CELEBRUS PLAYBOOK

The Future of Fraud Prevention

Real-Time Identity, AI, and the Power of First-Party Data

celebrus®

Table of Contents

Introduction

Fraudsters are getting faster – and smarter. Now, AI is supercharging their efforts, making attacks more sophisticated and harder to detect than ever.

AI allows fraudsters to mimic human behavior with near-perfect precision, rendering many traditional fraud tools obsolete. Relying on delayed data, outdated models, or reactive systems that act only after damage is done is no longer enough. The question is: **what are you doing about it?**

Effective fraud prevention starts with first-party data and the ability to run AI models in real time. By leveraging high-quality, millisecond-level data, organizations can build comprehensive evidence profiles, enable instant decision-making, and power predictive models for proactive, preemptive intervention.

Fraud is constantly evolving, and fraudsters never stop innovating. Winning this arms race requires one thing above all: **granular, timely, actionable data**. When harnessed effectively, data allows organizations to spot emerging threats before they escalate – protecting customers and safeguarding the bottom line. Prevention has to happen before login, not after a loss.

Say goodbye to:

- Incomplete customer journeys
- Slower fraud responses
- Lower personalization accuracy
- Erosion of trust

Reactive = Risky: Shift from Detection to Prevention

Many organizations are engaged in **fraud management** rather than true **fraud prevention**, accepting an "acceptable" fraud limit to avoid disrupting the customer journey. They face tremendous data limitations with a focus on single, completed transactions and historical patterns, ignoring the behaviors detected around each transaction.

Reactive systems flag fraud only after a transaction is completed. That means you're analyzing losses instead of preventing them. Most traditional fraud tools:

- Depend on delayed or incomplete data
- Focus on single transactions, not behavior
- Operate on one channel or device at a time
- Create high false positives that frustrate real customers

2025 requires **real-time identity data** that detects risk in milliseconds. The modern defense shifts the focus from managing fraud after it occurs to **real-time prevention**. By connecting real-time behavioral and identity data, organizations can act in *milliseconds* to block emerging threats.

By preventing fraud early, you:

- Reduce chargebacks and financial loss
- Improve customer satisfaction and loyalty
- Strengthen brand trust with ethical, compliant data practices

The Power of Digital Identity: How First-Party Data Protects Your Customers and Your Reputation

If your customer data lives in someone else's system, you're not in control, you're at risk. **First-party data is the foundation of modern fraud prevention**. It is data that is captured and processed within a company's four walls, meaning the data is known and owned by the company. Owning your data is the ultimate defense against fraud, churn, and chaos.

Rising fraud, stricter privacy laws, and closed-box CDPs have one thing in common: They all limit your visibility into the truth about your customers. This requires moving beyond siloed, third-party "closed-box" systems that offer limited context and visibility.

Closed-box = Closed eyes

When data leaves your four walls, you lose: Context, Control, Confidence

When fraud, marketing, and compliance teams share a single, trusted data source, customers stay protected, operations move faster, and decisions are based on facts, not scores. When customer data is trapped in closed-box CDPs or delayed by batch processing, you lose the context needed to act in real time.

That loss of visibility leads to:

- **Siloed View:** Traditional solutions often operate in closed-box environments, where systems and data processors are outside the company's digital perimeter, leaving organizations with limited visibility and a lack of clarity into their own data.
- **Lack of Context:** Closed-box systems typically "spit out a score" for a single use case, providing no context or explainability, which leads to numerous false positives.
- **Privacy & Compliance Risk:** Relying on third-party data is complicated by tightening global privacy regulations that prohibit the transfer of Personally Identifiable Information (PII), limiting the utility of external data sources.

To protect both customers and brand reputation, you need data that's immediate, transparent, and fully yours. High-quality, structured data is the foundation for any analytics or predictive model — without it, even the most sophisticated systems can only react after the fact. In a world of fragmented data, privacy laws, and rising fraud, visibility is everything.

The Engine of Prevention: Identity Graphs and Behavioral Biometrics

Effective fraud prevention is powered by two critical capabilities: robust identity graphs and advanced behavioral biometrics.

Robust Identity Graphs

A first-party ID graph captures and connects a user's many digital identifiers across all owned digital properties.

- **360-Degree View:** Captures and persists data for all interactions – for both known and unknown visitors – building a complete view of every individual across domains, channels, devices, and sessions.
- **Contextual Insight:** Persisting profiles over time builds deeper context and continuously layers data to construct an identity and identify behavioral patterns. This merged evidence enables better, quicker, and more informed decisions.

Behavioral Biometrics and Analytics

Behavioral analytics and biometrics are essential for swift prevention, as they monitor every single digital interaction at an individual level. This is used to map an individual's unique profile and determine whether each visit is legitimate. Key behavioral data captured includes:

- **Keystroke Dynamics:** Typing speed, patterns, and corrections (e.g., in name, income, or address fields).
- **Mouse Movements/Touch Gestures:** Hesitations, erratic movements, and abnormal interaction styles.
- **Navigation Habits**: Detecting unnatural browsing flows, such as jumping directly to key sections.

How Anomalies Detect Fraud

By comparing real-time behavior to a user's established profile in the moment, the system can instantly flag anomalies that signal fraudulent intent:

Fraud Type	Key Indicator (Example)	Genuine User (Baseline)
First-Party	Frequent, repeated edits to sensitive fields (e.g., income, address) during an application.	Quickly and confidently entering known details.
Third-Party	Unnatural typing patterns or rapid, repetitive actions consistent with a bot or script.	Typing rhythm and interaction styles remain stable over time.
Account Takeover (ATO)	Login from a new device, a proxy server, or inconsistent geolocation	Device usage and geolocation align with known patterns.

Enter Celebrus: First-Party Data, Millisecond Decisions, Maximum Protection

Celebrus captures and unifies every digital interaction directly from your own environment – tag-free and in milliseconds. We deliver instant, evidence-based identity verification that spans every session, device, and channel – **pre and post authentication**. The goal isn't to stop one transaction; it's to understand the entire customer journey.

The new standard:

1. Capture behavioral and contextual data on the first interaction.
2. Assess fraud risk instantly, before the first page loads.
3. Intervene seamlessly, without disrupting legitimate users before the loss occurs.
4. Personalize user action to reduce friction for legitimate customers.
5. Continuously learn and evolve to detect new threats.

Celebrus builds **evidence-based digital identities** that persist across sessions, devices, browsers, and channels. Because all captured data is high-quality, structured, and compliant, these rich identity profiles fuel machine learning that continuously adapts in real time, detecting anomalies the moment they happen while providing accurate, transparent, and actionable insights. Celebrus patented digital identity technology provides:

Real-Time Alerts and Actionable Insights: Assigns a risk score to each session and provides immediate alerts and a detailed audit trail for high-risk behaviors, enabling instant intervention.

Full-Journey Evidence Profiles: Collects a comprehensive, chronological record of user activity for both known and anonymous users, including behavioral and biometric insights, capturing every click, keystroke, and behavioral signal.

Contextual Machine Learning: Models are trained to detect specific fraud typologies by building detailed profiles and flagging anomalies like unusual transaction disputes or excessive refunds. Because these models are fed high-quality, structured data, AI continuously learns and adapts in real time.

Ownership and Control: Celebrus is designed for transparency, security, ownership, and scale, ensuring your fraud solution is future-proof and compliant.

Seamless Integration: Integrates with existing fraud prevention platforms, CRM tools, and risk management solutions to enhance workflows and support collaboration across teams.

Your 4-Step Playbook

To shift from reactive management to proactive prevention, enterprises should adopt a unified strategy centered on digital identity resolution.

01

Capture and Build Comprehensive Profiles

This step focuses on capturing a user's entire digital journey to build a complete profile, starting from the very first anonymous visit.

- **Action:** Capture **behavioral biometrics** from the initial anonymous visit.
- **Data Integration:** Merge this data with existing customer data over time to build comprehensive **customer evidence profiles.**
- **Resolution:** Employ **digital identity resolution** to connect all interactions across channels, devices, sessions, and time to a single 360-degree view.

02 Assess Risk in Real Time

Leverage robust data models and AI-powered machine learning to analyze the profile and transaction in milliseconds.

- **Action:** Instantly deploy **machine learning** to assess each transaction's risk of fraud.
- **Detection:** Identify anomalies in user behavior by connecting the full customer view with technologies like **behavioral biometrics and link analysis**.

03 Determine Intervention

Based on the real-time risk assessment, determine if an action is required to stop the fraud before it completes.

- **Action:** Intervene in **real time** to stop a potentially fraudulent transaction.
- **Mule Accounts:** The robust data model allows for identifying **known mule accounts** and tracing them to other connected accounts and profiles.

04 Deliver a Personalized Action

The final step is to keep the majority of interactions low friction for legitimate customers, intervening only where necessary.

- **Action:** Deliver a personalized message or other action to the user to prevent the fraud before it happens.
- **Soft Disruption:** This could be a "soft and personalized buyer journey disruption," such as "holding" an account while checking a flag, allowing a legitimate customer to proceed while protecting the organization.

Driving Results: From Risk to ROI

Owning and securing your data isn't just about compliance – it's about performance. When your data is unified, secure, and real-time, your business wins, too.

With Celebrus, brands see measurable gains and speed to value. Customers see an average response time of 100ms and an average time to value of a few weeks.

- Reduced chargebacks and fraud losses
- Higher engagement through trusted personalization
- Stronger customer retention and lifetime value

Organizations using Celebrus have achieved:

- **20%+ improvement** in fraud detection accuracy
- **30% fewer false positives** in the first year
- Millisecond-data delivery before the first page loads for faster interventions

By building a digital identity and first-party data approach, your organization can effectively outfox fraudsters by preventing fraud before it causes harm. Because in fraud prevention, milliseconds matter – and Celebrus delivers them.

celebrus®

Stop reacting. Start preventing.

Mitigate threats in real time, protect every customer interaction, and safeguard your brand's reputation with Celebrus.

Book your demo

 Copyright © Celebrus Technologies plc