csg Forte

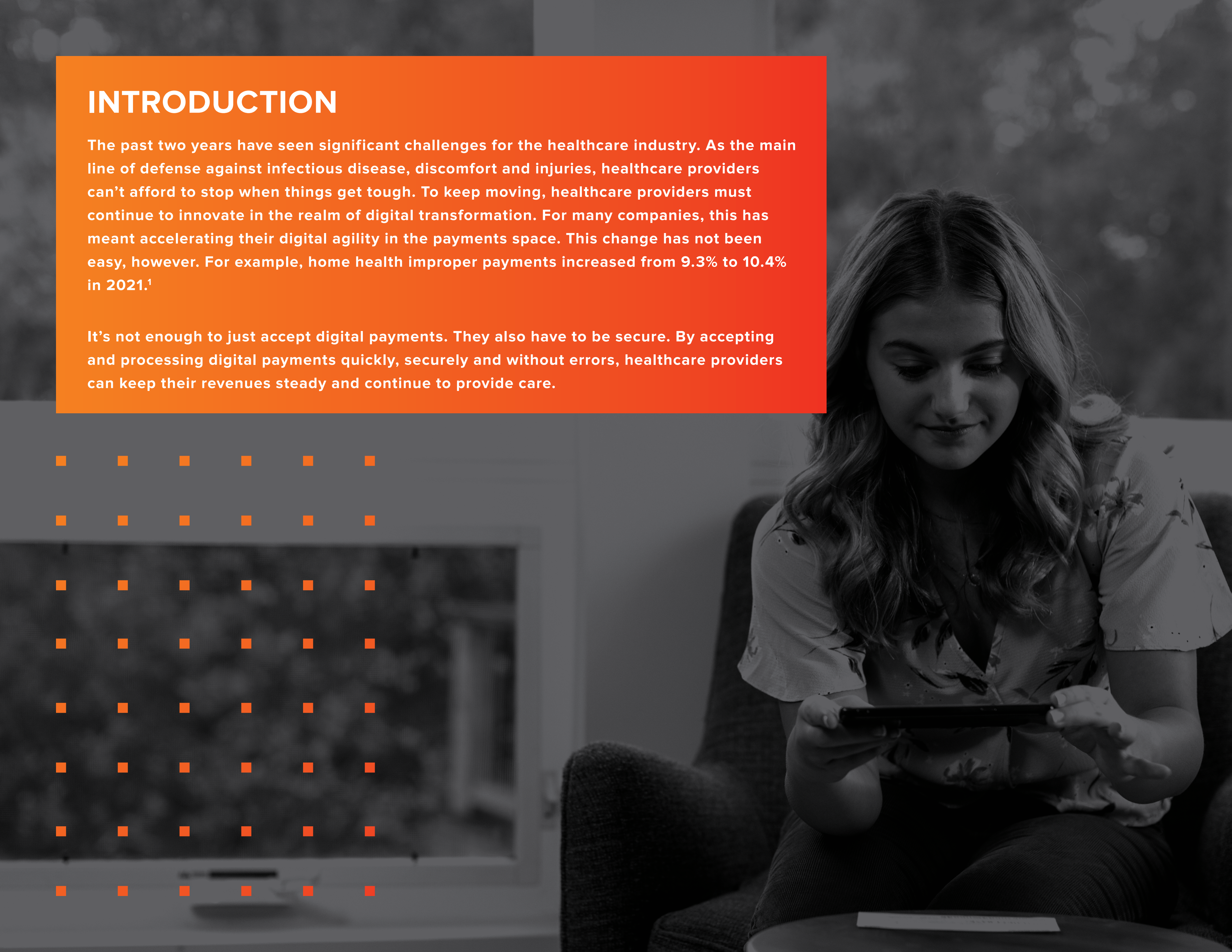
3 STEPS TO ENSURE PAYMENTS SECURITY

How healthcare companies can increase revenue with secure digital payments

INTRODUCTION

The past two years have seen significant challenges for the healthcare industry. As the main line of defense against infectious disease, discomfort and injuries, healthcare providers can't afford to stop when things get tough. To keep moving, healthcare providers must continue to innovate in the realm of digital transformation. For many companies, this has meant accelerating their digital agility in the payments space. This change has not been easy, however. For example, home health improper payments increased from 9.3% to 10.4% in 2021.[1]

It's not enough to just accept digital payments. They also have to be secure. By accepting and processing digital payments quickly, securely and without errors, healthcare providers can keep their revenues steady and continue to provide care.



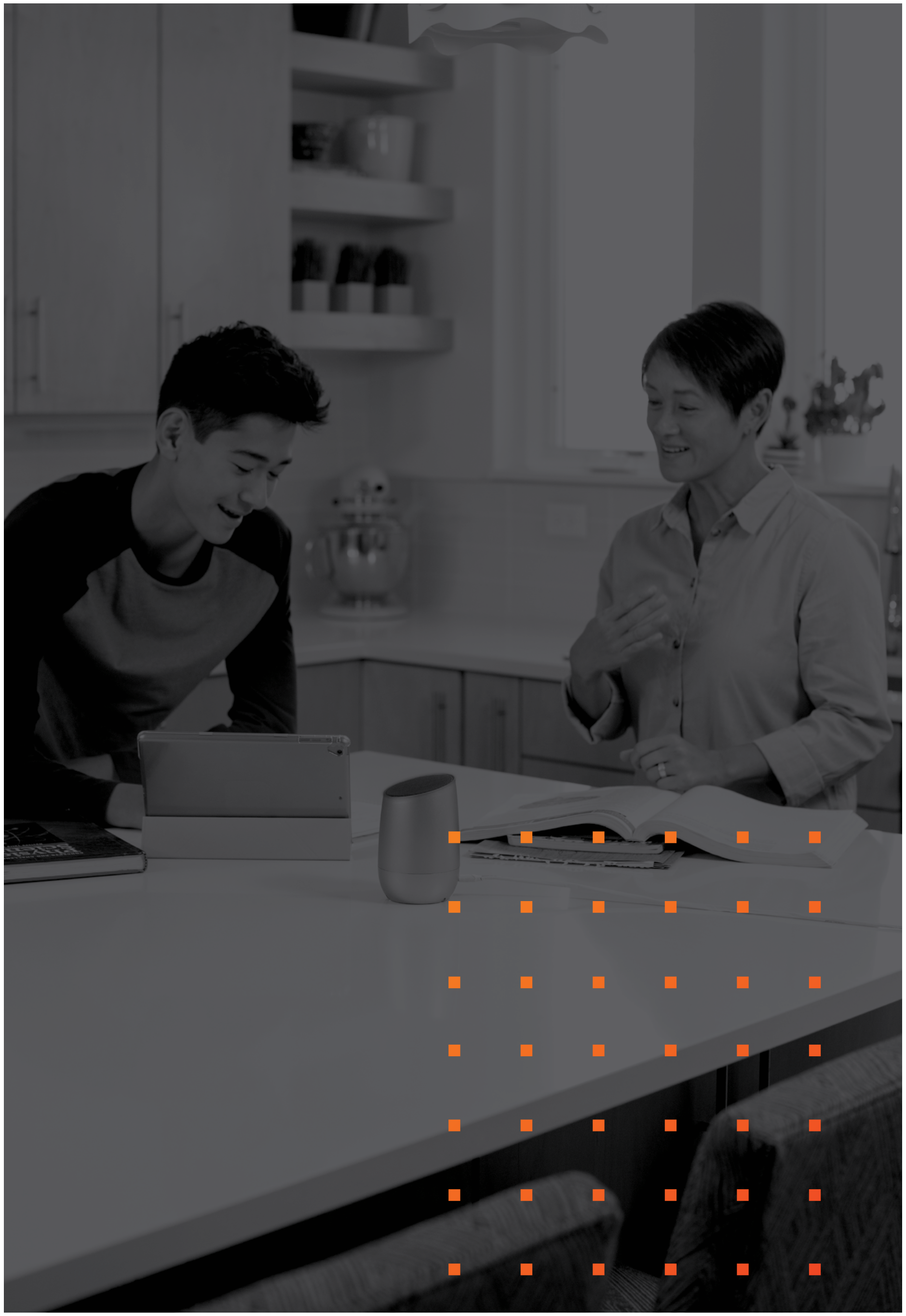
The explosive growth of digital payments hasn't slowed since it began. For healthcare, out-of-pocket expenses have shifted from cash and into the digital sphere. This is in line with the wider trend towards digital payments. Accenture predicts that almost 420 billion global transactions worth $7 trillion will shift from cash to cards and digital payments by 2023.[2] By leaning into this trend, hospitals, practitioners, and medical groups can ensure their operational efficiency even in the face of an ongoing or future global pandemic.

Consumer interest in digital payments is also at a new high. 95% of patients indicate that they would be willing to pay a bill online, while only 20% of healthcare businesses have the infrastructure to support them.[3] This makes digital payments a vital component of any digital transformation plan in the healthcare industry. Implementing a digital payment solution may be the prescription but adhering to the goal of a great digital payment experience remains a challenge. To be successful, healthcare companies must partner and integrate with a digital payments provider so that they can not only accept digital and contactless payments, but also mitigate the threat of fraud, maintain compliance and keep their customer's payments secure.

1) Compliance—Organizations need to secure their offering to comply with constantly changing regulations. They will need to be ready to face auditing and support end-customers with their compliance requirements. Otherwise, they face fines and penalties.

2) Protect customer data—With constantly evolving security risks, payment processors need to utilize powerful technology to protect against data breaches. Robust security features can protect against the most pervasive methods of fraud.

82 percent of Americans using digital payments and prevalent fraud on the rise, it's time to level up payments security.[4] Read on to find out the three steps companies can take to maintain cash flow from digital payments while keeping consumer information and payments secure.



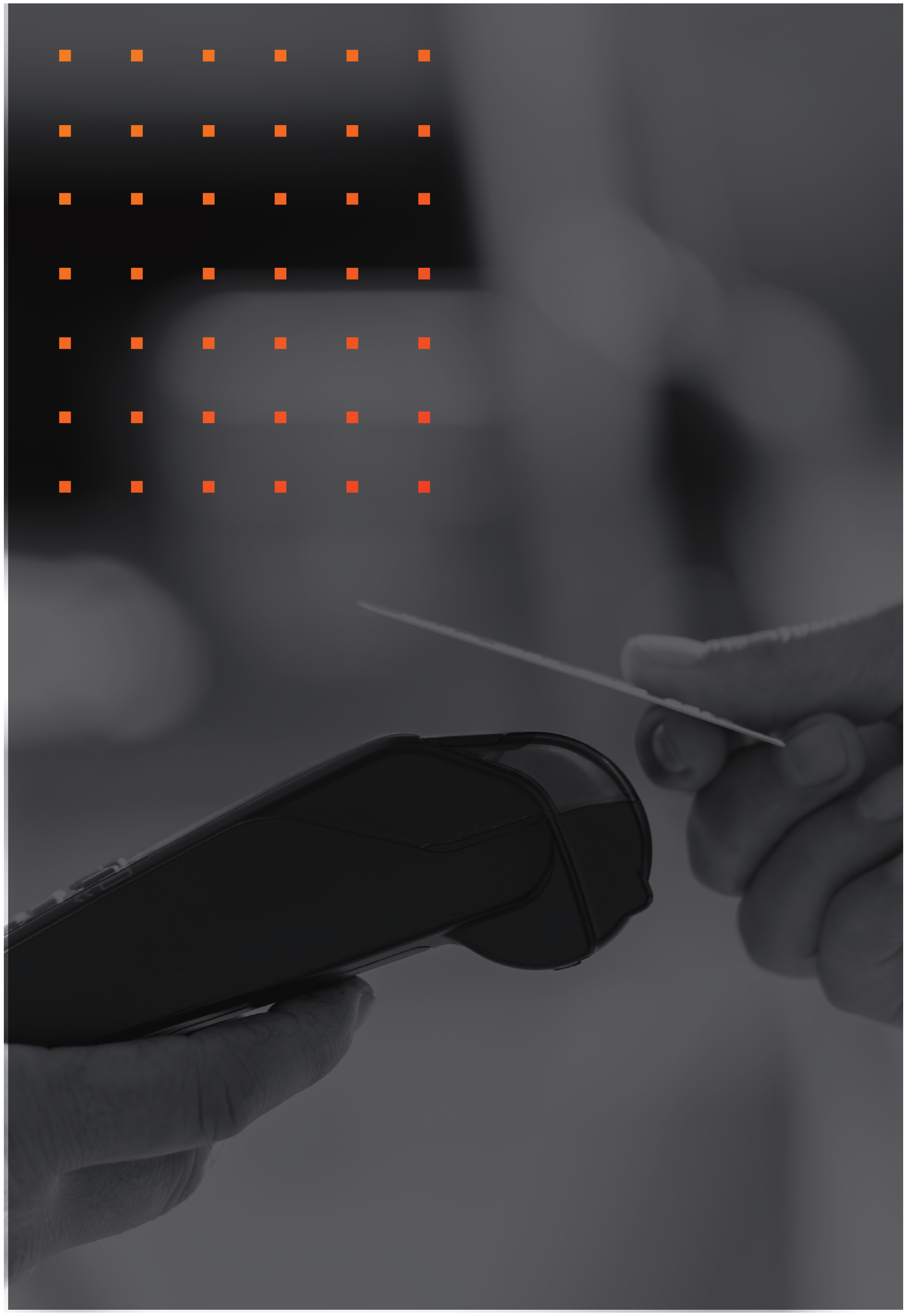
STEP 1: UNDERSTAND COMPLIANCE WITH KEY INDUSTRY STANDARDS

It may sound cliché, but one of the best defenses against online payments fraud is a good offense. And part of that offense is an understanding of the standards and procedures that are in place to prevent fraud. Once companies know what they're up against, they can better prepare themselves to stop fraud before it starts.

Compliance with these standards can help form the foundation of a payment security and fraud prevention program. Companies with a fraud program in place reduced their expenses responding to fraud by over 40 percent.[5] Familiarizing yourself with key industry bodies and standards like the Payment Card Industry Data Security Standard (PCI-DSS), International Standards Organization (ISO) and National Automated Clearing House Association (Nacha) can help companies and merchants defend themselves and their customers against fraud.

PCI-DSS

PCI-DSS is the Payment Card Industry Data Security Standard, with the goal of protecting cardholder data and maintaining payment security. While 59 percent of in-person payments are with cards, consumers can also store their credit card information online for automatic payments or enter it for one-time payments.[6]



Any organization that processes card payments needs to comply with 12 PCI-DSS requirements, including but not limited to:

- Protecting stored cardholder data
- Encrypting transmission of cardholder data across open, public networks
- Developing and maintaining secure systems and applications
- Restricting physical access to cardholder data
- Regularly testing security systems and processes[7]

Organizations have three ways to ensure they are PCI-compliant. The first option is to conduct their own PCI compliance assessment by using the forms located on the PCI Security Standards Council website. The second option is to work with a third-party qualified security assessor (QSA) approved by the PCI Security Standards Council and then provide a copy of your Attestation of Compliance and Scan.

However, the most convenient option for companies and merchants is to participate in a payment provider's PCI-DSS compliance program to streamline the compliance validation process. Look for payment platform providers who work with both an Approved Scanning Vendor (ASV) and a Qualified Security Assessor (QSA) for the card associations.

ISO

The International Standards Organization (ISO) develops global best practices and processes for businesses to follow, ranging from food safety to energy management to IT security. For businesses processing secure customer information (like payment information), the ISO 27001 standard is especially important.

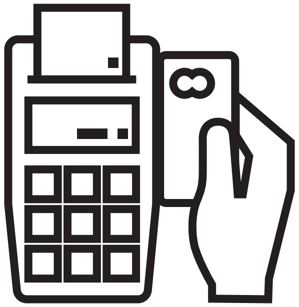
That standard provides "requirements for an information security management system… enabl[ing] organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties."[8]

At a high level, ISO 27001 requires organizations to complete an annual assessment of their physical and in-person security procedures. For companies accepting payments, this helps them ensure that their customers' sensitive financial data is secure not just in person, but also on-premises.

NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION (NACHA)

Nacha facilitates the administration, development and government of the ACH network, which is the linchpin for the electronic movement of money in data in the United States. In 2020 alone, nearly $62 trillion moved across the ACH network.[9]

As the facilitator of a vital network, Nacha regularly updates its standards through periodic rule changes to more efficiently govern the ACH network. By creating new rules while also establishing the roles and responsibilities of participants in the network ecosystem, Nacha fosters a safe and innovative environment for the payments industry.



STEP 2: DEPLOY THE RIGHT PAYMENTS SECURITY TECHNOLOGY

Deploying the right payments security technology not only ensures compliance—it also ensures that your customers' private data remains secure. But as technology advances, so do methods of fraud. Several payment security technologies offer robust protection against bad actors.

END-TO-END (E2E) ENCRYPTION

How It Works

E2E encryption protects data as it travels across a network by encrypting data through a random alphanumeric code. The data can only be decrypted when it reaches its final destination through the use of a private key.

Why It's Important

This method provides superior protection because the encryption key is housed only at the final destination. Even if the data were to be intercepted during transmission, the random code would be worthless without the encryption key. Additionally, E2E encryption can be used alongside digital platforms that support point-of-sale (POS) transactions and IVR phone payments.

HASH SIGNATURES

How It Works

A hash signature is an algorithm-generated, fixed-length combination of numbers and letters and is encrypted through a private key known as a digital signature.[10] At checkout, a hash signature is needed for authentication.

Why It's Important

Hash signatures play a crucial role in confirming that a key matches a specific individual or entity. This adds an additional level of security and can prevent instances of mistaken identity or fraud.

TOKENIZATION

How It Works

The tokenization process involves replacing data, such as bank account numbers or credit card information, with a randomly generated stand-in with no relationship to the original data. Critically, the token retains no value throughout the process. A payment gateway provider stores the actual sensitive data in a virtual vault and issues tokens in its place. Tokens can only be exchanged for payment data during the transaction authorization.

Why It's Important

With tokenization, there's no need for merchants or organizations to store sensitive data. This protects organizations in the event of a data breach, as any stolen materials are inherently valueless. Only the payment process can exchange tokens for actual data, ensuring external and internal protection.

TWO-FACTOR AUTHENTICATION (2FA)

How It Works

Two-factor authentication is quickly becoming a popular method to verify identities by requiring two different types of information from a user.[11] For example, a user might log into a site with their password, then receive a text with a PIN code to enter for additional verification.

Why It's Important

Using two forms of authentication can be useful when dealing with disputed transactions. Additionally, it adds another valuable layer of security. Microsoft believes that 99.9 percent of compromising attacks can be prevented through the use of multi-factor authentication.[12]

STEP 3: OFFER SECURE PAYMENT METHODS

Customers expect their data to remain secure through the transaction process. They also expect to be able to pay through their payment method of choice. As discussed, there has been a significant shift toward digital payments. Now, more than 75 percent of Americans use some form of digital payments, with 58 percent using two or more different methods.[13] To satisfy customer demands, it's valuable to offer a wide range of secure payment methods.

EMV CARDS

Many new credit and debit cards come embedded with EMV chips. As opposed to traditional swiping, EMV cards are inserted into a terminal. The chip creates a unique transaction code with each purchase, protecting against potential fraud.

By the end of 2020, there were over 10.8 billion EMV chip cards in circulation, a 10 percent increase over the previous year.[14] In the fourth quarter of 2020, 86 percent of all card-present transactions used EMV cards. As EMV cards are now the most common type of card, customers expect this method to be widely available.

CONTACTLESS CARDS

Contactless cards let consumers make payments without needing to enter a PIN, swipe a card or sign to approve a transaction. Often enabled by radio frequency identification (RFID) technology, contactless card payments can be used at point-of-sale terminals.

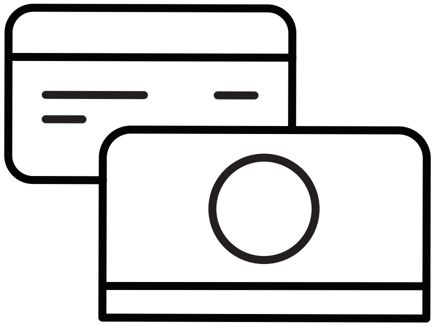
A recent survey found that contactless payments increased by 69 percent for retailers in 2020.[15] Today, more than half of Americans now use at least one form of contactless payments.[16]

In the past year, individuals have become increasingly aware of their personal hygiene in public areas to ensure their personal safety. This habit is likely to become ingrained, and avoidable hand-to-hand contact will become rare. Additionally, accepting contactless cards provides another simple way for customers to pay safely and quickly.

CARD ON FILE

Having a card on file allows customers to add and save a payment method at any time and without needing to manually enter payment details every time. Customers can securely save a variety of payment methods, including credit and debit cards and bank accounts, for either online or in-person transactions.

One industry survey found that 30 percent of consumers will abandon their purchase if they are asked to re-enter their payment information.[17] By having their information securely saved on file, customers are more likely to complete transactions and purchases. Additionally, having their card on file is ideal for recurring payments for monthly payments such as utilities, communications and subscription charges.



MOBILE PAYMENTS AND APPS

Mobile payments include any transactions made from a portable device, most commonly smartphones and tablets. These mobile apps store payment card information or allow consumers to transfer money to other users from their bank accounts. Popular mobile apps include Apple Pay, Google Pay and PayPal.

While mobile payments were initially more popular in Europe and Asia, they have experienced significant growth in North America. In 2019, the value of the U.S. mobile payment market increased by 41 percent to $98.8 billion.[18] The market is projected to grow to $220 billion by 2023. Mobile payments are not only easier for consumers, but they are also significantly safer. Individual security codes are created by the provider for each transaction, making them easier to track and verify.[19]

INTERACTIVE VOICE RESPONSE (IVR)

An IVR solution allows customers to make payments over the phone. The IVR walks customers through their options, providing an interactive option for customers to pay at their convenience. As an automated service, it adds an additional layer of security when processing payments over the phone, reducing the likelihood of agent error.

HOSTED PAYMENT PAGES

On a hosted payment page, a third-party vendor accepts digital payments and is responsible for the total payment process, including data protection and security. Having a hosted payment page provides a safe and compliant method to process online payments. Additionally, it ensures that customers enjoy a seamless payment experience.

A recent report from Paysafe showed that 76 percent of businesses have noticed that customers are opting for more secure payment methods online when possible.[20] To generate revenue, organizations need to be able to securely accept payments on a hosted web page. The economic incentive is clear: eCommerce sales are predicted to reach $4.2 trillion this year, with the United States accounting for nearly a quarter of the total.

[1] "Home Health Improper Payments Increased to $1.84 Billion in 2021," Home Healthcare News

[2] "COVID-19 Increases Urgency for Banks to Transform Payment Systems as Digital Payments Soar, Finds Research from Accenture," Accenture

[3] "It's Time to Go Digital With Your Payments: Here's Why," Health Leaders Media

[4] "New trends in US consumer digital payments," McKinsey

[5] "Fighting fraud: A never-ending battle," PwC

[6] "2020 Findings from the Diary of Consumer Payment Choice," Federal Reserve Bank of San Francisco

[7] "Maintaining Payment Security," PCI Security Standards Council

[8] "ISO/EIC 27001 Information Security Management," ISO

[9] "Strong Growth Continues for ACH Network as Volume Climbs Nearly 10% in Second Quarter of 2021," Nacha

[10] "Digital signatures," IBM

[11] "Two-factor Authentication," Investopedia

[12] "One simple action you can take to prevent 99.9 percent of attacks on your accounts," Microsoft

[13] "US digital payments: Achieving the next phase of consumer engagement," McKinsey

[14] "EMV chip credit card technology," Thales

[15] "Coronavirus leads to more use of contactless credit cards and mobile payments despite cost and security concerns," National Retail Federation

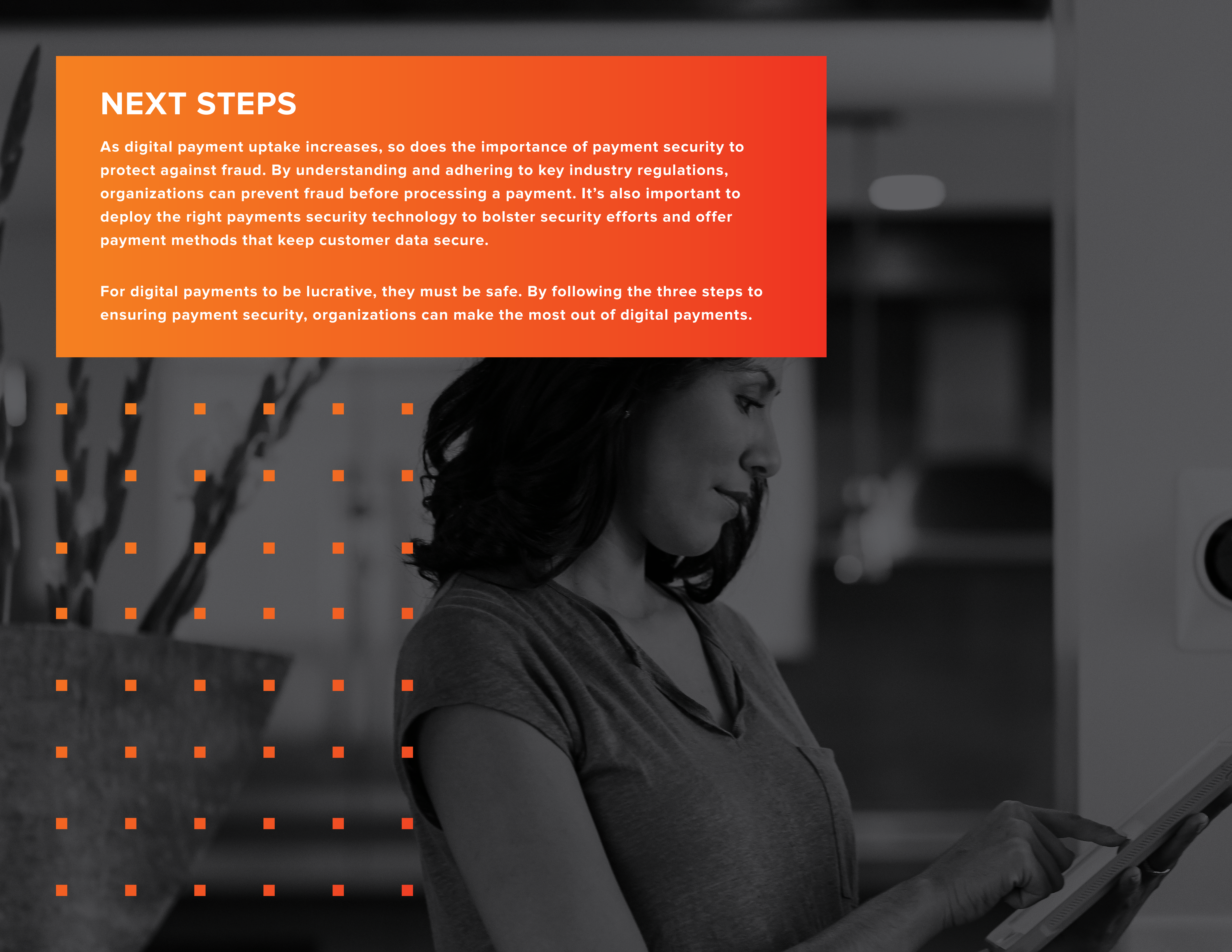
[16] "More than half of Americans now use contactless payments," CNBC

[17] "15 Cart Abandonment Statistics You Must Know in 2021," Sleeknote

[18] "Fueled By Increased Consumer Comfort, Mobile Payments In The US Will Exceed $130 Billion in 2020," Forbes

[19] "The Most Popular Mobile Payment Apps," Investopedia

[20] "Payment security issues remains a big worry for online retailers and consumers alike," TechRadar



NEXT STEPS

As digital payment uptake increases, so does the importance of payment security to protect against fraud. By understanding and adhering to key industry regulations, organizations can prevent fraud before processing a payment. It’s also important to deploy the right payments security technology to bolster security efforts and offer payment methods that keep customer data secure.

For digital payments to be lucrative, they must be safe. By following the three steps to ensuring payment security, organizations can make the most out of digital payments.

WANT TO LEARN MORE?

Visit our website or call us at 866-290-5400 for more information about payments integration and to learn how you can get started today.