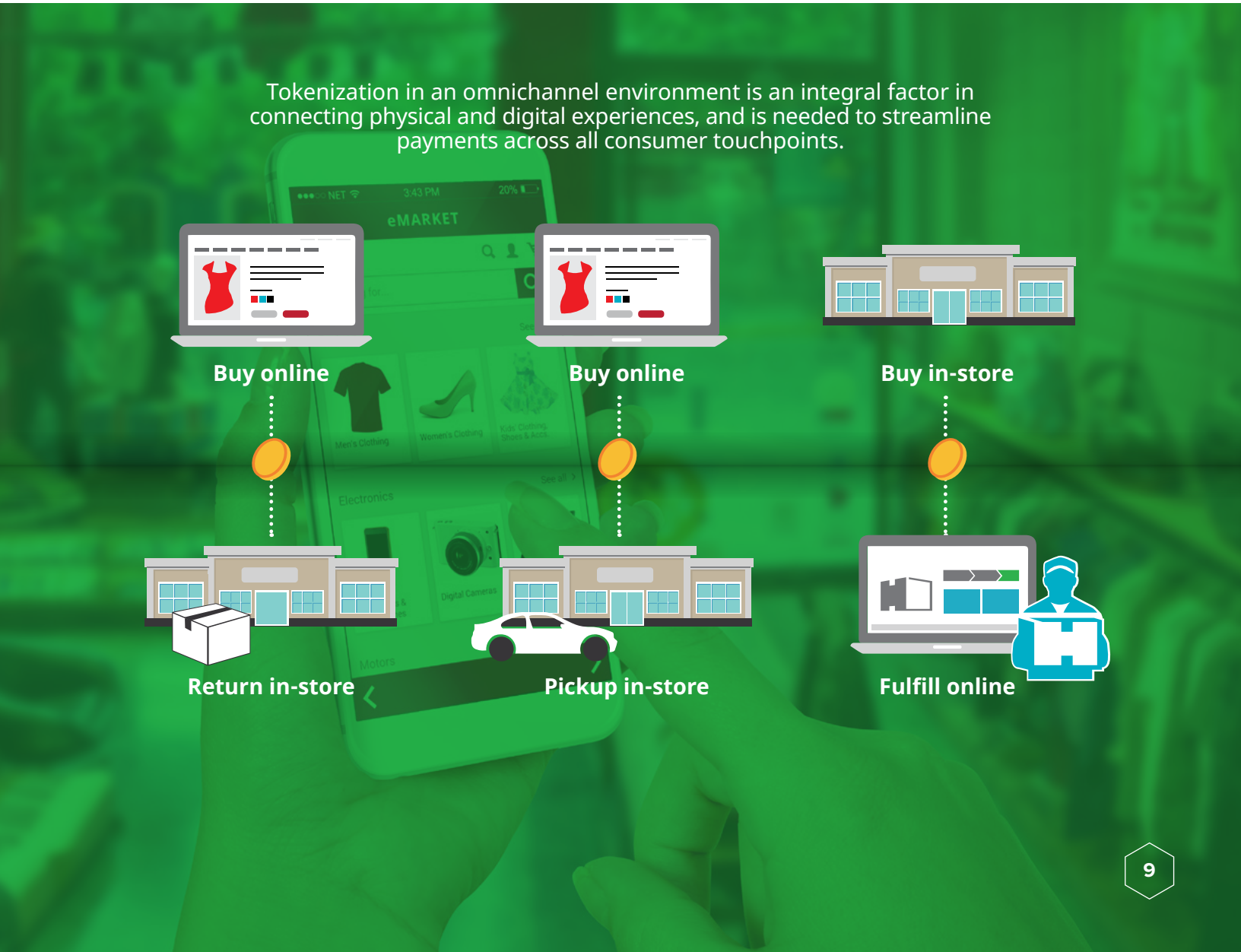
Blending Physical and Digital Commerce

CONSUMER EXPERIENCE

Consumers want a unified shopping experience, and this extends to payments, which are a defining moment in the shopping journey. And, according to a recent Cayan report and LuxuryDaily.com, 62 percent of retailers named customer identification and personalization of customer experience among their top three customer engagement priorities. Payments solutions need to be as seamless as any experience in an omnichannel environment and having a single view of the consumer applies to their payment interaction.

Tokenization in an omnichannel environment is an integral factor in connecting physical and digital experiences, and is needed to streamline payments across all consumer touchpoints. When a token is assigned to a customer's payment card, retailers are able to see behavior and spending patterns, which in turns helps them personalize their customer engagements.

With access to customer history, past purchases, payment types and other customer data, tokenization allows retailers to better reach customers when, where and how they want to shop all while keeping transaction data safe and secure.



CAYAN + salesforce commerce cloud

Our Partnership

Salesforce Commerce Cloud empowers retailers to unify customer experiences across all points of commerce, including web, social, mobile and store. From shopping to fulfillment to customer service, the Commerce Cloud delivers 1-to-1 shopping experiences that consistently delight customers, driving increased engagement, loyalty and conversion. With embedded predictive intelligence and a robust partner ecosystem, the Commerce Cloud delivers customer satisfaction and growth from planning to launch and beyond.

Cayan solves the challenge of supporting the payment types and payment platforms that customers demand. Engagement at the point of sale is rapidly evolving. Advanced payment options from Apple Pay, Android Pay, Samsung Pay and others, as well as new form factors including EMV, NFC and QR codes, have turned a simple transaction into a valuable customer interaction. Integrated with your point-of-sale system, Cayan provides retailers a true path forward by being the only flexible payment solution that scales to their business's growth of their business and industry needs. Paving the way, Cayan/Demandware retailers have true unified commerce capability with the same payment token being used for e-commerce payments and in-store transactions, further expanding the retail experience that can be offered to today's consumer.