GLASSBOX

Preventive Customer Journeys:

Stopping Fraud Before It Starts

Introduction: Balancing Security with Experience

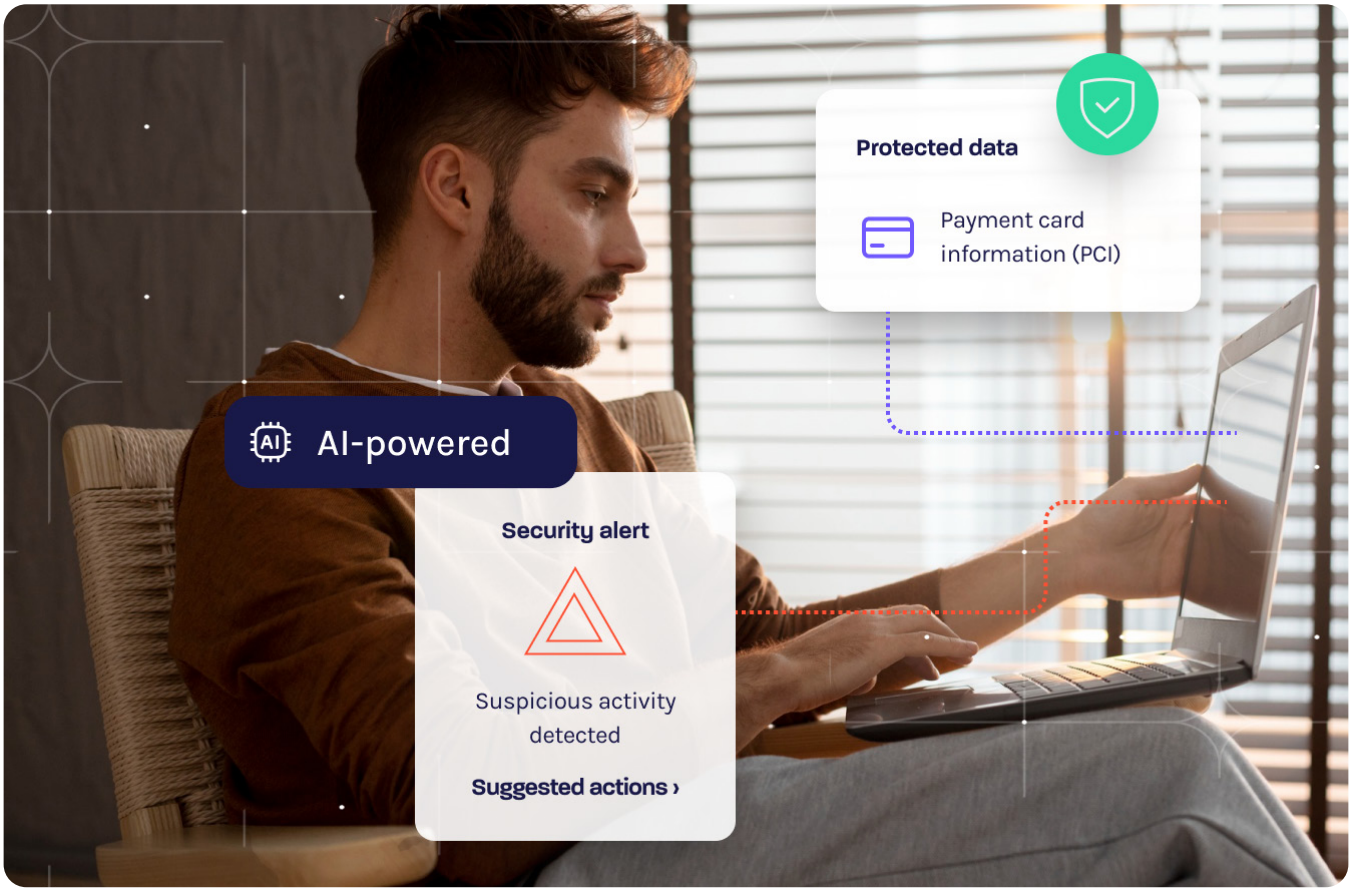
Digital experiences in finance are high stakes—every click, swipe and transaction can either build trust or create risk.

Fraud is rising fast. **Attempted digital payment fraud surged** 43% in 2024, reaching 5.57 attempts per 100,000 transactions.

Yet, security alone can't satisfy customers. They expect speed, simplicity and frictionless interactions—and they leave when those expectations aren't met.

In fact, **91% report being affected by poor digital experiences,** with half switching to competitors.

Preventive customer journeys offer a solution. By detecting and stopping fraud in real time, organizations can safeguard both revenue and customer confidence. Real-time insights, intelligent data strategies and cross-team collaboration intercept threats before they escalate—enabling financial institutions to deliver fast, seamless experiences while staying one step ahead of fraud.



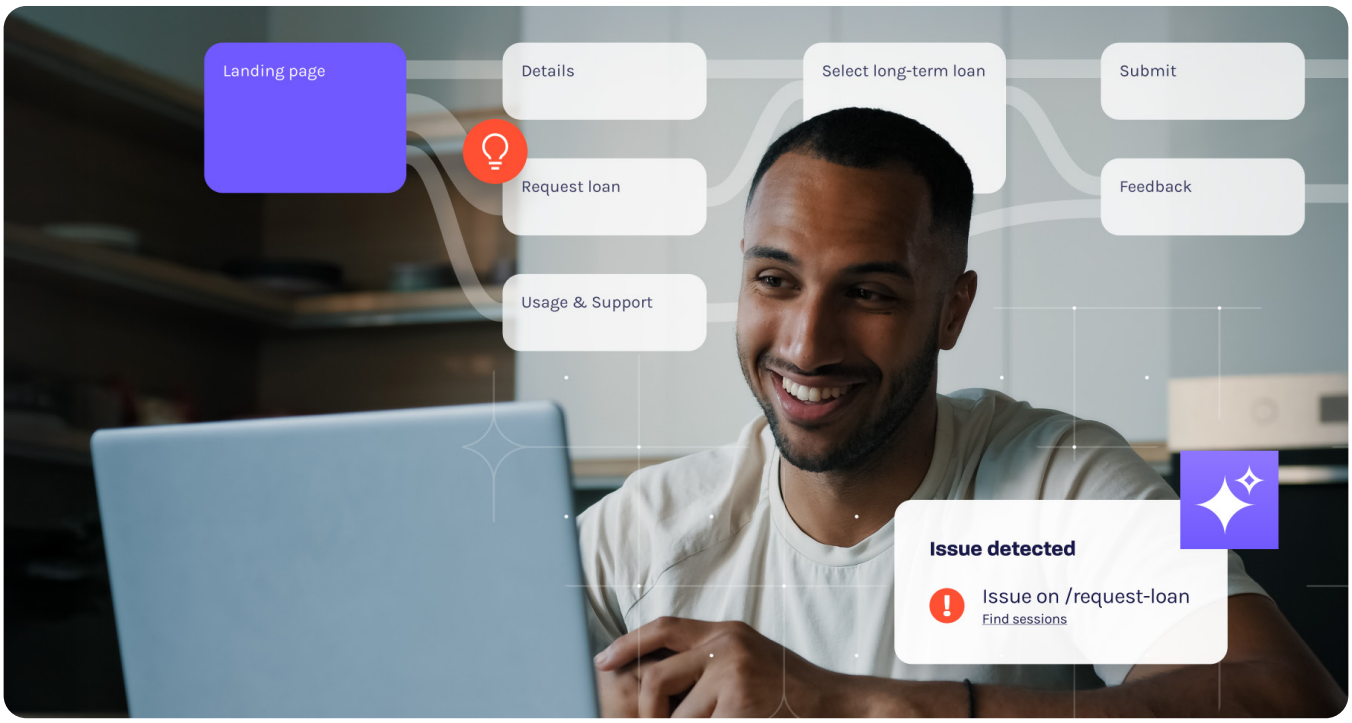
GLASSBOX

What Is a Preventive Customer Journey?

In digital finance, speed is everything. Preventive customer journeys detect suspicious activity in real time so organizations can stop fraud before it escalates. This proactive monitoring protects revenue, reduces operational risk and safeguards reputation—all while keeping CX smooth and uninterrupted.

A preventive approach monitors user interactions continuously, spotting anomalies before transactions are completed. Rather than reacting after an account takeover or fraudulent activity, organizations gain real-time visibility into digital behavior, enabling faster intervention, reducing risk exposure and strengthening overall security without disrupting legitimate customer activity.

This real-time monitoring strengthens the organization's ability to respond to fraud quickly and effectively. By detecting suspicious activity as it occurs, financial institutions reduce operational risk, limit potential losses and protect their reputation. Continuous visibility into digital interactions enables teams to intervene swiftly and discreetly, maintaining control and confidence in their security posture.



GLASSBOX

Recognizing the Signals of Risk

To prevent fraud, organizations monitor user behavior patterns in real time. Risk signals often appear as subtle deviations from typical patterns and may span multiple sessions. For example, a user might navigate illogical page sequences from a high-risk location in one session and attempt fraud later. Early detection allows teams to intervene by suspending or flagging accounts before losses occur.

Key risk indicators include:

- **Unusual page sequences:** Navigating in illogical or non-linear ways.
- **DOM tampering:** Altering page structure or content to bypass security controls or inject malicious code.
- **Multiple logins in one session:** Indicative of credential stuffing or account takeover attempts.
- **Suspicious form activity:** Rage clicks, form zigzags, rapid typing, excessive backspacing or hidden field manipulation.
- **Geographic anomalies:** Logins from unusual or high-risk regions.

Tools such as the Glassbox Insights Assistant (GIA) help teams filter sessions by country or region, spot suspicious patterns and investigate quickly. Continuous capture of every interaction enables real-time detection, empowering swift intervention before fraud escalates.

Data Depth Matters: Why Glassbox Excels

Effective fraud detection depends heavily on the quality and depth of data captured. The more comprehensive the data, the more robust the defense against sophisticated threats. Glassbox records every digital interaction across devices, browsers and platforms, providing visibility into subtle manipulations such as DOM tampering—a type of behavior that other CX platforms cannot currently fully capture.

This extensive data capture enables organizations to uncover hidden risks, enhance fraud detection capabilities and continuously adapt to emerging patterns.

Reviews on **Gartner Peer Insights** underscore this strength: users report that visibility into DOM tampering "has saved us both time and money" and enables them to "identify other patterns which are risky" before they escalate.

By capturing a rich dataset, Glassbox reduces blind spots, empowers smarter prevention strategies and increases overall confidence in fraud detection efforts, making data depth a critical foundation for preventative security.

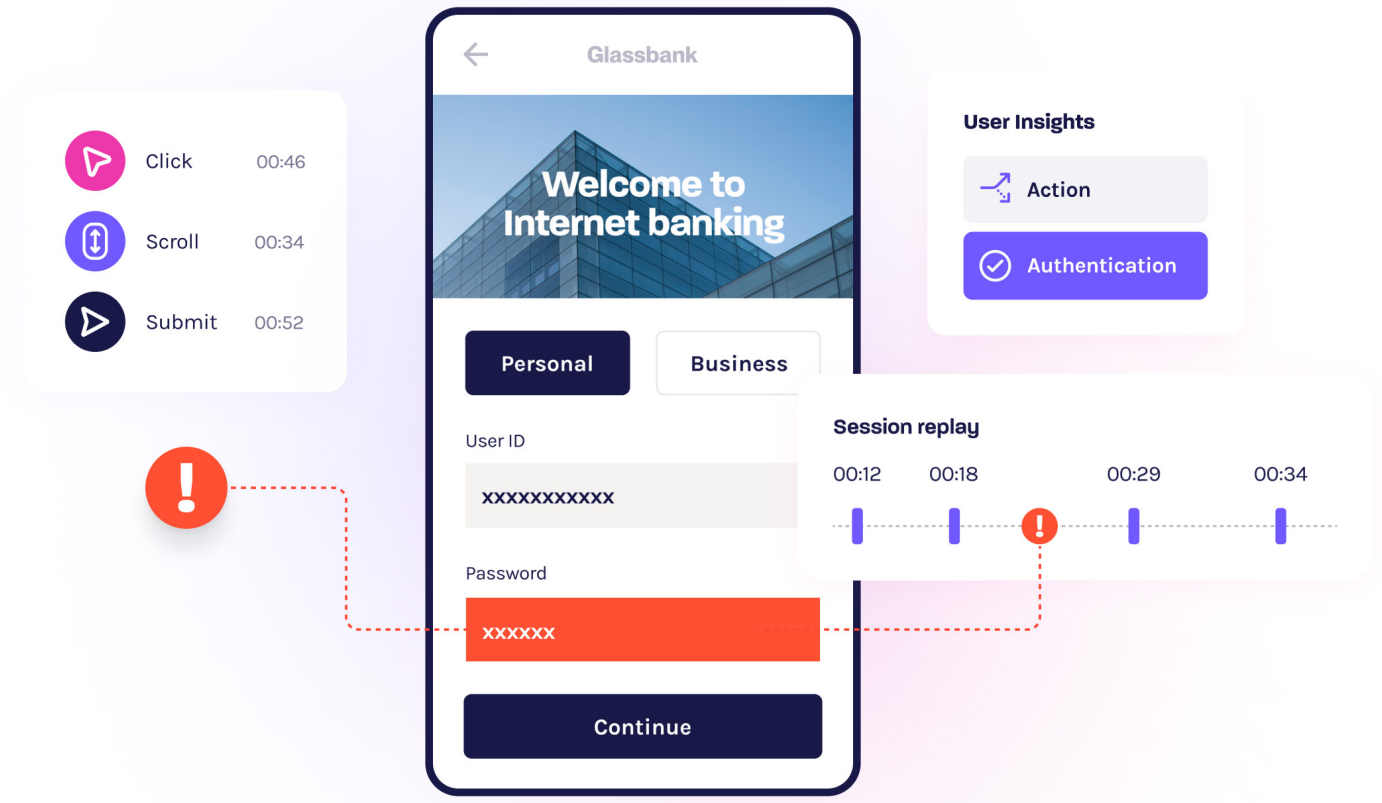
GLASSBOX

Real-Time User Interaction Analysis vs. Traditional Fraud Detection

Traditional fraud detection often depends on static, rule-based systems that react only after suspicious transactions occur, leaving gaps for fast-moving, adaptive fraud schemes. Glassbox offers a more dynamic solution by monitoring real-time user behavior to detect anomalies as they happen. Its core features include AI-powered alerts, live anomaly detection and session replay for clear visual evidence.

A strong example of Glassbox's real-time fraud prevention comes from a **U.S.-based fintech company** that was combating sophisticated abuse of its sign-up bonus program. Fraudsters created multiple usernames, devices and IP addresses to conceal their actions, complicating detection. Glassbox linked these sessions in real time, automatically flagging suspicious behavior. The fraud team quickly investigated through an interface that mapped connections between usernames, IPs and devices.

Session replays provided auditable proof, allowing the company to block fraudulent activity before bonuses were paid, protecting revenue and customer trust. This proactive, behavior-based approach greatly reduced losses and streamlined investigations.



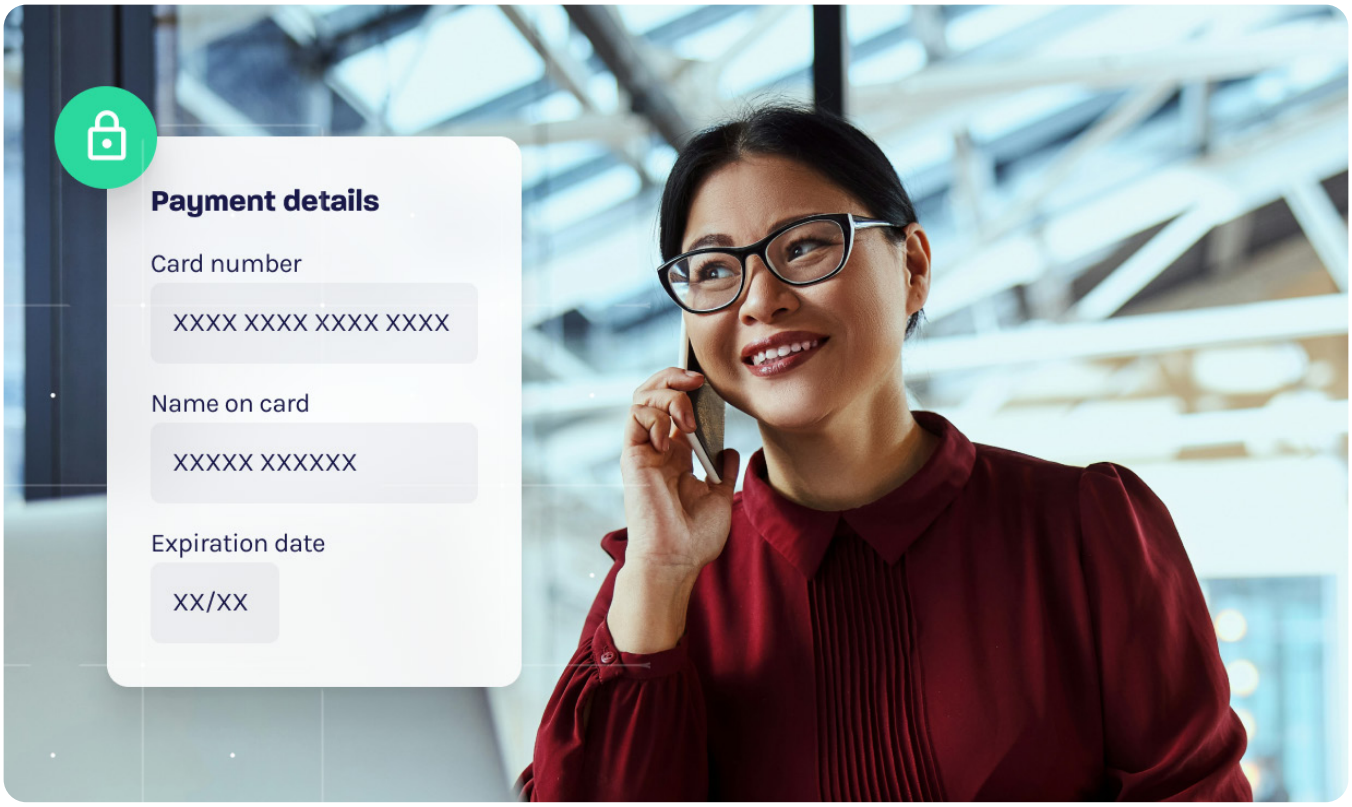
GLASSBOX

The Balancing Act: Security Without Friction

Effective fraud prevention must protect customers without creating unnecessary barriers. Traditional security measures—repeated identity checks, security questions or CAPTCHA challenges—can frustrate users and increase abandonment rates, especially in high-stakes financial apps where smooth experiences are crucial.

Glassbox helps strike the right balance by reducing false positives using precise detection, so legitimate users aren't wrongly flagged. It also identifies where users abandon processes in real time, giving teams insight into friction points.

By continuously analyzing user behavior and adapting security flows based on actual risk, financial institutions can ensure safe transactions proceed smoothly while blocking threats. This approach leads to fewer drop-offs, stronger protection and more loyal, engaged customers. Security is now a competitive advantage.



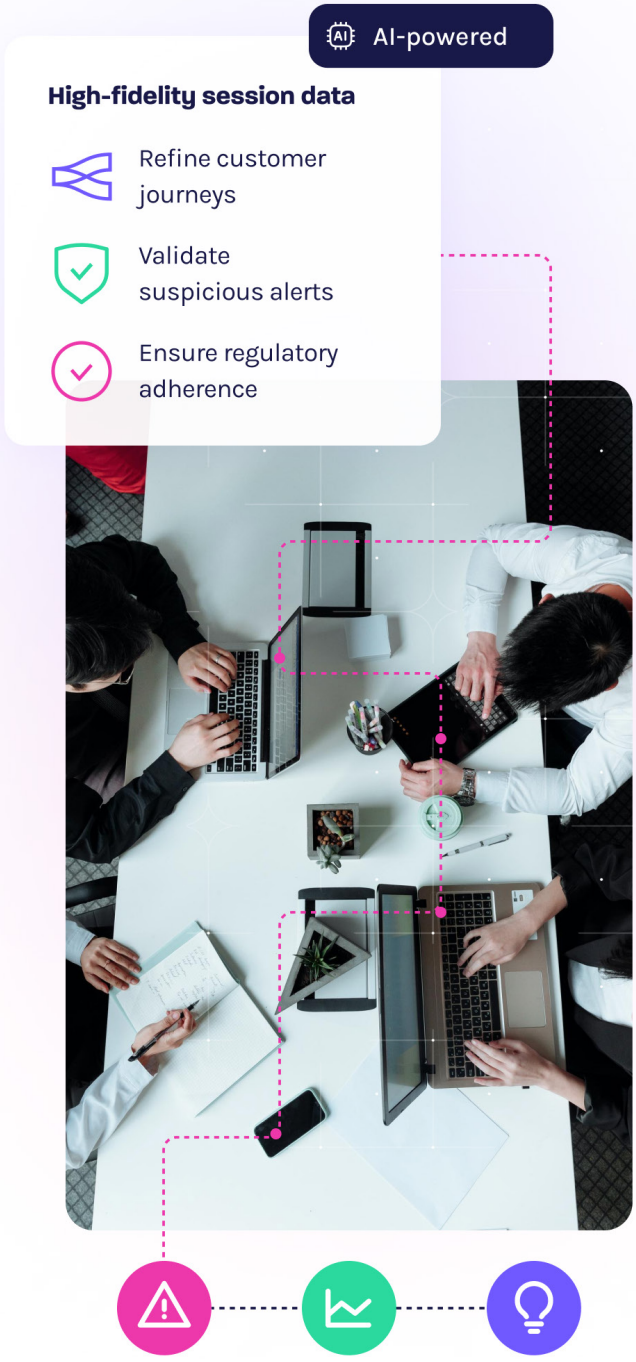
Why Cross-Functional Collaboration Is Essential

Fraud prevention is a collective responsibility that extends beyond the fraud team to include IT, product, compliance, security and operations teams. Breaking down these silos is essential to effectively detect and respond to threats.

Glassbox provides a single source of truth by delivering high-fidelity session data accessible to all relevant departments. This unified visibility fosters faster decision-making, reduces misunderstandings and promotes consistent responses.

For instance, session replays offer valuable insights that enable product teams to refine customer journeys, fraud teams to validate suspicious alerts and compliance teams to ensure regulatory adherence.

When every team can see the same detailed digital interactions, collaboration becomes seamless, enabling organizations to respond swiftly and accurately to fraud risks. This shared understanding not only enhances operational efficiency but also increases protection and reinforces customer trust.



Getting Started and Avoiding Pitfalls

Effective preventive customer journeys require a strong foundation across your organization. By aligning fraud, compliance and product teams, you build the cross-functional collaboration needed to detect risks early and act decisively.

Capturing complete digital interaction data is crucial for spotting subtle fraud signals before they escalate. Glassbox's advanced reporting tools reveal suspicious behaviors, including DOM tampering, rage clicks and form zigzags, giving organizations clear, actionable insights to identify and stop fraud faster.

With Glassbox's GIA, teams can quickly summarize session data and surface common patterns, enabling analysts to spot trends and investigate suspicious behavior more efficiently.

By integrating fraud detection throughout the digital journey, organizations can identify and stop suspicious activity before it escalates. This continuous oversight strengthens control, reduces losses and builds trust.

Discover how Glassbox can help you build truly preventive customer journeys that stop fraud before it starts.

GLASSBOX

glassbox.com | info@glassbox.com