verifone

The Biometric Advantage: Converging Identity, Loyalty, and Payments

www.verifone.com

Contents

Contents

Emerging biometric technologies are reshaping the global payments landscape, enabling more seamless and personalized customer experiences.

Biometrics uses unique individual characteristics like facial features or fingerprints to verify identity. Introducing biometrics solutions can solve two key challenges that merchants face: enhancing customer experience and improving payment security.

As digital payment volumes surge—the global payments industry saw 3.4 trillion non-cash transactions in 2023 alone, according to McKinsey—they're expected to exceed $28.16 trillion by 2032. With this influx, biometrics like fingerprints, facial recognition, and palm scans have created new opportunities across retail, quick-service restaurants (QSRs), and convenience sectors. For merchants, biometrics solutions can deliver measurable benefits: Pilot implementations have reduced checkout times by up to 90 seconds per transaction and increased average ticket sizes by 4%.

Global digital payment volumes are growing, increasing the need for better customer convenience and security solutions that can adapt to modern settings, and there's real urgency for more secure, scalable authentication methods. Biometrics can help solve rising credit card fraud losses, which reached $33.8 billion globally in 2023, with the United States accounting for 42% of global fraud, according to the Nilson Report. These solutions can also play a critical role in delivering the seamless experience today's customers want—and expect—both online and in person. With 83% of Gen Z and 87% of Millennials comfortable using biometric authentication and an estimated one-half of Americans using the technology daily, implementing biometric authentication can position merchants at the forefront of payment innovation.

$33.8B

in credit card fraud losses

42%

of global fraud accounted for in the U.S.

> For merchants, biometric solutions can deliver measurable benefits: Pilot implementations have reduced checkout times by up to 90 seconds per transaction and increased average ticket sizes by 4%.
>
> — Payments Journal

Personalizing and securing the payments industry

As business and day-to-day life are reshaped by evolving digital and virtual interactions, verifying digital identity has become vital.

But for merchants and financial institutions alike, the ability to recognize and serve customers securely without adding friction to the experience is a core challenge. Biometric authentication is one of the most natural and secure ways to assess digital identity, providing a solution that can transform the customer's experience and solve key payment-related issues at the same time.

Conversations around biometrics in the payments industry today focus mostly on security and fraud detection. These are important, but the true power of biometrics begins with how it enhances the customer's experience.

Biometric authentication allows businesses to identify customers in context. After identifying customers through facial recognition, for example, a merchant can deliver personalization, convenience, and seamless interactions tailored to a specific individual. Biometrics unlocks the ability to personalize greetings, connect to loyalty programs, use coupons, speed up transactions, remember preferences, and facilitate contactless secure payments in seconds.

Two-thirds of adults globally use digital payments—a number that rises to an estimated 89% in the United States. Traditional authentication methods, like passwords and PINs, aren't keeping pace with security needs. A four-digit PIN has a one in 10,000 chance of being guessed, and those odds increase when considering the sophisticated techniques fraudsters use to attack systems today. Passwords aren't much better, with Pew Research Center finding that 69% of people are overwhelmed with how many passwords they have to remember, and nearly half feel unsure if those passwords are even secure enough.

Biometrics emerges as a natural, intuitive way to verify identity allowing for a more secure and personalized customer experience. A variety of biometric methods, including fingerprints, facial recognition, and even palm scans, are already driving everyday interactions, from unlocking digital devices to checking banking applications. As payment systems and the threats they face evolve, biometrics offers a dynamic balance between convenience and control.

2/3

of adults globally use digital payments

89%

of adults in the United States use digital payments

69%

are overwhelmed with how many passwords they have to remember

How digital identity shapes commerce

Verifying digital identity is a process that uses tools—from biometrics to multi-factor authentication—to confirm who a person is and that they're authorized to take a specific action, such as making a purchase or accessing sensitive information. Digital identity impacts many use cases in the physical and online worlds—without it, the digital economy can't function.

Merchants that verify digital identity can benefit from a host of different opportunities. Digital identity is the gateway to faster checkouts, instant loyalty rewards, personalized experiences, and streamlined operations. In addition, biometrics can provide a more secure digital payment environment, which can help fight fraud.

What does biometric verification actually mean? TechTarget notes that "biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits."

In physical settings, like stores or in-person events, facial recognition or other "body-based" modalities are popular. Face and palm are two biometrics models that will likely be widely adopted in payments, given their relatively non-intrusive nature, and the fact that both are more acceptable for consumers versus other models like iris patterns or fingerprints.

Biometric verification technologies use a variety of physical characteristics to verify identity, including:

Fingerprints

Facial image

Voice characteristics

Palm vein mapping

Iris patterns

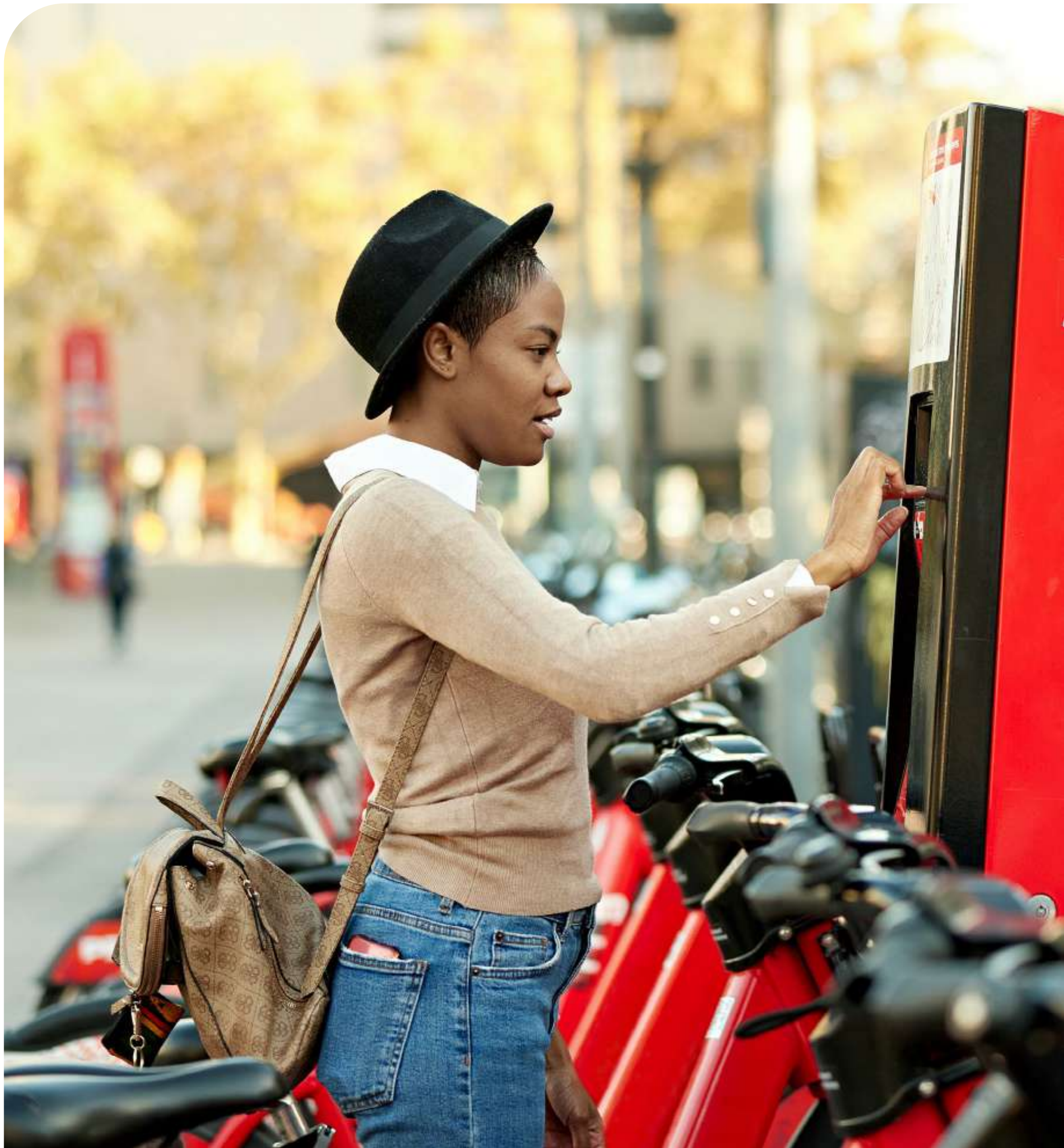
Behavioral biometrics

Navigating the evolution of payment initiation

Non-cash payment verification has been on a trajectory toward greater convenience, speed, and security.

In the 1950s, BankAmericard introduced paper payment cards, which quickly evolved to the plastic cards still in use today. By the 1970s, magnetic stripe technology was added to offer electronic data capture capabilities at checkout. EMV chip cards with embedded microchips made it easier to authenticate payments, widely in use by the early 2000s. As smartphones and other mobile devices became more sophisticated, mobile devices transformed payments again with the introduction of digital wallets.

Over the last decade, biometric authentication has gained wider acceptance largely through its use in Android and iOS digital devices. Smartphone users around the world started using biometrics with their devices daily. Merchants have taken biometrics further into everyday commerce, allowing seamless checkouts and plan to pilot them in a variety of settings. As commerce and merchants gravitate towards an omni-channel strategy prioritizing fast, convenient transactions with consumer preferences and personalization built in, biometric-initiated transactions are the next evolution. Just as cards became the industry norm in the 70s, it's expected that biometrics will grow from the current state to the norm by the 2030s.



The modern biometrics landscape

Improvement in identity verification isn't just about solving a single problem; it's also about addressing critical pain points.

Repeat friction during checkout, including poor or lengthy identity verification at the point of sale, can lead to long lines, abandoned purchases, and customer frustration. Over time, these experiences can hurt both merchant revenue and consumer trust. Biometric authentication can help address these hurdles while improving security and compliance.

Expanding legislation on privacy and security are creating alignment for biometric authentication. Regulations like GDPR, PSD2, and ISO 27001 are increasing the demand for secure and privacy-oriented authentication methods. GDPR, for example, requires explicit user consent and clear disclosure regarding personal data handling. PSD2's Strong Customer Authentication (SCA) requirement highlights biometrics as a secure means of verifying customer identity during transactions.

ISO 19092 also underscores this trend, outlining the security framework for the use of biometrics in financial services. It focuses specifically on retail payment authentication and provides guidelines for implementing biometrics technologies. Biometrics solutions that offer privacy by design, advanced encryption, localized storage of data, and resistance to common fraud techniques are becoming part of the toolkit merchants can use to meet the increasing burden of staying in compliance with growing privacy and security laws.

GDPR, PSD2, and ISO 27001
are increasing the demand for secure and privacy-oriented authentication methods, such as explicit user consent and clear disclosure regarding personal data handling.

ISO 19092
focuses specifically on retail payment authentication and provides guidelines for implementing biometrics technologies.

Understanding the key drivers for biometric adoption

Consumer convenience and user experience

One of the most important advantages of biometric authentication is faster checkout and enriched personalization.

In fact, 82% of customers avoid businesses with long lines and 40% will abandon a purchase if it takes too long to check out. Solving this issue can translate to bottom-line growth.

Today's shoppers want a consistent experience across channels. Within online environments, consumers are "known" via logins, cookies, credentials, and other factors, leading to curated content, one-click checkouts, and personalized experiences. Biometrics allows the instant recognition needed for the physical retail experience to mirror the personalized, efficient experience of digital shopping. With biometrics, people can be recognized, remembered, and rewarded, enabling them to have consistent customer experiences across a merchant's digital and in-person touchpoints.

82% of consumers avoid businesses with long lines

40% will abandon a purchase if it takes too long to checkout

Biometrics provides the following advantages:

- Instant recognition
- Personalization with curated content
- Customer rewards and loyalty
- Consistent checkout process across digital and in-person transactions

Imagine walking into a store, being instantly recognized, and offered product recommendations based on your past purchases and preferences.

Then, when you go to checkout, you get immediate access to loyalty programs, coupons, and a digital wallet that lets you check out with just a smile or a swipe of your palm. Biometrics can reduce checkout friction while utilizing personalization to simplify choices, suggest favorites, and drive loyalty. And, you have the same experience you're used to online, in-store.

Merchants are also using biometrics to explore a variety of use cases. For example, biometrics could be used to allow access to changing rooms when shoppers are trying on clothes. Other retailers are piloting the in-store equivalent of retargeting based on items shoppers interacted with but didn't purchase. Biometrics can enhance the data merchants collect and have to act on, without being intrusive or creating a burden for their customers.

Potential use cases

- Recognize and offer product recommendations based on your customer's past purchases and preferences
- Provide immediate access to loyalty programs and coupons
- Offer additional personalized options based on what shoppers currently have in the fitting room and previous purchases
- Retargeting based on items shoppers interacted with but didn't purchase

Seamless integration

Another point driving biometrics adoption is the development of solutions that integrate with merchants' existing technology stack and customer experience design.

Modern biometrics systems can be deployed easily at the point-of-sale, with a user experience that improves checkout. For example, an integrated camera at eye level that's designed with a "smile and checkout" experience can easily disarm wary customers.

Technology integration is also key. One aspect of this may be integrating the biometrics reader into the processing support that already exists within checkout lanes. It's important that systems seamlessly integrate with loyalty programs, payment systems, and other identity verification layers, too.

Vendors that offer open APIs, SDKs, and modular and compatible hardware can help merchants avoid "rip-and-replace" scenarios. Choosing a partner with proven interoperability, hardware-agnostic design, and flexible deployment options can drive a smooth technical integration, along with a better customer experience.

Operational efficiency for merchants

Biometrics can also unlock improved efficiencies. Across industries, use cases show faster throughput, reduced transaction times, and streamlined workforce management.

For example, facial authentication at stadiums supported faster entry and improved customer experience during active trials. Biometric ticketing gates processed fans 68% faster than the next-fastest option and achieved 2.5x throughput over standard gates in one pilot.

In high-volume locations, integrations with technology, like AI-powered autonomous retail solutions, allow a user experience where you can simply pick up items from store shelves and walk out. As a result, lines can move faster and staff are freed up for higher-value activities, such as interacting with customers and opening additional lines to speed up processing during peak hours.

68%

faster ticketing gate processed by biometrics

2.5X

throughput achieved over standard gates in one pilot

Security and fraud prevention

The Nilson Report projects that, over the next decade, global credit card fraud card will hit an accumulated $403.88 billion.

Biometrics eliminates many common fraud techniques, including the fastest-growing type of fraud: account takeover (ATO). By verifying the identity of the person conducting the transaction, ATO fraud becomes much harder to execute.

By using unique personal characteristics and live detection methodologies, biometrics can create verified identity trails. Not only can this improve the approval rates of transactions and dissuade fraud, but it can also make it easier to resolve other payment-related issues. Friendly fraud, or a customer disputing a legitimate charge, is less likely to happen when there’s biometric information verifying a purchase. Customers know it was them who made the purchase based on the biometric requirements, and can have confidence in their transaction history. Fighting first-party fraudulent chargebacks is also easier with biometric authentication, which serves as strong evidence that a purchase was valid.

$403B

of global credit card fraud card is projected to accumulate over the next decade

Biometric authentication: Real-world use cases and applications

Biometric authentication supports a wide variety of use cases across industries. Whether it's a personalized experience at a retail store or online, or a quick transaction at a fast-food restaurant or convenience store, brands are seeing biometrics elevate the checkout experience in a number of ways.

Retail and e-commerce

Member verification
A global warehouse retailer uses biometrics for faster member check-ins. Other merchants validate membership in loyalty or discount programs.

Personalization
High-end retailers use biometrics to deliver white-glove service. A luxury department store enabled customers to "opt-in" at checkout, linking identity with personalized offers and VIP services.

Faster checkout
A global retailer deployed a solution in hundreds of retail stores that allows shoppers to check out by scanning their palms, connecting payment and identity seamlessly.

Convenience stores and gas stations

Loyalty programs
Biometrics can simplify loyalty programs. A regional gas store chain implemented palm authentication at gas pumps to auto-apply loyalty points and discounts.

Payments for outside purchases
With biometrics, users can pay quickly at the pump and skip a trip inside the store to verify their identity or payment. Expense managers can ensure fleet card use is authorized.

Age verification
When stores sell age-restricted products, biometrics can be used to estimate age and validate IDs for smoother adherence to relevant laws.

Quick service restaurants

Speed of transaction
Fast-food brands use facial recognition for order recall and loyalty benefits, improving order speed and upsell opportunities.

Personalized offers
With biometrics, QSRs can access a user's order history and preferences to recommend relevant deals, promotions, and items to increase average order value and conversions.

Order pickup
Biometrics can be used to verify the identity of pickups for online orders and order-ahead apps.

Live events and travel

Faster check-in
From sports events to theme parks to airports, biometrics can quickly verify identity and speed up the check-in process to minimize long lines.

Age-verification
Whether it's selling age-restricted products or verifying age for access to "above 21 only" areas, biometrics can validate identity and age.

Identity verification
In settings such as international travel or healthcare where tight identity controls are crucial for safety, biometrics adds another layer of security that identities have been validated.

Faster checkout
A fingerprint or face scan can alleviate a lengthy wait and long checkout time at the concessions stand for concerts, sports games, or theme parks.

Cross-industry applications

Employee authentication
Biometrics can simplify clock-in/clock-out access management and other employee interactions. The technology can also reduce time theft, automate HR tracking, and manage access to sensitive data or spaces.

Omni-channel integration
No matter the context, biometrics can unify the customer experience across digital and physical touchpoints with one identity thread. For example, the ability to associate the online purchase of a concert ticket with the arrival of the consumer at the concert venue.

Biometrics concerns and challenges

While biometric authentication offers significant advantages for managing digital identity, improving customer experiences, and eliminating fraud, there may be some concerns and challenges to consider before deploying it.

Often, companies are concerned that customers won't be willing to use biometrics. However, people are increasingly exposed to and comfortable with biometrics, using the technology to access digital devices, banking applications, and more.

In a study from Aware, 75% of respondents believed biometrics were more secure than passwords. Over half of respondents reported they were comfortable using biometrics in a public setting, such as at a bank or retailer. The willingness to adopt biometrics is only going to increase as younger generations grow more familiar with and open to the technology throughout the course of their lives. In the same study, around 85% of Gen Z and Millennials reported that they're comfortable using biometrics in their daily lives.

While 69% of respondents in a recent survey self-identify as excited to try new payments, biometrics requires transparent data practices to support adoption. Successful systems emphasize local data storage, user control, and voluntary participation.

According to McKinsey, 85% of consumers want clear data privacy policies before making a purchase. Transparency and control over biometric data are essential to fostering user trust.

75%

of respondents believed biometrics are more secured than passwords

69%

self-identified as excited to try new payment methods

When looking at biometrics system deployments, these factors underlie success:

Consent and the ability to opt-in
Biometrics that allow users to opt-in, rather than forcing them to adopt a single approach or opt-out, tend to be more successful.

Transparent data policies
Clearly highlight what data you're collecting, how it's being used, and how customers can access (or delete) their data as requested.

Data management
Be upfront about how long data is retained and where it is stored. For example, biometric data that's retained on a local device and deleted after a period of time is more likely to feel privacy-aligned to concerned users.

Communication
Transparency in communication around biometrics, privacy, and data usage is critical. Outline your protections in straightforward policies, physical signage, onboarding flows, and opt-in moments to give customers clarity and build trust.

Evaluating and implementing biometric solutions

When choosing a biometrics solutions provider, it's important to evaluate potential vendors through a multi-faceted lens.

Choosing a partner involves understanding what features they offer, the modalities they support, their approach to security, and whether they're positioned to advise you on critical factors, such as regulatory compliance and adapting biometrics to take advantage of new opportunities.

Factors to consider include:

Encryption

Where are reference data and live-captured data stored, on the local device or in the cloud? Is the data encrypted while in transit and at rest? Understand the vendor's data architecture and approaches to encryption, security, and data management.

Ability to scale

Does the vendor prioritize the features needed to scale easily? Look for open architecture, interoperability, and the ability to run on different devices to better understand the vendor's commitment to scaling with you as you grow and supporting your preferred architecture.

Deployment flexibility

When evaluating vendors, consider how flexible the deployment of solutions is. For example, are they designed to be mounted with ease in a variety of settings, or do they require highly specialized talent to deploy? Deployment flexibility can have a significant impact on the timing, budget, and support needed to deploy biometrics at scale.

Multiple biometrics modalities

Does the biometrics provider you're considering support only one modality, such as facial ID, or are they able to use different forms of biometric data to validate identity? The ability to support multiple biometric modalities is important for two reasons. First, it allows you the flexibility to select the options right for your needs in any scenario. Second, if you plan to implement two-factor authentication, you can look at multiple biometric data points—for example, facial ID and fingerprint—in a single transaction for greater security controls.

Security measures

Fraud detection systems continuously analyze transaction patterns, user behaviors, and biometric authentication attempts to spot anomalies. These cutting-edge solutions can quickly find and block spoofing attempts, unusual spending habits, or suspicious device activities.

Point-of-sale compatibility

Does the vendor's biometrics solution work with your current hardware, specifically point-of-sale or terminal? Are they limited to a specific set of devices, or are they manufacturer-agnostic? When a biometrics solution is hardware-agnostic, merchants can change systems without disrupting their identity verification processes.

Consistent performance

Biometrics solutions are often operating in difficult environments. For example, a convenience store may have spotty connectivity, while an outdoor event operates rain or shine. Does the solution leverage different sensors and cameras to complete its work and potentially provide a fallback in case of a technical failure? In environments where IT staff may not be immediately available to solve issues, reliable performance through intelligent design becomes critical.

Standards-driven, interoperable solution

While there's currently no unifying standard for biometrics in the payments field, there's an urgent need for standards in the space. Consider choosing a vendor that's actively calling attention to the need and taking a standards-based approach to their development. Does the underlying design reflect a commitment to interoperability with the solutions you use now or are likely to adopt in the future?

Implementation support

What kind of implementation support and long-term partnership management does the vendor offer? From day one, a strong partner will help develop a blueprint to make the most of biometrics capabilities in your business and be ready to advise, scale, and adapt to your changing needs over time. Implementing biometrics can feel challenging, so choose a vendor that provides comprehensive support and services that can help you turn biometrics into a competitive advantage.

Compliance

When selecting a biometrics payment processing provider, choose one that understands regulatory compliance. Prioritize providers that offer clear, user-friendly consent mechanisms and have specific procedures to comply with major privacy laws, like GDPR (E.U.) and CCPA (U.S.), and biometric-specific regulations, such as Illinois's BIPA. In addition to providing detailed information about how they comply, strong partners will have the resources to advise you on how to keep your deployment compliant and updated with fast-moving regulations.

Liveness detection

Liveness detection differentiates between a real biometric sample and a spoof or photograph. Deepfake mechanisms form a core component of liveness detection to identify synthetic media used to impersonate real users. What algorithms and other strategies does the vendor use for liveness and deepfake detection, which can be as simple as detecting blinking, breathing, and other tiny movements? Does the solution employ AI-based image forensics and behavioral analysis to detect deepfakes? There are different approaches to liveness detection, but a vendor's approach should be current, comprehensive, and evolving.

Verifone biometrics: How we’re differentiated

Verifone’s biometric solutions support facial and palm recognition, integrating directly into both Verifone and third-party POS systems.

Our solution enables merchants to quickly deploy technology that supports:

- Seamless customer check-ins, faster checkouts, and personalized experiences
- Loyalty and rewards integration at checkout
- Payment authorization via biometrics
- Support for multiple payment methods

Our system is designed with privacy and a positive end-user experience in mind. The solutions support opt-in enrollment, localized data control, and privacy-first principles that make it easy to align the technology with your data policies and proactively address customer concerns.

Our biometric modules integrate with both Verifone and non-Verifone payment terminals for maximum interoperability across retail environments without lock-ins. With merchant rails compatibility, it works without requiring new backend systems.

Open architecture and multi-modal capability make it easier to scale or adopt new hardware in the future, without impacting biometric verification capabilities.

Innovative technologies must be designed with edge use cases in mind. Merchants rarely have IT support on hand to troubleshoot issues, so reliability is a core consideration. Verifone's biometric hardware drives quick, accurate identification, integrating an array of sensors and cameras that deliver reliable performance even in challenging conditions.

Since our biometric platform is built with interoperability in mind, we're working with the industry to create the industry standards. This allows interconnectivity between different types of biometrics solutions and ensures a seamless experience for the consumer. The goal is that once a consumer enrolls with any consumer platform, that same consumer would be able to check-in and pay on any Verifone biometrics-enabled terminal around the world.

From a consumer perspective, Verifone's biometrics enhance convenience. They integrate smoothly into payment and loyalty systems, creating personalized, frictionless transactions with a user experience that encourages adoption and long-term use.

Understanding the technology behind Verifone's biometrics highlights our key differentiators. With solutions designed for both small-to-midsize (SMB) organizations and enterprise clients, our modules offer versatile mounting solutions ensuring adaptability to diverse use cases, such as countertop, mobile, or in-lane environments. With privacy and security central to design, data processing and storage occur on highly secure biometric vaults.

Verifone's approach also supports flexible connectivity options, using USB-C for robust enterprise setups and Bluetooth for SMB deployments for consistent performance tailored to varying business needs. Ultimately, choosing Verifone biometrics means investing in proven technology optimized for performance, adaptability, and security.

For customers, Verifone's UX emphasizes speed and clarity: check-in takes seconds, loyalty is automatically applied, and payments are seamless. For merchants, it means increased throughput and stronger customer retention.

> Our system is designed with privacy and a positive end-user experience in mind. The solutions support opt-in enrollment, localized data control, and privacy-first principles that make it easy to align the technology with your data policies and proactively address customer concerns.
>
> —Verifone

Future outlook: Why invest in biometrics in payments now?

Biometrics technology is evolving rapidly.

Behavioral biometrics, AI-assisted verification, and multimodal systems are offering new levels of security and expanding biometrics into entirely new use cases. For merchants, integrating biometrics capabilities now lays the foundation for digital identity offerings that provide a competitive advantage.

There's never been a moment when consumers are more willing to adopt biometrics. Generation Alpha, raised on digital interactions and biometric-enabled devices, expects fluid, secure experiences. Gen Z and Millennials are ready to embrace biometrics on a daily basis. And there's a willingness to explore how biometrics can create value across other demographics, with the right data policies and communication.

Tomorrow's biometric systems will power immersive virtual shopping experiences, self-checkout without scanning, and voice-activated personalized commerce. The future of payment initiation is hands-free, identity-driven, and context-aware. With advanced security and anti-fraud capabilities supported by biometric identity verification, payment security and ease will continue to increase.

As more companies align with standards and customer expectations shift, those who invest now will be positioned to lead the next revolution in the payments industry. It's time to explore how biometric solutions can transform your customer experience and payments process.

Discover how Verifone can help future-proof your payment system with a secure and seamless biometric solution today by connecting with a representative.

Appendix A

Glossary

1. **Behavioral biometrics**
   Non-physical identity verification that's based on patterns of behavior in digital environments, like typing cadence, mouse movement, or navigation habits.

2. **Biometric authentication**
   Verifying identity using unique biological traits, such as a person's fingerprints, facial features, iris patterns, or voice.

3. **Card-Not-Present (CNP)**
   A transaction where the cardholder does not physically present the card to the merchant, typically online or by phone.

4. **CCPA (California Consumer Privacy Act)**
   U.S. state legislation that gives California residents rights over how their personal data—including biometric data—is collected, used, and shared.

5. **Contactless payment**
   A transaction method that uses RFID or NFC technology, allowing users to tap a card or device to complete a payment without swiping or inserting.

6. **Digital identity**
   A digital validation of a person's identity, typically used for online access, authentication, and personalized services.

7. **EMV (Europay, Mastercard, and Visa)**
   A global standard for smart payment cards and terminals that use chip-based authentication for secure transactions.

8. **Face ID**
   A facial recognition system used to unlock digital devices or authorize transactions, often via device cameras.

9. **Fingerprint recognition**
   A widely used biometric technology that identifies individuals by matching unique fingerprint patterns.

10. **Fraud Detection AI**
    Artificial intelligence algorithms that monitor and detect anomalies in transactions or user behavior to prevent fraud.

11. **GDPR (General Data Protection Regulation)**
    A regulation that governs data protection and privacy in the European Union, with specific provisions for handling biometric data.

12. **KYC (Know Your Customer)**
    Regulatory standards requiring businesses to verify the identity of their customers to prevent fraud, money laundering, or terrorism financing.

13. **Liveness detection**
    A biometric security feature that determines whether the trait being captured (e.g., face or fingerprint) is from a live person and not a spoof or replica.

14. **Palm vein recognition**
    A biometric method that maps the unique pattern of veins inside a person's palm using infrared light to validate identity.

15. **POS (Point of Sale)**
    The physical or digital location where a retail transaction is completed, including the software and hardware that processes payments.

16. **PSD2 (Payment Services Directive 2)**
    A European regulation that requires strong customer authentication and promotes innovation, competition, and security in digital payments.

Appendix B

Regulatory compliance checklist for biometric payment systems

Accessibility and inclusion

- Provide alternative authentication methods for users who don't want to use biometrics.
- Choose systems that are tested across a diverse demographic population.
- Identify potential biases or gaps in data training sets that may impact customers or specific user groups.

Authentication and security standards

- Adhere to PSD2 SCA requirements for strong customer authentication in Europe.
- Align with ISO/IEC 30107-3 standards for presentation attack detection (liveness).
- Use AI-driven fraud detection tools for real-time threat monitoring.

Biometric-specific legislation

- Comply with GDPR (E.U.): Define legal basis for processing; register as a data controller if necessary.
- Comply with CCPA (U.S.): Offer opt-out rights, data access, and deletion requests.
- Follow BIPA (Illinois): Get written consent and inform users of purpose, duration, and use of biometric data.

Data privacy and consent

- Offer clear, affirmative opt-in for biometric data collection.
- Develop transparent, accessible privacy policies.
- Allow users to manage, delete, or revoke their data through easily accessible means.
- Document how data is collected, used, and retained in an understandable public statement.

Interoperability and vendor compliance

- Verify that vendor platforms are compliant with ISO 27001 and PCI DSS.
- Conduct vendor risk assessments and request third-party security audits.
- Require transparency about how biometric data is processed, stored, and deleted.
- Discuss the ecosystem as a whole, ensuring software, hardware, and biometrics solutions that have true interoperability.

Monitoring and response

- Establish a data breach response plan for biometric data incidents.
- Create a schedule to regularly review compliance practices and update policies as regulations evolve.
- Train staff on biometric system security, data handling, and regulatory awareness.

Secure data storage and transmission

- Role-based access control for biometrics data.
- Encrypt biometric data from end-to-end, both at rest and in-transit.
- Ensure biometrics data are secure and protected based on industry standards.

Verifone
817 Broadway Ste 100
New York
NY 10003, USA
Fax: 4545 233
Phone: 001 454 2333

www.verifone.com

Verifone is a leading global payments technology provider trusted by the world’s top brands. We power the boundless payments grid—enabling distinctive, seamless payment experiences for merchants, fintech companies, and financial institutions wherever commerce happens. Our flexible platform, open ecosystem of 2,500+ integrations, and decades of on-the-ground payments expertise help eliminate complexity, unlock new markets, and expand what’s possible with every transaction. Operating in 165 countries and processing $8 trillion in annual transaction value, Verifone is the front door to global commerce in a rapidly changing payments landscape.

Learn more at www.verifone.com

WP202505TBA | Published May 2025

verifone