VIEW POINT

FOSTERING PAYMENTS SECURITY WITH BEHAVIORAL BIOMETRICS

Abstract

Despite the technological advancements, Financial Institutions still grapple with Customer authentication—passwords, PINs, OTPs, and even physical biometrics—as they fail to counter modern fraud techniques. To address the security and customer experience challenges, banks are adopting **behavioral biometrics**, which analyzes unique user interaction patterns to provide a powerful, frictionless layer of defense. This approach complements the prevalent methods and further enhances both security and usability. Maximizing the value of behavioral biometrics implementation requires thorough evaluation of the technology, its uses, limitations, and implementation factors.

Infosys | CONSULTING

Why Prevalent Authentication Sometimes Falls Short

Prevalent authentication methods—passwords, OTPs, and even physical biometrics—fall short in today's threat landscape.

1. **Weakness of Static Credentials**
   Passwords & PINs are weak links. In 2023, 86% of data breaches involved stolen credentials[1]. Users often reuse simple passwords or PINs like "1234," making them easy targets. Managing them is frustrating—51% of users reset passwords monthly[2], leading to lockouts and poor UX.
2. **OTP Vulnerabilities**
   OTPs are no longer reliable. SIM-swapping, phishing, malware apps etc. allow attackers to intercept codes. OTPs can also get delayed or fail to arrive, frustrating users and driving up support costs.
3. **Risks in Physical Biometrics**
   Physical Biometrics (like fingerprints or facial recognition) offer convenience but are vulnerable. Deepfake attacks surged 704% in 2023[3], and malware like GoldPickaxe can steal facial data. Unlike passwords, compromised biometrics can't be changed.
4. **Rising Digital Fraud**
   The post-pandemic digital boom has expanded attack surfaces. Account takeovers, synthetic identities, and social engineering are outpacing traditional defenses. ATO fraud rose 62% YoY, and online payment fraud is projected to exceed $343B globally by 2027[4].

In addition to the above limitations, emerging market trends are driving the need for advanced authentication layers in banking:

1. **Regulatory Momentum:** Global regulations (PSD2, CCPA, RBI guidelines) demand stronger, privacy-compliant authentication. Behavioral biometrics supports PSD2's "inherence" factor for real-time, low-friction identity verification.
2. **Smarter AI Models:** Modern behavioral models self-adjust in real time, reducing false positives and improving fraud detection and customer satisfaction.
3. **Demand for Seamless UX:** Users expect invisible security that doesn't disrupt their digital experience.

Behavior Driven Banking Security

Behavioral biometrics convert digital behaviors into an individual's unique behavioral fingerprints, examining how people interact with devices, like typing speeds, mouse movements and swipe gestures, rather than their static physical traits like fingerprints.

These interactions are analyzed in real-time to build behavioral fingerprints and detect anomalies that may indicate account takeover or fraud.

When the risk score increases, the system triggers a step-up authentication (e.g. biometric re-check, security questions or out-of-band challenge) to confirm the genuine user while keeping low-risk journeys seamless.

1. Key Advantages of Behavioral Biometrics over Traditional Methods

- **Frictionless Security:** It silently verifies identity through natural behavior, enhancing security without disrupting the experience[5].
- **Continuous Authentication:** It can continuously monitor user behavior throughout a session, and not just at login. If an attacker gains access, their behavior will likely differ, triggering alerts or re-authentication[6].
- **High Accuracy:** It detects subtle anomalies which static methods miss. AI-driven systems analyze thousands of behavioral data points per session. These traits are difficult to fake, making it easier to detect bots, remote access, or social engineering attempts[7].
- **Spoof-Resistant:** Behavioral traits are harder to replicate than passwords or fingerprints. Even AI deepfakes struggle to mimic real-time behavior like typing cadence or device handling[8].
- **Adaptive Learning:** The system evolves with the user, updating profiles over time. It uses risk scoring to determine when to prompt for additional verification, balancing security and convenience[9].

2. Limitations of Behavioral Biometrics

Despite all the advantages, behavioral biometrics is best treated as a probabilistic risk signal, not a silver bullet – its effectiveness depends on layering with other controls, careful tuning, and strong governance.

Behavior changes over time: Behavioral biometrics is vulnerable to "behavior drift" or model drift (model's performance degrades because the data on which it has been trained has changed). A user's interaction style is shaped by context, device, mood, health, and habit changes, so a profile built last month may not fit perfectly today. This is the main reason it should not be treated as a hard yes/no authenticator on its own.

It produces both false positives and false negatives: Like all biometrics systems, behavioral systems make errors. Tightening thresholds may catch more fraud but can also challenge more legitimate users; loosening thresholds improves convenience but can let more bad sessions through.

Accessibility and inclusion can be difficult: User temporary injuries, assistive technologies, or non-standard interaction pattern may not fit the normal profile the system expects.

Device and sensor dependency can hurt accuracy: Behavioral models can be sensitive to the quality of the input stream. On mobile, damaged sensors, missing data, different screen size, keyboard layout, OS updates, browser changes, and app redesigns can all distort the captured behavior and degrade model performance.

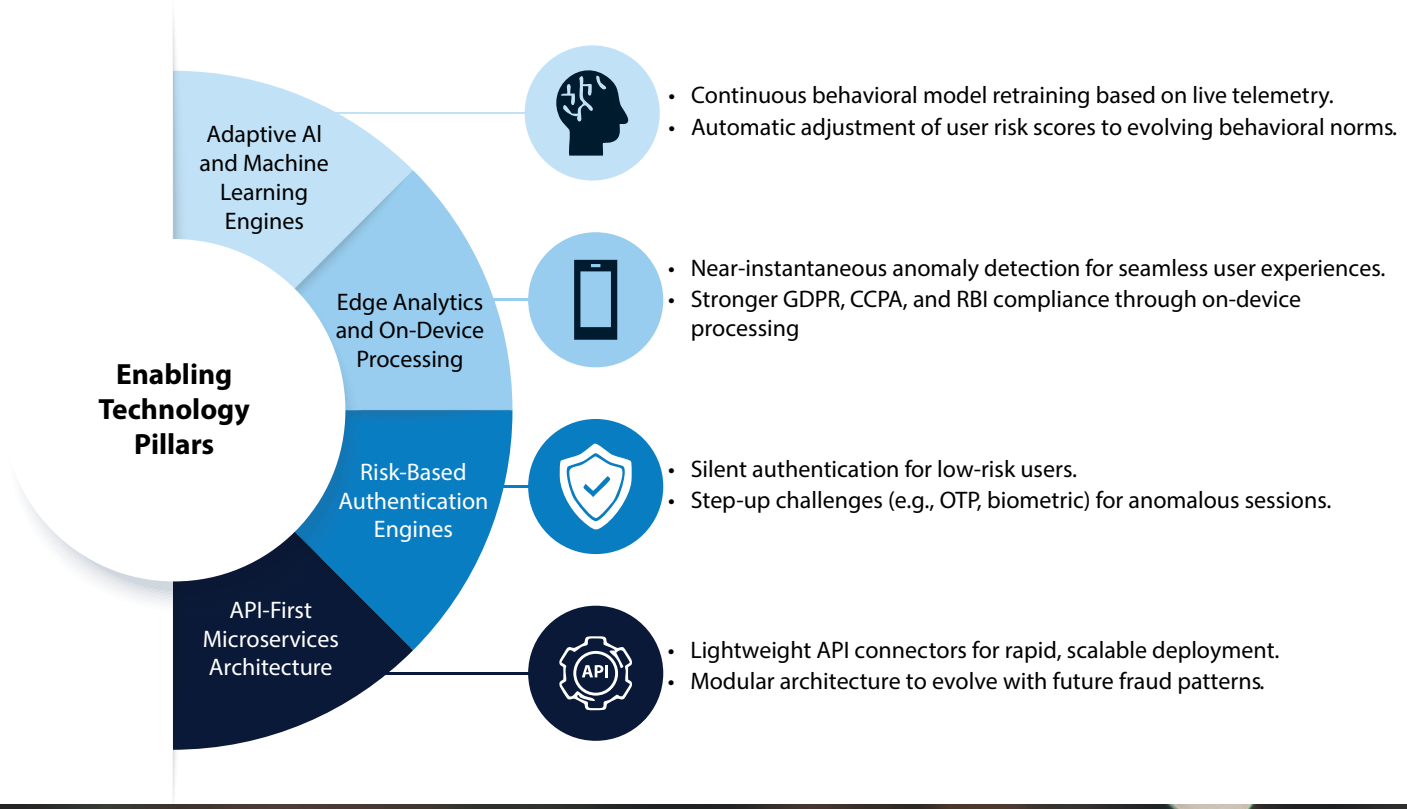
Above shortcomings can be addressed through disciplined lifecycle management rather than one-time deployment. Behavior models should be retrained regularly using recent trusted data and adaptive baselines so that genuine changes in user behavior do not trigger unnecessary alerts. Device and sensor dependency

can be reduced by using device-aware normalization, cross-channel calibration, and fallback to other signals when telemetry quality is weak. Model tuning should be continuous, with threshold reviews, champion-challenger testing, and segment-wise monitoring of false positives. Most importantly, behavioral biometrics should remain one input into a broader risk engine, supported by step-up authentication and manual review where needed.

Enabling Technology Pillars

Behavioral biometrics rely on a set of interconnected technologies to deliver real-time, scalable, and privacy-conscious authentication solutions. It must be architected as part of an adaptive, API-driven digital trust ecosystem - not as a siloed fraud solution. An API-first, microservice based architecture enables behavioral biometric engines to ingest high-frequency behavioral telemetry (such as keystroke dynamics, touch interaction, and navigation patterns) directly from digital channels in real-time. These APIs expose risk scores, anomaly indicators, and confidence levels that can be consumed by downstream systems – to flag anomalous behavior.

Microservices also fit well with real-time decisioning. Behavioral Biometrics has multiple services for collecting session telemetry, feature engineering, risk scoring/model inference, decisioning/orchestration and case management or alerting. It is used for continuous authentication and risk-based response during the session, not just login. That means the platform must ingest signals, that means collecting session telemetry might require higher compute power than case management or alerting. Therefore, a loosely coupled architecture with independently deployable services, where compute-intensive components can scale independently, is best suited for behavioral biometrics.

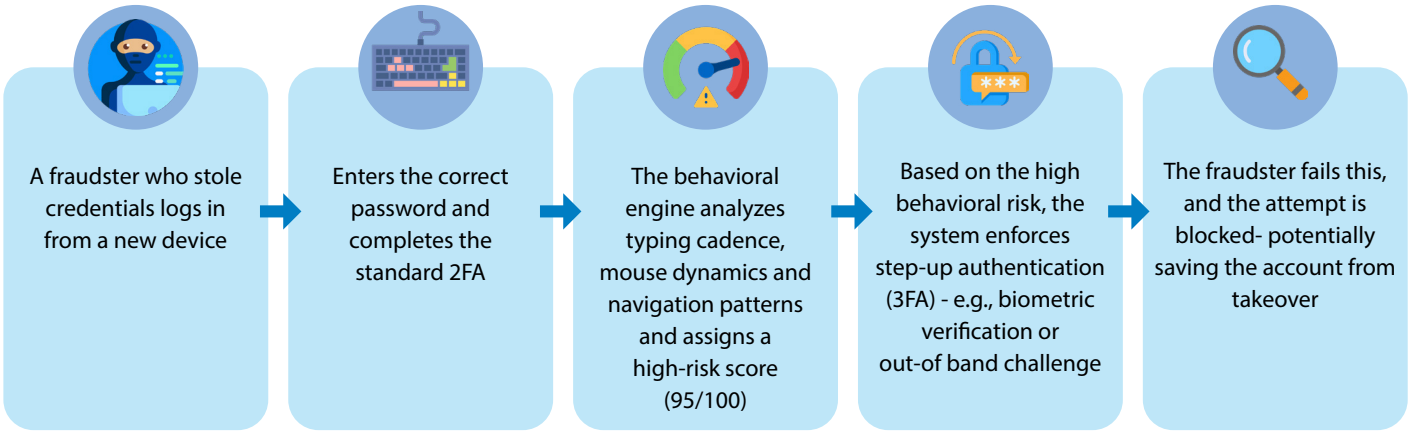


Behavioral Biometrics in action

Use Cases

In this section, we understand the typical use cases and user journeys where behavioral biometrics come into action and help in detecting anomalies in real-time.

1. Anomaly Detection Workflow



User Journeys that can be secured using Anomaly Detection Workflow:

A. New Payee / Beneficiary Addition

Adding a new beneficiary is a high -risk event in digital banking. Fraudsters often take over an account and then add a mule account before making a transfer.

Example -

Behavior Signals may detect:

- Unusual hesitation or speed
- Pasting account details rather than normal entry
- Robotic Navigation
- Different interaction style from historical profile

Fallback:

- OTP plus app approval
- Cooling period before beneficiary activation
- Static biometric confirmation
- Manual Verification for very high-value cases

This is one of the strongest use cases of anomaly detection because it sits at a fraud-critical point in the customer journey.

B. Payment Initiation and Authentication

When a user initiates a transfer, bill payment or card-not-present transaction, behavioral biometrics can assess whether the way the payment is being created feels genuine.

Examples:

- Normal user behavior with a familiar payee and typical amount: low friction
- Unusual amount, rushed interaction, copied values, odd navigation pattern: step-up
- Highly abnormal behavior combined with risky device/network indicator: block or hold

Fallback:

- OTP
- Transaction signing/app based confirmation
- Face/fingerprint confirmation
- Delay-and-review for very high-risk payment

C. Account recovery/password reset

Recovery journeys are heavily targeted because they let attackers regain control without knowing the user's normal credentials.

Example:

Behavioral biometrics can help assess whether the claimant behaves like the genuine user while entering details, navigating the reset flow, or responding to prompts.

Fallback:

- OTP to registered channel
- Email + mobile verification
- Static biometrics match
- Assisted verification through contact center or branch

This use case is valuable because recovery is often a weak point in authentication architecture.

D. Profile changes and sensitive maintenance

Changes such as updating mobile number, email, address, device, communication preferences, or notification settings may not look like payment fraud at first, but they are often part of fraud preparation.

Example:

Behavioral biometrics can identify suspicious behavior during:

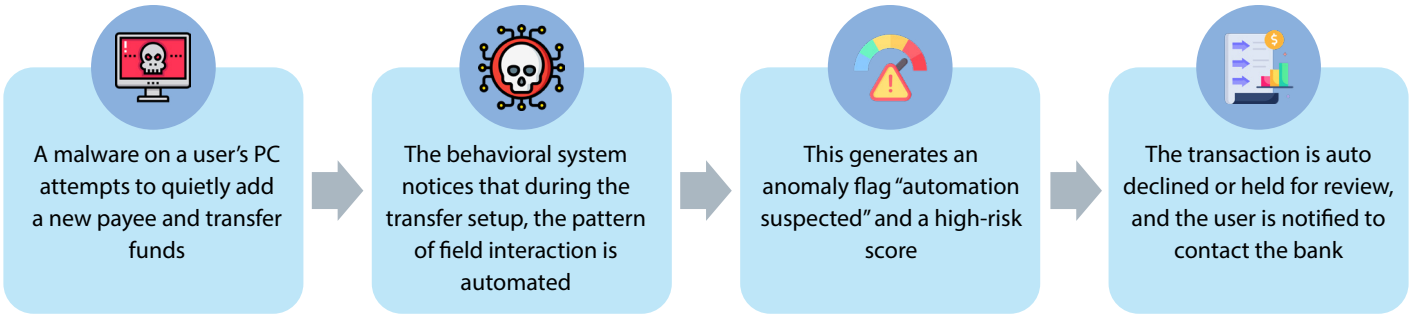
- Changing registered contact details
- Disabling alerts
- Updating device trust settings
- Modifying transaction limits

Fallback:

- Re-authentication
- OTP to old registered contact before change is finalized
- App push confirmation
- Temporary hold until review

This protects against fraudsters who first change profile settings and then attack later.

2. Bot Prevention Workflow



Behavioral biometrics is particularly useful where traditional authentication succeeds but the session is not user driven.

Examples:

- Bot-driven credential stuffing that passes some controls
- Scripted onboarding attempts
- Remote access scam where a fraudster is guiding the customer
- Session manipulation by malware or overlays

Fallback:

- CAPTCHA or device challenge for low-confidence bot suspicion
- Step-up authentication
- Session termination for strong evidence
- Assisted support path for genuine users wrongly challenged

User journey that can be secured using bot detection workflow -

Digital Onboarding/ account opening

During onboarding, there may be no historical behavior profiles yet, but behavioral biometrics can still help detect suspicious interaction patterns such as automation, synthetic identity behavior, form-filling anomalies, or mule-account creation attempts.

Fallback:

- Document verification
- Liveness/selfie check
- Additional KYC verification
- Manual Review

This is more of a fraud-screening use case than a pure returning-user authentication use case.

3. Genuine User with Quirky Behavior

Consider a legitimate user has an unusual habit of using the numpad for typing PINs quickly, which might look slightly anomalous compared to peers. However, over time the system has learned this user's pattern, so it scores it as low risk for them (personalized baseline). No false alarm is raised, demonstrating the benefit of user-specific profiling in real time.

4. User and Entity Behavior Analytics (UEBA)

It is an advancement to behavior analytics. While behavioral analytics is focused solely on the users, UEBA widens the security perimeter to monitor the activities of both the users and entities (e.g., hardware devices, IoT devices, machines, routers, servers, applications, storage repositories, hosts, IP addresses, endpoints, cloud services, etc.) connected in a firm's IT network. The solution then compares the actual activities of the users and entities to their baseline behavioral profile. In case it detects unusual behavior, it undertakes immediate remedial next steps.

Exploratory Use Cases

Behavioral biometrics simplify authentication for persons with disabilities (PWD) in digital banking by reducing reliance on traditional methods like passwords or OTPs.

Key Benefits:

- **Reduced Cognitive Load:** Continuous authentication eliminates the need to remember complex credentials, aiding users with memory or cognitive challenges.
- **Motor Accessibility:** Authenticates based on natural gestures (swipes, taps), removing the need for precise typing or CAPTCHA entry.
- **Support for Visual Impairments:** Works in the background, allowing screen reader users to navigate without interruptions.
- **Inclusive Multi-Factor Authentication:** Complements voice or facial recognition, adding layered security without extra complexity.

Live Implementations

Banks across the world are exploring behavioral biometrics as an enhancement layer to bolster their digital security ecosystem. A few notable implementations from globally leading players are as below:

Live Implementations					
HSBC	LLOYDS BANK	BBVA	nab	Commonwealth Bank	RBS
Fraud prevention during onboarding and session monitoring using Featurespace ARIC platform.[10]	Authentication enhancement and fraud detection using Callsign behavioral analytics.[11]	Impersonation fraud detection and login security enhancement via TypingDNA and neoEYED.[12]	Continuous behavioral monitoring for fraud detection across banking apps using BioCatch.[13]	Integrated behavioral biometrics into authentication to prevent real-time fraud.[14]	Anomaly detection in online session behavior to block unauthorized transactions.[15]

Banks that have implemented behavioral biometrics have realised clear, tangible value across fraud reduction, customer experience and operational efficiency. Live deployments at institutions such as Lloyds, HSBC, BBVA and NAB show material reductions in scams, account takeover and impersonation fraud, with some banks blocking thousands of attacks annually through realtime behavioural analysis. By continuously monitoring how customers interact with devices—keystrokes, navigation patterns and device handling—banks are able to detect social engineering and remote access attacks earlier in the transaction lifecycle. Importantly, this is getting achieved with minimal customer friction, improving trust, login success rates and digital engagement while strengthening compliance and risk outcomes.

Implementation Roadmap & How Infosys can help

Successful adoption of behavioral biometrics typically unfolds through a multi phased, cross functional roadmap. This includes defining a clear strategy and scope aligned to priority fraud risks and customer journeys, assessing organizational and technology readiness, selecting the right solution partners, designing and building the capability, and continuously training and refining behavioral models. Each phase introduces its own considerations, requiring close collaboration across business, technology, risk, data science, and compliance teams.

While banks are well positioned to articulate their strategic objectives, translating intent into a focused, execution ready scope often involves nuanced decisions around where behavioral signals deliver the highest impact. Readiness assessments may highlight opportunities to strengthen data capture, telemetry consistency, authentication flows, or fraud operations processes to fully support behavioral insights. Vendor selection also requires thoughtful evaluation in a fast evolving market, balancing accuracy, latency, privacy, explainability, regulatory alignment, and ease of integration. The design and build phase can be particularly demanding, as behavioral intelligence must be embedded seamlessly into existing digital channels, identity platforms, real time decision engines, and case management workflows. Over time, sustaining value depends on robust model training, monitoring, and governance to manage drift, bias, and regulatory expectations around transparency and data protection.

Infosys recommended Approach

Infosys Value Adds & Accelerators

Strategic Advisory and Roadmap Development

We help define a clear adoption strategy aligned with regulatory requirements, customer experience goals, and fraud prevention objectives. This includes readiness assessments, cost-benefit analysis, and phased implementation planning.

Technology Selection and Integration

Infosys Consulting evaluates leading behavioral biometrics platforms and ensures they integrate smoothly with your core banking systems, mobile apps, and fraud engines. Our API-driven architecture approach enables rapid deployment without disrupting existing workflows.

AI and ML Model Optimization

We design and calibrate machine learning models for behavioral biometrics, leveraging population-level and user-specific profiles. Our teams implement continuous learning frameworks to adapt to evolving fraud patterns and minimize false positives.

Operational Enablement

From SOC integration to fraud analyst training, we enable operational teams to leverage behavioral insights effectively. Our managed services provide ongoing model tuning and performance optimization.

By combining domain expertise with advanced technology capabilities, Infosys Consulting helps banks build a secure, frictionless, and future-ready authentication ecosystem powered by behavioral biometrics.

Compliance and Governance

Infosys Consulting ensures GDPR, PSD2, and local regulatory compliance through robust data privacy frameworks, consent management, and ethical AI governance. We also establish monitoring and reporting mechanisms for transparency and audit readiness.

An experienced transformation partner like Infosys brings deep strengths in digital transformation, cybersecurity, advanced analytics, and financial services to support banks across the end-to-end behavioral biometrics journey. We work alongside bank teams to shape strategy, conduct readiness assessments, guide vendor evaluation, and design scalable, future ready solutions. By orchestrating the full lifecycle—from implementation to continuous optimization—Infosys helps banks accelerate time to value, reduce execution risk, and embed behavioral biometrics as a sustainable pillar of their fraud prevention and risk management architecture.

Final Thoughts

Behavioral biometrics is redefining modern digital-banking security by adding a powerful, invisible layer of protection that operates continuously in the background. As fraudsters adopt increasingly sophisticated techniques—ranging from social engineering and authorized push-payment scams to bots and deepfakes—traditional, point-in-time authentication methods are no longer sufficient on their own. Behavioral biometrics addresses this gap by analyzing natural interaction patterns to distinguish genuine users from impostors, enabling banks to detect anomalies early, reduce friction, and protect customers across channels without disrupting the experience. It complements existing controls, strengthens adaptive authentication, counters automated attacks, improves inclusivity, and materially reduces account takeover and scam-related losses.

Looking ahead, the value of behavioral biometrics is expected to increase through controlled, consent-driven data sharing across institutions using open APIs. Aggregated and anonymized behavioral signals across banks and ecosystem partners can expand training datasets, improve accuracy, and support industrywide defense against coordinated fraud and synthetic identities. In parallel, regulatory frameworks are likely to evolve to govern ethical, transparent, and secure use of behavioral data, with emphasis on customer consent, explainability, bias mitigation, and strong data protection standards.

Realizing this potential requires more than technology—it demands strategic clarity, crossfunctional alignment, and continuous model evolution, often best accelerated through an experienced implementation partner.

About the Authors

Shreyas Tripathi
Consultant, FSI, Infosys Consulting | shreyas.tripathi@infosys.com

Shreyas has over 5 years of experience in Banking and IT consulting sector. His experience spans digital banking customer journeys and credit card transaction processing, partnering with business and technology teams to translate requirements into executable solutions. He has worked with diverse banking clients to translate business objectives into deliverable payment solutions across channels and operating models.

Onkar Sovani
Principal, FSI, Infosys Consulting | onkarjayant.sovani@infosys.com

Onkar has over 15 years of experience in Banking and IT Consulting sector. Working at cross-section of Business & Technology, Onkar has helped his clients by managing end-to-end large-scale transformations & implementing technology solutions which are critical for optimizing & modernizing various banking functions and delivering tangible business value.

Anurag Arora
Senior Principal, FSI, Infosys Consulting | anurag_arora01@infosys.com

Anurag is a digital transformation leader in Banking and Payments. He has extensive experience of providing business consulting and advisory services to financial services firms. He is passionate about driving strategic growth and innovation for clients, particularly through business blueprinting and roadmap, AI-first advisory, new product development, and process transformation.

References

1. McDaniel, D. (2024, September 26). Verizon 2023 DBIR: Credential leaks continue to be a major issue. GitGuardian Blog - Take Control of Your Secrets Security. https://blog.gitguardian.com/verizon-2023-dbir-credential-leaks
2. Security Magazine. 51% of users admit to resetting forgotten passwords once a month. securitymagazine.com. https://www.securitymagazine.com/articles/99116-51-of-users-admit-to-resetting-forgotten-passwords-once-a-month
3. Bandara, P. (2024, February 12). Deepfake 'Face swap' attacks surged by 704% in 2023. PetaPixel. https://petapixel.com/2024/02/12/deepfake-face-swap-attacks-surged-by-704-in-2023/
4. Meehan, A. (2022, July 11). Online payment fraud to top $343bn over next five years. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/online-payment-fraud-five-years/
5. Behavioral biometrics: Frictionless security in the fight against fraud. (n.d.). OneSpan. https://www.onespan.com/sites/default/files/2019-08/OneSpan-Whitepaper-LT-Behavioral-Biometrics.pdf
6. Oduri, S. (2024). Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era, 13(7), 11. https://www.ijirset.com/upload/2024/july/140_Continuous.pdf
7. Salomon, S. (2024, December 19). What is Behavioral Biometrics and How Does It Work Against Fraud? feedzai. https://www.feedzai.com/blog/behavioral-biometrics-next-generation-fraud-prevention/
8. White, M. (2025, November 11). Behavioral biometric authentication: Could it replace passwords? Specops. https://specopssoft.com/blog/behavioral-biometrics-authentication-passwords/
9. Ogunwobi, E. (2025). Advancing financial security using behavioral biometrics and AI-driven authentication. International Journal of Research Publication and Reviews, 6(3), 720-727. https://doi.org/10.55248/gengpi.6.0325.1121
10. Touchton, M. (2019, September 3). Featurespace Announces HSBC as the Latest Global Bank Using its ARIC™ Platform to Combat AML and Fraud. https://www.featurespace.com/newsroom/hsbc-selects-featurespace-in-fight-against-money-laundering
11. Finextra. (2019, September 24). Lloyds sets the Rat on fraudsters. Finextra. https://www.finextra.com/newsarticle/34461/lloyds-sets-the-rat-on-fraudsters
12. Typingdna. Case Study: BBVA. https://www.typingdna.com/use-cases/case-study/bbva.html
13. PYMNTS. (2024, June 26). Australian Bank Spots Scams via How Users Hold Their Phones. pymnts.com. https://www.pymnts.com/news/security-and-risk/2024/australian-bank-spots-scams-via-how-users-hold-phones/
14. Commonwealth Bank. (2022, March 1). Building a brighter future for all: CBA CEO. https://www.commbank.com.au/articles/newsroom/2022/03/AICC-keynote-address-CBA-CEO.html
15. PYMNTS. (2018, August 15). What's Behind The Rise Of Behavioral Biometrics? https://www.pymnts.com/fraud-prevention/2018/behavioral-biometrics-uk-banks-authentication-security-privacy/

ABOUT INFOSYS CONSULTING

Infosys Consulting is a next-generation consulting partner that bridges strategy and execution. With an AI-first mindset, deep industry knowledge, and the combined strengths of business and technology consulting, it helps enterprises turn bold vision into tangible outcomes, faster, smarter, and at scale. Infosys Consulting is helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage.

For more information, contact consulting@infosys.com

Infosys® | CONSULTING