csg Forte

3 Steps to Ensure Payments Security

How to securely accept digital payments

Introduction

If we were to make a list of everything that has changed in our lives since March 2020, we'd probably start with the social impact. We temporarily had fewer in-person interactions, bought more items online instead of in-person and subscribed to more streaming services than we probably ever imagined. Some of these changes subsisted.

But take a closer look at these social changes and you'll notice that payments are embedded in many of these changes. When we couldn't meet in person, we bought subscriptions to video conferencing platforms. When we couldn't or didn't want to go into stores, we used contactless or digital payment methods to limit contact. And when we had nothing else to do, we signed up to watch content from video streaming providers.

With this seismic change in payment preferences, the consumer shift to digital payments (encompassing online and mobile payments) is likely here to stay, if not increase at a steady pace.

The Global Digital Payment Market is expected to reach $ 12.55 trillion by 2027.[1] And there are multiple reasons why consumers have and will continue to embrace digital payments:

Ease of use—A key reason why U.S. consumers prefer to transact with merchants with digital payments capabilities is the ease of use and convenience. Over 28 percent of Generation Z prefers to use digital payments for this reason, and over 23 percent of Generation Y (millennials).

Security—Unlike cash, digital payment methods have built-in security features like tokenization and encryption to secure consumer payment information.

Consumers also have the choice to make digital payments on a variety of digital channels from their mobile devices and can choose what works best for them.

While digital payment channels have made it easier and safer to conduct transactions, information security is another story. As the rapid uptake of digital payments has increased, so has fraud. In fact, over 75 percent of companies have suffered some form of digital payment fraud.[3]

At a micro level, every dollar in fraud results in an average of $3.60 in losses for merchants.[4] At a macro level, 65 percent of organizations were victims of payments fraud attacks/attempts in 2022.[5]

Consumers are also losing money. In 2023, the average loss per consumer was $3,685.[6] Although consumers have quickly adopted online shopping and payment methods, over two-thirds of them believe that shopping online has "put them at a higher risk of fraud," and over 50 percent have reported being a victim of digital payment fraud.[7]

But customers aren't just losing money—they're losing trust in companies as well, especially when they try to pay on mobile channels. U.S. retailers have seen a threefold increase in mobile fraud, and U.S. e-commerce companies have seen a nearly eightfold increase in mobile fraud. For example, some users of peer-to-peer (P2P) apps like Venmo and Zelle have lost hundreds of dollars through online money transfers to unknown scammers.[8] When these consumers reached out to P2P payment processors to get their money back, they had trouble recouping their losses, since these payment transactions occur instantly.

With 25 percent of merchants having trouble implementing payment security solutions, and 31 percent of North American merchants struggling to offer emerging payment types, it's time to level up payments security.[9] Read on to find out the three steps merchants can take to maintain cash flow from digital payments while keeping consumer information and payments secure.

CUSTOMERS AREN'T JUST LOSING MONEY—THEY'RE LOSING TRUST IN COMPANIES AS WELL, ESPECIALLY WHEN THEY TRY TO PAY ON MOBILE CHANNELS.

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.[10] 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.[11]

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

- Protecting stored account data
- Encrypting transmission of cardholder data across open, public networks
- Developing and maintaining secure systems and software
- Restricting access to cardholder data
- Regularly testing security systems and networks[12]

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.

March 2024 marks the beginning of PCI DSS version 4.0 application, and you should make sure your compliance goals and processes are up to date with the latest standard.

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."[13]

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 2023 alone, more than $31 billion moved across the ACH network.[14]
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

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.[15] 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.

Multi-Factor Authentication (MFA)

How It Works

Multi-factor authentication is a popular method to verify identities by requiring two or more types of information from a user.[16] For example, a user might log into a site with their username and password, then receive a text with a PIN code to enter for additional verification.

Why It's Important

MFA makes it harder for hackers or fraudsters to access your customers' data, even if they have a username and password. It adds an extra layer of security that deters or delays attackers. Microsoft believes that 99.9 percent of compromising attacks can be prevented through the use of multi-factor authentication.[17]

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. Digital-payments penetration increased to 89 percent in 2022. Additionally, the share of respondents who report using two or more forms of digital payments has grown even more rapidly—from 51 percent in 2021 to 62 percent.[18] 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.

There are now 2.4 billion active EMV chip cards used for credit and debit payment at 37 million EMV acceptance terminals deployed around the world.[19] 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. The total value of contactless payments leapt 49.7 percent in 2022.[20] Today, more than half of Americans now use at least one form of contactless payments.[21]

Since the COVID-19 pandemic, individuals have become increasingly aware of their personal hygiene in public areas to ensure their personal safety. This habit is likely to become ingrained. 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.[22] 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. Forty-three percent of U.S. smartphone users use mobile payments, the most popular mobile payment app being Apple Pay.[23] 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.[24]

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.[25] To generate revenue, organizations need to be able to securely accept payments on a hosted web page. The economic incentive is clear: it's estimated that cross-border ecommerce sales will skyrocket to an impressive $3.3 trillion in 2028.[26]

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.

1 "Global Digital Payments Market Size and Forecasts 2022-2027: The Future of Digital Payment Is Frictionless" ResearchAndMarkets.com

2 "The Emerging Post-COVID-19 Consumer," PYMNTS

3 "2019 Digital Payments Survey," American Express

4 "True Cost of Fraud," LexisNexis

5 "65 percent of organizations were victims of payments fraud attacks/attempts in 2022," American Association of Financial Professionals

6 "Scams Cost Consumers $8.8 Billion in 2022 — The Top Five Frauds," Kiplinger

7 "Payment Fraud Fears Grow," Marqeta

8 "Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams," CBS News

9 "Merchants say they're losing revenue to online fraud, FIS report finds," Payments Dive

10 "Fighting fraud: A never-ending battle," PwC

11 "2020 Findings from the Diary of Consumer Payment Choice," Federal Reserve Bank of San Francisco

12 "Maintaining Payment Security," PCI Security Standards Council

13 "ISO/EIC 27001 Information Security Management," ISO

14 "Overall ACH Network Volume," Nacha

15 "Digital signatures," IBM

16 "Two-factor Authentication," Investopedia

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

18 "Consumer Trends in Digital Payments," McKinsey

19 "EMV Chip," Visa

20 "Value of contactless payments up nearly 50 per cent in 2022," Barclays

21 "More than half of Americans now use contactless payments," CNBC

22 "15 Cart Abandonment Statistics You Must Know in 2021," Sleeknote

23 "Mobile Payment Statistics Detailing the Industry's Growth" Money Transfers

24 "The Most Popular Mobile Payment Apps," Investopedia

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

26 "Cross-border eCommerce Market Statistics" Juniper Research