

Securing modern commerce: How omnichannel payment security protects every interaction

White paper

Table of contents

01	Overview	p.03
02	Safeguarding every payment method and every channel: Verifone's multidimensional security approach	p.04
03	Future-ready payment security	p.10
04	Protecting payments across in-store, online, and omnichannel	p.11
05	Accelerating boundless security for a boundless payments ecosystem	p.17



Overview

Nearly **80% of organizations** experienced payment fraud attacks or attempts in 2024. The global cost of digital payment fraud alone is projected to **surpass \$100 billion by 2029**.

For merchants, the cost isn't just financial. It's lost trust, disrupted operations, and compromised brand loyalty at the moment of checkout.

Fueled by AI, criminals now can easily launch massive email phishing, voice phishing (vishing), and social engineering campaigns in a fraction of the time. These attacks are also more personalized and convincing, which increases their success rate.

"AI has created a smarter bad actor," says Ron Fridman, Vice President of EMV and Security at Verifone.

New payment technologies that enable faster real-time transactions make these attacks more challenging to detect and reverse. With a growing number of payment channels and methods, merchants now have more vulnerabilities and access points they need to protect. Quantum computing, another future threat, also could make encryption and authentication technologies less effective.

To combat these growing risks, securing the omnichannel ecosystem now means protecting payment data from the moment it's captured. Recognizing the point where the card or credentials interact with the device is foundational to securing the entire data journey and preventing digital compromise.

Basic, point-in-time compliance is no longer enough. Payment security must be continuous, omnichannel, and multifaceted.

With a three-dimensional security approach across hardware, software, and deployment, and future innovations in post-quantum cryptography, Verifone protects merchants from current and future security threats.

Payment fraud schemes
have become increasingly
sophisticated and more
difficult to stop.



80%

of organizations experienced payment
fraud attacks or attempts in 2024

\$100B+

global cost of digital payment
fraud projected by 2029



Safeguarding every payment method and every channel: Verifone's multidimensional security approach

Verifone offers a robust, omnichannel payment security stack that combats today's most critical security risks in a [bound-less payments ecosystem](#). Fridman says a “three-legged stool approach” encompassing hardware, software, and deployment anchors Verifone's secure design language.

Hardware, software, and deployment security are designed to work in tandem. Retailers often struggle with multiple vendors and siloed technologies, which increases complexity and risk. Verifone simplifies security by delivering a unified, multi-layered solution that reduces complexity, lowers operational burden, and strengthens protection across all payment touchpoints.





First leg of the stool

Hardware

“We first focus on the hardware. It’s a top-down design approach, ensuring the device is inherently secure,”

—
Ron Fridman, Vice President of EMV and Security, Verifone



Verifone's payment hardware solutions are “designed like vaults,” Fridman adds.

This includes anti-skimming devices, tamper-evident payment terminals that shut down when an unauthorized user tries to corrupt the device, and case open switches that remove key information from a payment device once they sense a breach.

“We also embed security meshes into our devices and secure bunkers that protect secure processors and other sensitive components, so it makes it extremely difficult for bad actors to penetrate the device and implement bugs that capture card-holder data,” Fridman says.

Additionally, Verifone focuses on certification, including EMV certification and certification with local security standards. EMV certification certifies the hardware itself and chipset, the payment application, and the entire end-to-end transaction processing flow with the acquirer to ensure secure payment processing. This approach validates the physical card against counterfeit cards and provides protection for lost or stolen cards.





Second leg of the stool

Software

Verifone leverages proven engineering practices developed over decades serving merchants in more than 165 countries and handling \$8 trillion in transaction volume annually. This approach also includes a trusted, secure architecture and firmware.

Its software and application-based security tools range from encryption and cryptography solutions to remote skimming detection technology (RSD):

Cryptography

Verifone relies on public key infrastructure that encompasses loaded verified keys (or digital certificates) on each payment device to establish what is trusted and what's not trusted. Through its signing portal, each device receives a cryptographic signature, which ensures only authorized software runs on them. These capabilities reduce the risk of tampering and malware attacks, and the possibility of fraudsters using customer card data across different devices.

Encryption

End-to-end encryption (E2E), along with PCI-validated point-to-point encryption (P2PE), safeguards cardholder data from point of entry to processing. These capabilities encrypt payment data at rest and in transit, securing transactions across multiple integration points and network processors.

"When we receive the data right in an encrypted tunnel, wherever we need to keep that data at rest, we encrypt it. When we pass that on to the acquirer, the bank, we use secure channels during transmission to ensure the security and integrity of that transaction to the acquirer and back to us," says Bill Wade, Verifone's Global Head of Cybersecurity.

Verifone also has adopted the Advanced Encryption Standard Derived Unique Key Per Transaction (AES DUKPT) software protocol, which changes encryption keys with every transaction. These sophisticated capabilities can help thwart bad actors' fast-moving, AI-driven fraud attacks.

Joachim Vance, Verifone's Chief Security Architect, says Verifone's approach exceeds the industry's current encryption standard, which often leaves merchants more exposed. "Most of the world uses the Advanced Encryption Standard or AES, but the payment industry does not," Vance says. "We do have a lot of deployments with customers that have really found it valuable that we've been a leader in that space."

165

countries where Verifone
merchants are located

\$8T

annual transaction volume
handled by Verifone



3D Secure

Verifone's [3D Secure authentication protocol](#) adds an additional authentication layer, introducing a cardholder identification loop to ensure the cardholder actually has ownership of the physical card.

Verifone offers basic blocking rules (related to the payment amount, IP address, and issuer risk profile) and address verification against billing information. These capabilities reduce the risks of counterfeit, lost or stolen cards, and re-use of card data if there's a breach.

Tokenization

Tokens serve as a proxy for customers' primary account number (PAN). Each token is meaningless if a fraudster intercepts it during the payment process, which protects the customer's real card information.



“Features like tokenization and point-to-point encryption... are really just fundamental validations and protections of that [payment] data. Sometimes in cybersecurity, everybody loves the new cool thing, but 95% of it is just doing the fundamentals,”

Will Morgan, Chief Information Security Officer, Verifone



How omnichannel payment security
protects every interaction

Biometrics

As consumers have grown more comfortable with providing biometric information like a fingerprint, palm, or face scan, more payments technologies are leveraging this trust to establish powerful, new authentication standards for transactions.

Verifone has [incorporated biometric technology](#) into its payment devices to drive secure, frictionless authentication and checkout experiences.

“It’s hard to steal someone’s palm, fingerprint, or face. It only works for one person. It reduces the amount of chargebacks and card replacement,” Fridman says about the benefits of biometrics.

Remote skimming detection (RSD)

Verifone’s overlay detection technology uses hardware and software security to protect against card skimming attacks. It detects unauthorized skimming devices on payment terminals and sends covert, real-time alerts to merchants without alerting fraudsters.

This technology safeguards the magnetic stripe data on Verifone’s multilane POS devices, enabling retailers to securely accept payments and activate rewards, loyalty programs, and digital coupons at the point of sale — without increasing exposure to malware or cyberattacks.



Third leg of the stool

Deployment

Verifone works closely with merchants to help them implement these solutions securely and compliantly. All of its solutions are PCI-compliant (Payment Card Industry), with a strong focus on PIN transaction security.

Verifone also helps merchants meet new PCI DSS compliance rules (PCI Data Security Standard) and implement DSS-compliant solutions, which secures cardholder data if a merchant stores this information.

“We’re PCI-compliant from a PCI PIN in a terminal perspective, and on all three fronts from a PCI perspective,” Wade says. “We provide good uptime and resiliency — 99.5% or higher — and we have 24/7 support and incident response capabilities.”

Though Verifone offers strong, multilayered payment security, it isn’t solely focused on its customers’ current security needs. It is already taking steps to prepare for tomorrow’s emerging threats.

99.5%

uptime and resiliency
provided by Verifone

24/7

support and incident response
capabilities provided by Verifone

“We’re PCI-compliant from a PCI PIN in a terminal perspective, and on all three fronts from a PCI perspective,”

Bill Wade, Global Head of Cybersecurity, Verifone





Future-ready payment security

Proactive security testing is critical when threats are constantly changing. To fortify its payment solutions against new attack vectors, Verifone has created a patented security testing tool to simulate potential threats.

“By simulating their attacks, we can plug up any holes well in advance of them ever happening,” Fridman says.

Vance explains Verifone is thinking and planning ahead on the security front.

Quantum computing could have a significant impact on payment security, undermining and weakening current cryptography methods because these computers will be able to process data much faster than even supercomputers. Quantum computers could break current cryptography tools for asymmetric encryption, which is currently used for software signing and website authentication, “in minutes or seconds,” Vance says.

These computers could power “harvest now, decrypt later” threats, where attackers hold on to unauthorized data they’ve accessed until more sophisticated tools emerge for them to

use this data for greater financial gain.

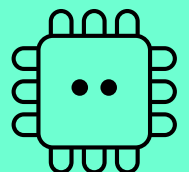
“The question is ‘how much time do we have and what do we do about it?’” Vance says about the potential threat of quantum computing. “Do we have anything to replace cryptography that is subject to the risks of a quantum computer?”

Verifone is proactively trying to answer that question by exploring post-quantum cryptography innovations. In 2024, the National Institute of Standards and Technology (NIST) unveiled quantum-safe algorithms. Vance is involved in writing new standards for how to use these algorithms.

“Verifone is at the forefront of this. We’re helping lead the technologies that will get us and the rest of the industry there,” he says. “You can be assured that we’ll also be deploying it as one of the first players [in the market].”

Quantum computing could have a significant impact on payment security, undermining and weakening current cryptography methods because these computers will be able to process data much faster than even supercomputers.

Joachim Vance, Chief Security Architect, Verifone





Protecting payments across in-store, online, and omnichannel



Verifone's proactive approach to payment security is already benefiting customers today across in-store, online, and omnichannel. Here's how advanced hardware and software tools modernize payment security in each of these environments.



In-store security: Quick Service Restaurants (QSRs)

Biometric security provides frictionless authentication that improves security and the customer checkout in fast-paced, high-volume processing environments. It adds an extra layer of protection for mobile wallet payments and enables QSRs to confidently offer personalized, loyalty-driven experiences without compromising speed or security.



Challenge:

QSRs have fast-paced operations, where they must quickly process a high volume of transactions across multiple payment methods and channels, including cash, card, and contactless payments for in-person and mobile ordering.

Along with trying to protect digital payment transactions, they also have to worry about fraudsters compromising physical payment devices, such as kiosks and self-checkout terminals, with skimming tools and spyware.

Solutions:

QSRs need multilane security solutions that balance speed and security.

“The consumer expectation is that the transaction is going to be as fast inserting it as it is swiping it,” Fridman says.

This is where end-to-end encryption and biometric security are invaluable. E2E encryption protects card data by encrypting it as soon as a customer enters it into a payment device or channel, securing it all the way through to the payment processor. This capability also helps prevent malware attacks that can occur while data is in transit.

Biometric verification technologies that provide more protection for mobile wallet payments



Facial
recognition



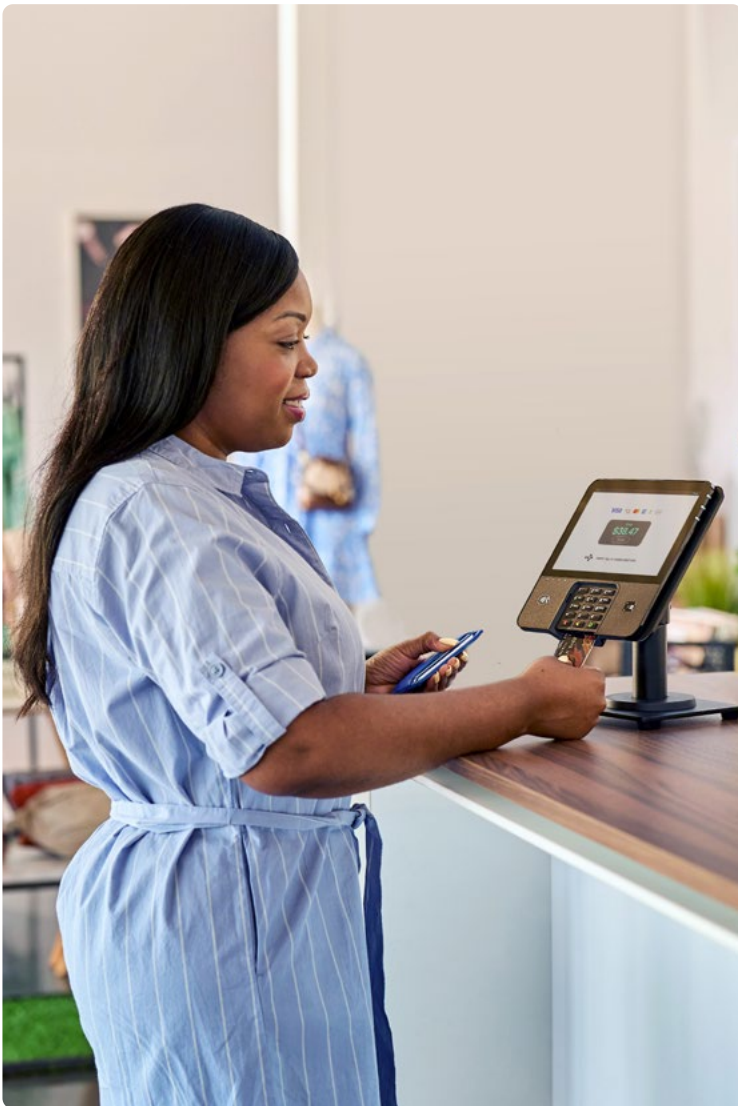
Fingerprints
ID



Palm vein
scanning



In-store security: Retailers



Challenge:

Retailers face many of the same challenges as QSRs — large transaction volumes, diverse payment options, and omnichannel payment complexity.

However, the majority of commerce [still happens in-store](#), so securing physical commerce is also vital for retailers.

Solutions:

Remote skimming detection (RSD) technology provides stronger protection in retail environments. It not only protects payment terminals from physical intrusion, but it also secretly alerts merchants in real time when bad actors make these attempts.

Tamper-evident payment devices and case-open switches provide the built-in, hardware-based security retailers need in-store, especially as payment terminals become increasingly unattended or exposed to support self-service convenience for consumers.

These solutions also help retailers meet PCI PIN Transaction Security (PTS) and PCI DSS requirements, serving as a frontline defense against in-store security threats.





Online payment security: Retailers

Challenge:

Retailers often process a high volume of card-not-present transactions through their online direct-to-consumer (D2C) channels, branded mobile apps, or white label integrations with third-party online ordering or fulfillment apps.

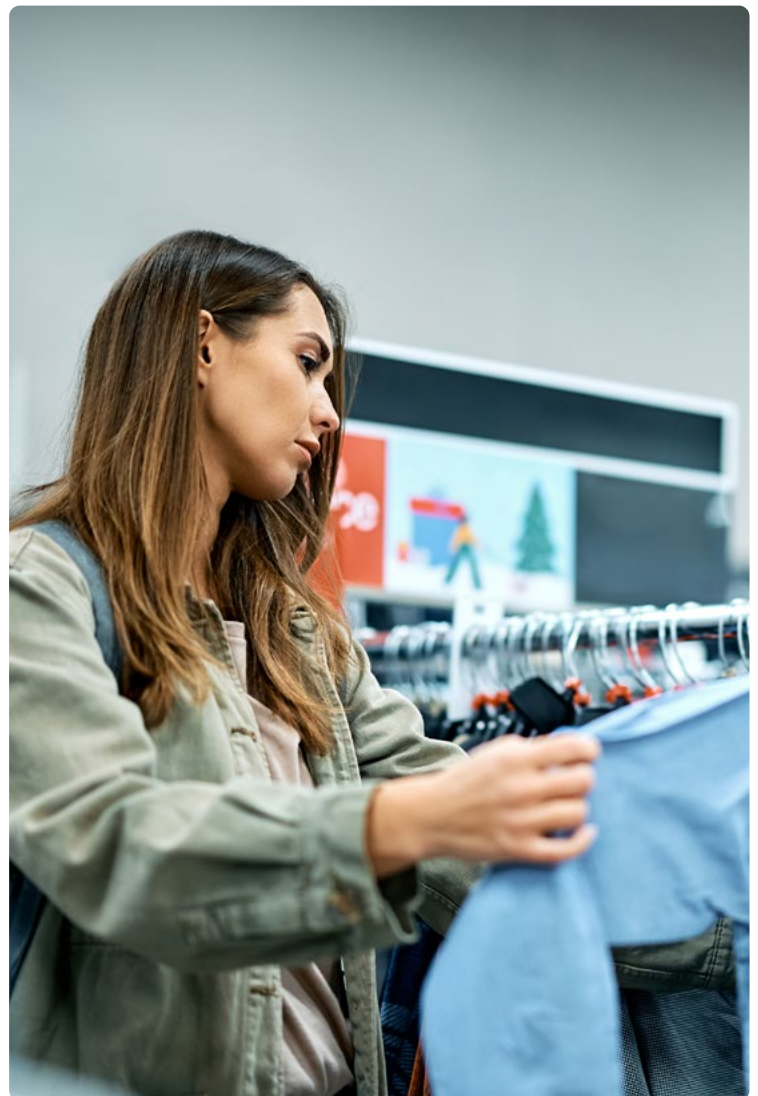
Online payments are more vulnerable to data breaches that expose card data and fraudsters using previously stolen personally identifiable information (PII) to make unauthorized transactions in someone else's name.

Solution:

End-to-end encryption and token-based security can help prevent fraud in card-not-present transactions.

Tokenization replaces sensitive card data with a token, obscuring it and making it worthless to fraudsters if there is a breach. Token-based security is non-negotiable as more retailers launch branded apps that may store card and loyalty program information.

Tokenization significantly reduces the online attack surface for retailers, enabling them to deliver a seamless, yet highly secure payments experience.





Omnichannel payment security: Hospitality

Challenge:

Hospitality businesses face growing complexity as payments span mobile, in-store, and unattended environments. From mobile checkout at hotels to QR code payments in restaurants and card-present transactions at gift shops, merchants must secure every touchpoint without adding friction, because convenience drives repeat business.

Solutions:

In hospitality, E2E and tokens can support secure QR code and mobile payments, but biometric security takes protection and convenience to the next level.

Biometrics deliver frictionless authentication that works across mobile, in-store, and unattended environments. By linking payment credentials to a customer's unique physical attributes, biometrics make transactions harder to compromise while eliminating the need for passwords or PINs.

Beyond mobile wallets, biometrics enable hotels, restaurants, and entertainment venues to offer personalized loyalty experiences, speed up in-person checkout, and secure self-service kiosks — all without adding complexity for staff or guests.

With [83% of consumers viewing biometric payments as safer](#) than traditional methods, adoption is accelerating and Verifone helps merchants leverage this technology to strengthen security and enhance the customer experience.

“Mobile devices are a great opportunity [for security]. This is the first time we’ve ever seen where people are comfortable with biometrics. Face ID is a great example. People are very comfortable with that. If we can leverage that so it doesn’t feel like it’s higher friction, we get a much higher level of security.”

Will Morgan, Chief Information Security Officer,
Verifone

83%

of consumers view
biometric payments as safer





Omnichannel payment security: Specialty retailers

Challenge:

Specialty retailers sell virtually everywhere, including brick and mortar, online, marketplaces, and more.

Selling through all these touchpoints creates more opportunities for fraudsters to access card data. These often high-value, loyalty-based transactions also may be more attractive to them, making specialized retailers a prime target.

Solution:

Specialized retailers need strong omnichannel payment security that encompasses hardware, software, and deployment.

Token-based security can protect card-not-present transactions as specialized retailers offer more payment methods, including mobile wallets and store card payments on their own D2C sites and companion apps.

PCI-validated point-to-point encryption combines secure devices, applications, and services, can protect data in transit and ensure it never touches the retailer's point-of-sale (POS) environment. Hardware-based security with tamper-proof devices and RSD technology can secure in-store transactions on payment terminals.

Payment orchestration to ensure end-to-end security across multiple integrated networks and processors is also critical.

Within its boundless payments ecosystem, Verifone empowers specialized retailers and other customers to operate with integrity, benefiting from built-in security and continuous fraud mitigation through a single point of access.





Accelerating boundless security for a boundless payments ecosystem

Whether it's a specialty retailer, QSR, or hospitality business, payment security must move beyond point-in-time, reactive compliance to a continuous, multi-dimensional process that proactively protects merchants across every payment touchpoint, method, and channel.

As businesses strive to offer consumers more convenience and choice, they must ensure their security infrastructure is just as boundless as their payments experience.

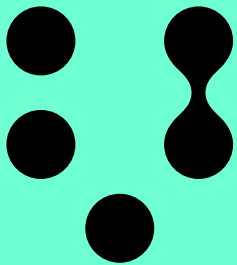
Verifone delivers a multi-layered security architecture that integrates hardware, software, and deployment protections into a cohesive strategy. This unified approach eliminates the need to manage fragmented solutions, reducing operational burdens while strengthening protection against evolving threats.

Verifone provides a trusted foundation for driving modern, seamless, and secure commerce experiences — protecting against today's threats while preparing businesses for tomorrow's.

**Contact us to see how
Verifone can help elevate your
omnichannel payment security.**

www.verifone.com





Get started today

The world's leading brands trust Verifone for global payments. We power the boundless payments grid — enabling distinctive commerce experiences for merchants, fintech companies, and financial institutions wherever commerce happens.

By combining a flexible payments platform comprised of devices, applications, services, acquiring and more, an open ecosystem of 2,500+ integrations, and four decades of payments expertise, Verifone eliminates complexity and expands what's possible across every payment channel.

Each year, Verifone processes \$8 trillion in transaction value across 165+ countries around the world helping businesses of all sizes to grow without limits.

Learn more at verifone.com

Verifone, Inc.

817 Broadway, Suite 1100

New York, NY 10003

United States