



versapay®

Payment Fraud Explained

How B2B Merchants Can Fight Fraud
and Maximize Customer Experience

Contents

- 3** The shifting landscape of payment fraud
- 6** The many faces of payment fraud
- 11** The most (and least) secure payment methods
- 15** The tradeoff between customer experience and security
- 17** How to detect payment fraud
- 19** How to prevent payment fraud
- 22** Process payments with peace of mind

01

The shifting landscape of payment fraud


87% of finance leaders believe their buyers are ready to transition to making payments digitally. With more B2B customers embracing online payment channels, it's important that finance leaders be aware of the risks of digital payment fraud and well-equipped to combat them.

Payment fraud is ever evolving. The threats that businesses and consumers now face are much different from the threats that prevailed at the turn of the 21st century—when check usage dominated and “online fraud” was to many a foreign concept.

Payment fraud—whether carried out online or through other means—is the act of completing counterfeit or illegal transactions, usually by stealing an unsuspecting victim's information. While fraud itself is nothing new, the tactics fraudsters and online criminals use are always evolving.

The United States—the most credit card fraud-prone country in the world—is most heavily impacted by payment fraud and is responsible for over one-third of card fraud losses the world-over.

Source: <https://www.cnn.com/2021/01/27/credit-card-fraud-is-on-the-rise-due-to-covid-pandemic.html>



Card fraud losses amounted to

\$28.58 billion

at the end of 2021.

This figure is expected to scale to **\$38.50 billion by 2027**, according to Nilson.

Source: https://nilsonreport.com/upload/content_promo/NilsonReport_Issue1209.pdf

Payment fraud can take the form of:

- Fraudulent or unauthorized transactions
- Merchandise stolen or criminally removed, or
- False requests for refunds and returns (also known as chargebacks).

There are countless methods of committing payment fraud, including physical, in-person attacks and digital fraud attacks. But how did we get here? Why is online fraud so pervasive? What digital fraud tactics do fraudsters use and why is payment fraud risk higher than it's ever been?

The primary culprits for the rise of payment fraud are the ecommerce boom and the COVID-19 pandemic. Already steadily growing year over year, ecommerce—for both business-to-consumer (B2C) and business-to-business (B2B) companies—surged during the pandemic as businesses pivoted to account for customers staying home. More businesses are transitioning from brick-and-mortar to online stores or are electing to start new with an online presence.

As 2021 began, it was estimated that roughly 27% of the world's population¹ would be shopping online by the end of the year. While ecommerce offers merchants unbridled growth potential, having the need for an online presence thrust onto them meant many businesses dove in with very little knowledge of online payments and fraud.

*“There are all these different, wonderful **avenues for fraudsters to get into a business’ ecosystem**. It only takes one organization with that supply chain to not update their security—for their devices or network—and that grants fraudsters access,”*

Chris Wassenaar, Chief Risk Officer, Versapay

**The percentage of finance leaders
who believe their buyers are ready
to transition to making payments
digitally**

In your opinion, are your buyers ready to
move away from making payments by check,
to making payments digitally?

87%	13%
Yes	No

Source: <https://www.versapay.com/resources/digital-payments-are-ready-for-the-spotlight>

02

The many faces of payment fraud

Payment fraud is multi-faceted. New breeds of fraudsters are continually emerging, with new types of attacks surfacing whenever one is stamped out. The challenge for businesses is being aware of these emerging forms of fraud and how to spot them. With the right technology, businesses can more readily detect and prevent fraud, lessen its impact on revenue and operations, and simultaneously enhance the customer experience.

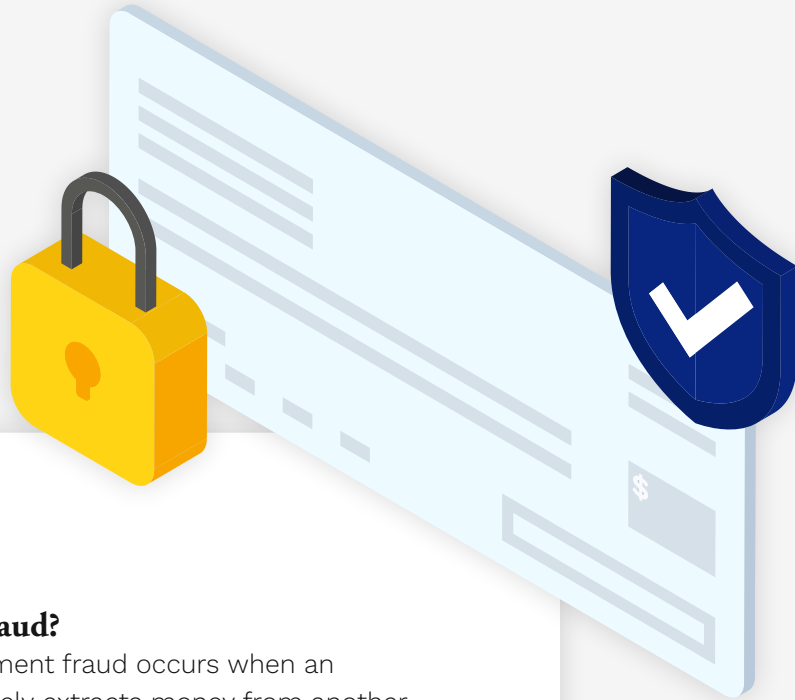
We've elected to break down payment fraud into two groups: check fraud and digital payment fraud.

Digital payments have long been ready for the spotlight, but 91% of finance tech leaders say their organizations are still receiving check payments from their customers². Digital payments are the future of B2B commerce—there's no denying it—but for now, checks are still prevalent. Although, if the customer experience and back-office accounting benefits of accepting digital payments weren't enough to turn you away from checks, maybe the fraud risks will.

*“There are all these different, wonderful **avenues for fraudsters to get into a business’ ecosystem**. It only takes one organization with that supply chain to not update their security—for their devices or network—and that grants fraudsters access,”*

Chris Wassenaar, Chief Risk Officer, Versapay

²<https://www.versapay.com/resources/digital-payments-are-ready-for-the-spotlight>



Check fraud

What is check fraud?

We know that payment fraud occurs when an individual deliberately extracts money from another individual or business entity through deceptive and criminal means. Check fraud is simply the process of using checks to commit payment fraud.

What are the different types of check fraud?

Check fraud comes in many different shapes and sizes. What's important to note, however, is that when dealing with physical checks, there are two critical vulnerabilities that aren't present for their digital payment method counterparts.

The first vulnerability is checks' actual physical, paper-based nature. Because checks have to be physically transported from one party to another, there's a higher likelihood that a fraudster can obtain checks while in transit or elsewhere.

The second vulnerability is the confidential information contained within checks. In having information like your name, address, account number, and routing number directly on a check, you're providing fraudsters upfront with all the information they need to commit check fraud.

The primary types of check fraud include:

Check forgery

This method is typically used when defrauding banks. The fraudster will intentionally sign a check without authorization or will endorse a check that's not payable to the endorser. In very rare cases, a fraudster will try to pass a check that's manufactured by themselves that represents an account that is not real.

Paper hanging

Paper hanging occurs when a fraudster knowingly writes a bad check. In this case the fraudster might purposely write a check that exceeds their balance to overdraw their account and take advantage of the float time. This is sometimes called check abandonment.

Check theft

This is the physical theft of checks with the intent to cash them fraudulently. The fraudster then typically forges a signature.

Check washing

This method often follows closely on the heels of check theft. Fraudsters will use highly volatile solvents to erase the ink off checks and then rewrite the checks as payable to themselves. They will likely increase the payable amount by hundreds or thousands of dollars.

Counterfeiting

A counterfeit check is printed on non-bank administered paper and made to look genuine. The information the fraudster includes on the check, however, will be tied to a real victim's account.

Check kiting

Similar to paper hanging, check kiting is reliant on check float, whereby fraudsters aim to delay the notice of non-existent funds. In essence, fraudsters will gain access to funds deposited in one account prior to the bank collecting them from another.

Check conversion

In the context of check fraud, check conversion takes place when a non-payee endorses a check and then deposits it fraudulently. That same non-payee will take possession of cash that does not belong to them, and the true recipient will be unaware until much later.



Digital payment fraud

What is digital payment fraud?

With the payment landscape evolving quickly, more digital payment channels are becoming available. Even payment methods traditionally popular within the B2C realm are becoming increasingly prevalent in B2B circles.

With this comes increased vulnerability to payment fraud, as each new payment method creates a new opportunity for fraudsters. According to the CEO of fraud detection company DataVisor, the advent of card-not-present (CNP) transactions replacing checks has seen fraudulent activity across digital channels ramp up significantly.³

Compounding matters further is the fact that many businesses are unable to keep up with the rate of change or lack the in-house expertise to confidently fight fraud.

At its core, digital payment fraud is no different than check fraud—fraud is fraud, after all. The difference lies in the tactics used by fraudsters and the need for businesses to remain highly vigilant as digital payment trends evolve.

³<https://www.forbes.com/sites/forbestechcouncil/2021/02/08/take-a-proactive-approach-to-fighting-digital-payment-fraud-in-2021/?sh=5b72f7dc3d13>

What are the different types of digital payment fraud?

There are many more types of internet frauds—which are often intertwined with payment fraud—than these, but here are some of the most common types that merchants should be on the lookout for:

Identity theft

The scheme is as old as commerce itself, but, like commerce, has evolved over time to remain a threat. In this modern, digital age, fraudsters might impersonate ecommerce websites and attempt to obtain personal data via corrupted shopping carts.

Card theft

This method makes use of fraudsters' theft of credit—or other card—details to then make purchases online. Businesses will often assume the purchase was legitimate and successfully process the transaction. The cardholder will likely dispute the transaction once they're made aware, however, the business will be unable to recoup their losses (the cost of goods and services provided and the dispute fees).

Chargebacks

This process—whereby a cardholder disputes a charge with their bank—is an important consumer protection mechanism. It's also a process that's often abused by fraudsters in B2B commerce. Fraudsters deploy tactics such as account takeovers, phishing and smishing, domain squatting, and identity theft to make fraudulent purchases resulting in chargebacks.

Overpayments

In this case, a fraudster will make a purchase using illegally obtained credit card credentials and then approach the supplier for a full or partial refund. The fraudster, however, will request that the refund be granted to a different credit card than the one initially used or request payment through other means. If a chargeback is filed, the supplier will be left hanging for the chargeback amount and the amount sent to the fraudster.

Credit card testing

This is a malicious attack—facilitated by a fraudster—on a merchant's website or shopping cart. It's usually triggered by a bot or automated script that tests lists of illegally obtained credit card information to identify valid cards. The merchant may incur significant fees from credit card testing, whether the transactions are successful or not.

Account fraud

This kind of fraud occurs when fraudsters create customer accounts using falsified or stolen identities, or gain access to existing, legitimate accounts by masquerading as a colleague and subsequently changing email and mailing addresses. After acquiring access, fraudsters can steal funds directly using fraudulent wire transfers and purchases. Funds deposited in one account prior to the bank collecting them from another.

03

The most (and least) secure payment methods

While the potential for fraud might dissuade some businesses from making the jump to online payments, there are plenty of reasons not to let payment fraud be a deterrent. We'd argue that now, more so than ever, is the best time to embrace digital payments.

Here is a list of the most—and the least—secure payment methods. Notice anything? (Hint, hint. The most secure are all digital payment methods).

“A fraud prevention and detection strategy is important for all businesses because fraudsters will always focus on the weakest link or most vulnerable target to attack. As more businesses adopt digital payments, the incentive for fraudsters to exploit vulnerable systems also increases. *It's important that all businesses accepting digital payments deploy a fraud mitigation strategy* that includes automated tools to verify the identity of a customer and provide real-time fraud scoring to properly evaluate the risk of a transaction,”

Chris Adams, VP of Product, Payments, Versapay



The **most secure** payment methods

1**ACH**

An ACH is an electronic transfer of funds system run by the National Automated Clearing House Association (NACHA) in the United States. With an ACH payment, funds are moved electronically from one bank to another through the ACH network. This network connects every single US financial institution, which gives them the ability to transfer money from one bank to another safely, quickly, and securely.

2**Virtual cards**

Virtual cards are single-use credit card numbers that are generated for each payment. As the name suggests, they are entirely virtual—no plastic, no chips, no PINs. Buyers typically enjoy using virtual cards as they offer improved security, better control, and complete transaction details. Sellers are increasingly embracing this payment method, with help from solutions that allow for straight-through-processing of virtual cards, integrated with their enterprise resource planning systems (ERPs).

3**Credit cards**

Despite how rampant payment fraud has become—and despite credit cards seemingly being the crux of all fraudulent attacks—credit cards are still one of the three most secure payment methods, especially for B2B buyers. Credit cards offer the benefit of not being linked to the buyer's actual bank account and the ability to lock the card at the sign of fraudulent activity.



The **least secure** payment methods

1**Paper check**

Familiarity and a false sense of security are driving check fraud. It's time to put those falsehoods to rest. Paper checks contain a wealth of sensitive information that can lead to severe consequences when in fraudsters' hands.

2**Wire transfers**








The term wire transfer is often used interchangeably with ACH. But while the two work very similarly, there are some notable differences that make wire transfers less secure. Wire transfers can be used to send several million dollars whereas ACH (Same Day) caps at \$100,000 per payment.⁴ Once settled, wire transfers are also very difficult to reverse.

3**Phone-initiated payments (card-not-present)**

Phone-initiated payments put B2B sellers firmly in PCI DSS scope and the actual effort of processing payments over the phone is sluggish, inefficient, and error-prone. Credit card information relayed over the phone must be handled by someone to process it, which opens your business up to risk. You'll also need to ensure that information is destroyed—if it was recorded on a piece of paper for instance—after it's been appropriately inputted into your accounting systems.

⁴<https://www.nacha.org/rules/increasing-same-day-ach-dollar-limit>

What are the differences between **ACH transfers and wire transfers?**

	Wire transfer	ACH
 Transfer speed	Minutes to one business day	Hours to several business days
 Settlement	Largely irrevocable	Several reversal rules
 Cost	Tens of dollars	Tenths of pennies to 1.5%
 Direction	Only sender can initiate	Sender or receiver can initiate
 Frequency	Largely one-off	One-off and recurring
 Size	Up to many, many \$ millions	98% of the time <\$25K
 International Reach	Wide support	Limited support

Source: <https://plaid.com/resources/ach/ach-vs-wire-transfers>

04

The tradeoff between customer experience and security

Beyond the extreme financial implications and the potential reputational damage, payment fraud threatens to destroy the trust you've worked so long to build with your customers.

But for businesses to offer assurances to their customers that the buying experience is secure, they must often implement a variety of security measures that can potentially disrupt the customer experience.

Business buyers are adopting many of the purchasing habits they have as consumers and increasingly expect the B2B buying experience to mirror the simplicity and convenience of B2C. The result is businesses undergoing rapid digital transformation and more B2B transactions taking place online. What many sellers are now struggling with, however, is the delicate balancing act between customer experience and heightened digital payment security.

“Fraudsters are increasingly aggressive and successful in their attempts to obtain accurate card information for fraudulent activity. So, ***businesses must do their due diligence and consider additional measures of protection*** outside of standard card industry practices,”

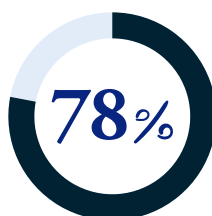
Brandy Luczywo, Interchange Analyst, Versapay

Sellers are generally hesitant to introduce additional security measures for fear it might negatively impact the buyer's experience. And they're not alone in their thinking. Too many choices often lead to indecision. And indecision often leads to fewer conversions. The same could be said about having to jump through multiple hoops during the transaction process.

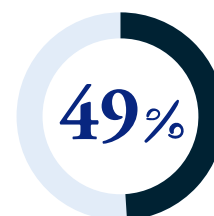
The difference is that buyers expect merchants to keep their data secure. Recent survey data shows that 78% of consumers would stop engaging with a brand online following a breach, and 49% would not sign up for an online service that had recently been breached.⁵ Another 47% of respondents have changed how they secure their personal data and 54% are more concerned with protecting their personal information than they were a year prior to the survey.

The takeaway here is that buyers take security seriously, and sellers mustn't sacrifice digital payment security at the cost of a few extra transactions—which might not even come. Instead, sellers should strike an optimal balance between digital payment security and customer experience.

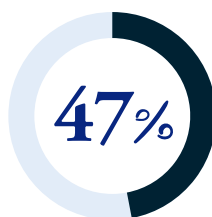
The percentage of buyers that expect merchants to keep their data secure



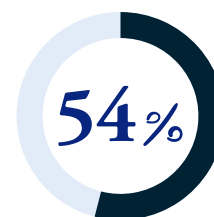
of consumers would stop engaging with a brand online following a breach



of consumers would not sign up for an online service that had recently been breached



of respondents have changed how they secure their personal data



of respondents are more concerned with protecting their personal information than they were a year prior

⁵<https://www.securitymagazine.com/articles/89777-shows-consumers-are-abandoning-brands-after-data-breaches>

05

How to detect payment fraud

With how fast payment fraud evolves, it can be difficult for businesses to be as educated—and prepared—as possible to fight it.

That's why having a fraud prevention and detection strategy in place is so vital for businesses. Rather than be reactive, it's important businesses take a proactive stance and identify suspicious behavior and patterns, as close to real-time as possible.

“Awareness of customer payment frequencies and behavioral patterns is imperative at detecting where vulnerabilities exist,”

Brandy Luczywo, Interchange Analyst, Versapay

Learn to spot what payment fraud looks like

1. Falsified or inconsistent information

Be on the lookout for buyers transacting using false information—such as phone numbers and email addresses. In many cases the information might appear to be accurate, but if there are inconsistencies—such as the same email address but different names used across multiple purchases—that's a red flag.

2. Abnormal or canned communications

Fraudsters look to target as many businesses as they can in as little time as possible. To expedite the process, they often use canned or scripted responses. If communication with a prospective customer seems stiff or off or abnormal in any way, it might signal the start of a fraudulent attack.

3. Unusually large orders

You likely have a general sense of what products sell when, and in what quantities. Be aware if you suddenly begin receiving unusually large orders (comprised of multiple high-value goods) and are unable to pinpoint to a reasonable cause.

4. Atypical requests

Identifying fraud unfortunately requires a fair amount of qualitative analysis. Listening to your gut feeling is important. If you notice some unusual requests are being made, this could be a sign of fraudulent activity. For example, you might receive requests to:

- Split a large order into multiple payments across different cards with different billing addresses
- Process a payment manually to overcharge a card and pay the difference to a third-party, or
- Provide a refund outside the card network from which the charge originated—such as via check or ACH

These might all be indicators of fraudulent behavior.

Recognize illegitimate traffic and behavioral changes easily

Once you know what you're looking for, you can create velocity logic rulesets—if you have an ecommerce or online shopping portal—to monitor data elements that occur within specific intervals. This means setting parameters that look for the aforementioned indicators to help reduce incoming fraudulent activity.

It's important you appoint a specific contact or team within your organization to receive notifications for these parameters. They should be someone who can be counted on to move into action when any of your controls are exceeded or triggered. This will allow you to quickly act and stop any incoming fraudulent activity as soon as it's identified.



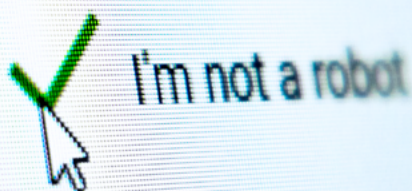
06

How to prevent payment fraud

A key realization for all B2B focused businesses is that it's impossible to eliminate all fraud. But, that doesn't mean it's impossible to mitigate and prevent it from severely damaging your business' financials and reputation. It just means you need to be highly vigilant and understand the inherent risks of accepting payment.

“Fraudsters are creatively identifying and capitalizing on vulnerabilities within shopping carts and API-related connections so having CAPTCHA-related functionality as well as *monitoring and ensuring appropriate PCI compliance with all forms of payment-related processing* connectors is strongly encouraged,”

Brandy Luczywo, Interchange Analyst, Versapay



“A little bit of friction—like having to engage a CAPTCHA—tells buyers that *merchants actually care about the security of their credit card data,*”

Chris Wassenaar, Chief Risk Officer,
Versapay

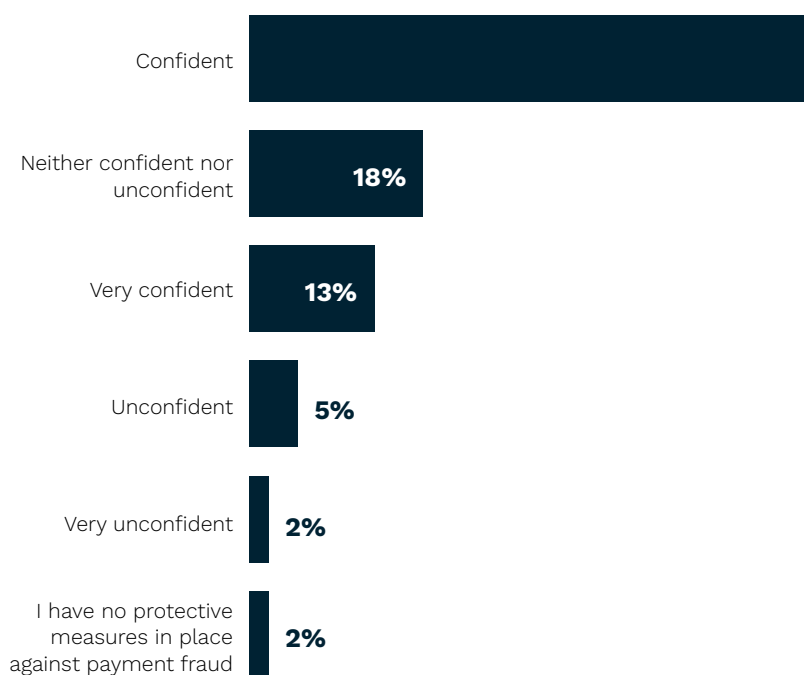
“The digital payment ecosystem is fragmented. Whether it’s B2C or B2B, businesses are engaging with multiple third-party service providers and weaving their solutions into their own internal information technology infrastructure. *Understanding the full landscape of that ecosystem is critical for businesses looking to prevent payment fraud,*”

Chris Wassenaar, Chief Risk Officer,
Versapay

A 2021 survey by Versapay and Pulse revealed that 27% of technology leaders lack confidence in the protective measures they currently have in place for preventing payment fraud. Nearly three quarters of respondents, however, are confident or very confident in the measures they’ve implemented.

While these are promising surface-level findings, confidence does not equal security. Businesses are being impacted by payment fraud to the tune of nearly \$30 billion a year.⁶ The most important thing you can do to maintain vigilance in the fight against fraud is to continually evaluate your position.

How confident or not confident are you in the protective measures you currently have in place for preventing payment fraud?



⁶https://nilsonreport.com/upload/content_promo/NilsonReport_Issue1209.pdf

There are further payment fraud prevention measures and anti-fraud controls businesses can action, including:

1. Monitoring, preventing, and blocking incoming fraudulent activity

One of the most important things you can do to prevent payment fraud is establish processes and tools that enable you to stop fraudulent activity early—not just merely detect it. With digital payments—specifically credit cards—the critical window to mitigate fraudulent activity is before authorization occurs—here, fees are still incurred even if a transaction is not approved.

One such tool that can help mitigate fraud is the use of CAPTCHAs. These are systems that help web hosts understand if humans or robots are accessing a website. They are unobtrusive safeguards that protect websites from spam and abuse. A common practice among fraudsters is card testing, which involves using automated scripts to run high volumes of authorization tests on illegally obtained credit cards. CAPTCHAs can block these mass tests.

2. Making compliance a year-round priority

While adhering to PCI compliance guidelines is necessary for businesses that handle credit card information, being PCI-compliant does not guarantee your business will not fall victim to a data breach or payment fraud.

There is, however, a noticeable trend of businesses being non-compliant at the time of experiencing a

data breach. According to Verizon's 2020 Payment Security Report, of the companies that experienced a breach between 2014 and 2019, 53% were confirmed to be non-compliant. A remarkable 0% of PCI compliant companies surveyed experienced a breach.⁷ It's important to view PCI compliance as a continuous effort that goes beyond the time of your annual certification.

3. Partnering with a secure, integrated payments provider

Many third-party providers—payment processors, payment gateways, merchant acquirers, issuing banks, and ERPs—are involved in processing digital payments. The more hands a payment passes through, the more vulnerabilities exist. And any vulnerability is an access point that fraudsters can exploit.

One of the best ways to increase the security of your digital payment acceptance is by using an integrated payments solution embedded seamlessly with your ERP. This eliminates many of the vulnerabilities arising from having multiple handoffs between third-party providers. These integrated payments solutions also allow buyers to securely store their payment information, simplifying repeat purchases.

Fraudsters will use what's publicly accessible, such as an ecommerce site or a non-gated web-based payment page, to carry out their schemes. Instances of fraud on integrated payments solutions are exceptionally low as buyers typically pay through secure portals that require logins.

⁷<https://www.verizon.com/business/resources/reports/2020-payment-security-report.pdf>

07

Process payments with peace of mind

With Versapay, you can process payments directly in your ERP. Accepting and processing digital payments within a unified ecosystem that you control will significantly reduce the need to handoff data to additional parties, helping you minimize risk.

Versapay does more than help merchants process payments within a secure environment:

- We remove you from PCI DSS scope by tokenizing and ensuring sensitive card information totally bypasses your ecommerce site. You can operate your ecommerce site with peace of mind, knowing sensitive data will never touch your servers.
- We enable you to accept the most secure digital payment methods
- We provide you with greater visibility into your payments data, helping you learn expected payment behavior and understand when anomalies occur.

Visit versapay.com/payment-services to learn more.