How to Leverage Digital Identity Data to Outfox Fraudsters

celebrus

Introduction

Traditional tactics are falling short

Fraudsters never rest on their laurels. They constantly adapt their methodologies alongside evolving technologies, with myriad vectors of attack becoming increasingly sophisticated and difficult to detect. And no industry is immune.

Unfortunately, most fraud solutions operate on a reactive rather than preventative or proactive basis, not having the sophisticated capability to activate all transaction and digital data. So, the focus is on completed single transactions and historical transaction patterns as the data sources. These solutions ignore behaviors detected around each transaction, instead relying on decisioning rules that are rigid and difficult to adapt.

Fraud teams are overrun trying to keep up with a myriad of fraud use cases and evolving vectors of attack. Incorrectly labeling a user or an activity as fraudulent when it isn't, requires manual review to assess, confirm, and work through the issue—draining already limited resources. A platform that lowers false positives enables fraud teams to focus on what really matters: preventing actual fraud.

Why closed box systems aren't enough

Fraud is not limited to a single environment. Fraudsters will often deploy different fraud types and tactics simultaneously as part of a larger fraud attack. Scams are a perfect example of the crossover between fraud types as they're regularly used to gather information that enables account takeover (ATO), identity theft, creation of false identities, and unauthorized push payments. And yet, many organizations are operating in a siloed, closed box environment and depending on third-party data to inform their business decisions and fraud strategies.

A closed box environment is when an organization's systems and data processors live and operate outside of the company's digital four walls. Because these types of environments will typically take in data and spit out a score for a single use case, companies are faced with limited visibility and a lack of clarity when it comes to their data.

Global tightening of privacy regulations means that any data that could be at risk and is transferred by a third party must be encrypted to protect that data, and that the transfer of personally identifiable information (PII), particularly in financial service and healthcare industries, is prohibited. By using third-party data and operating in a closed box environment, companies are limiting themselves and their data.

Doing so means they don't have access to their actual data, let alone any data captured in real time. Taking it a step further, most fraud technologies focus on one use case at a time, but fraud isn't singular—while companies might successfully deter one type of fraud, not inherently solving for a wide variety of use cases in the moment, means fraud is still getting past defenses.

By not being able to see or interpret their data, companies are stuck with a score that provides no context, explainability, or shareable intel into the captured and processed data. Such simplistic scoring can result in numerous false positives due to lack of context, resulting in a negative customer experience for the good customers incorrectly flagged due to ineffective data capture.

With first-party data, all the data captured for every digital identity is housed and processed within a company's four walls, so the data is known—and owned—by the company. This enables better accuracy, insights, attribution, and optimization of the data for fraud detection, while ensuring compliance with privacy regulations.

The power of focusing on prevention

Many organizations typically engage in "fraud management" rather than fraud prevention by setting an "acceptable" fraud limit to avoid disrupting the customer journey. This approach can ultimately lead to fraudulent transactions getting through before they're recognized as fraud, resulting in significant financial and reputational losses.

As part of their fraud strategy, enterprises must take steps to prevent fraud and protect themselves and their consumers. However, traditional solutions are designed to identify fraud after it's already happened—when it's too late to do anything about it. The key to reducing losses and protecting consumers is strong identity verification and authentication processes that help prevent fraud before it happens, rather than forcing fraud teams to chase after it. A digital identity and first-party data approach is essential.

4 Steps to Effective Fraud Prevention

01 Capture behavioral biometrics from the very first anonymous visit and merge it with existing customer data over time to build comprehensive customer evidence profiles

02 Instantly deploy machine learning to assess each transaction's risk of fraud

03 Determine if intervention is required in real time to stop a potential fraudulent transaction

04 Deliver a personalized message or other action to the user behind the transaction to prevent the fraud before it happens

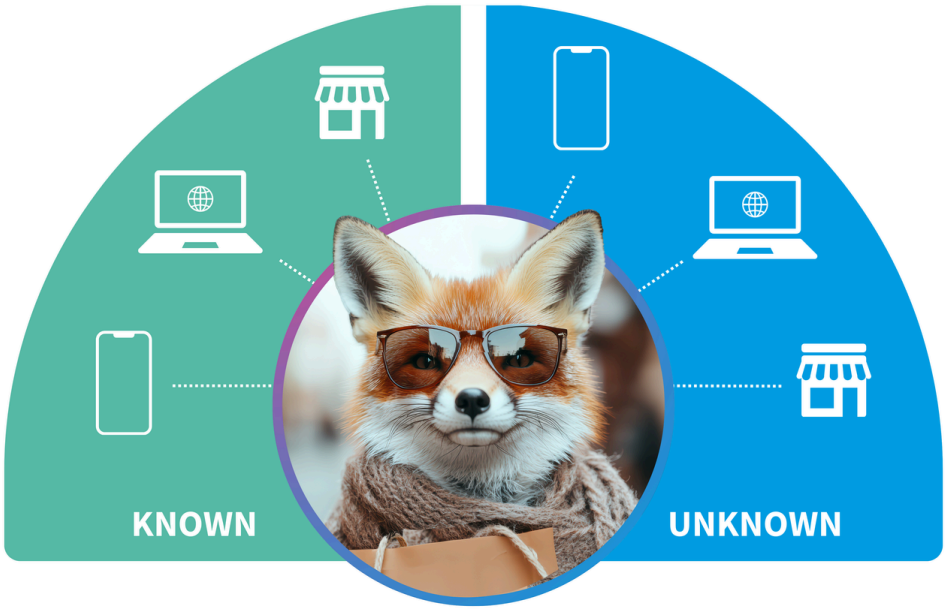
What Your Fraud Prevention is Missing

High-quality, actionable data

High-quality data is one of the most important aspects of effective fraud prevention, as many organizations struggle with fragmented, unstructured, inaccurate, and incomplete data sets, which can severely hinder their ability to detect and prevent fraud. Real first-party data is particularly critical in this context.

A user's journey is not linear. People (including fraudsters) will often visit a website more than once, use their computer one day and their phone weeks later, use different browsers, and/or at times be logged in and other times not. The key here is to have technology in place that can not only capture all of that user behavior instantly and across sessions, devices, channels, browsers, domains, and more, but can also assign that behavior to a digital identity and persist that identity over time to create a 360-degree view of every visitor. First-party data helps companies better know their customers—enabling a more accurate and detailed understanding of user behavior and identity to prevent fraudulent activities before they cause significant harm.

To effectively combat fraud—and more specifically prevent it—organizations across industries need a comprehensive solution that detects all types of fraud in the moment and builds comprehensive identity graphs that increase the ability to identify emerging threats and prevent all types of fraud. Capturing and consolidating data across session, device, domain, and over time, multiplies the power of a fraud solution and reduces false positives.



Digital identity resolution across channel, platform, and device connects:

PII	Journey data	Interactions
Behaviors	Preferences	Multiple identifiers

Robust identity graphs and data models

Every individual has several digital identifiers across channels and devices. A first-party ID graph captures and connects these identifiers to build and persist identity across all owned digital properties. When done correctly, an identity graph can capture and persist not just first-party identifiers, but second- and third-party ones as well.

This data is captured for all interactions, building a complete view of every individual across domains, channels, devices, sessions, and over time, for both known and unknown visitors. Capturing and persisting profiles over time builds deeper context and continually layers data to progressively build an identity and identify behavioral patterns.

These types of insights are then connected to decisioning systems within milliseconds to detect anomalies in user behavior. This is important because by merging the evidence into a single profile about a consumer, brands can make better, quicker, and more informed decisions.

Better data means better results. By connecting a full customer view with all data points within a protected environment, organizations can maximize the efficiency of technologies like behavioral biometrics, machine learning (ML), and link analysis, to not only instantly detect and prevent fraud by monitoring user anomalies, but to identify known mule accounts and trace them to other connected accounts and profiles.

With a robust data model that is at the core of everything we do, Celebrus digital identity verification and profiling capabilities across sessions, channels, and devices provide the best standard for digital evidence. This comprehensive view of consumer behavior equips organizations to detect and address potential fraud with precision, enhancing decision-making and operational efficiency.

By capturing and persisting digital identities, real first-party data enables companies to build comprehensive evidence profiles for every user—helping to monitor for issues and anomalies out of the box and without having to rely on scoring or lackluster data as the only indicator. With Celebrus, companies can act decisively and mitigate threats before they escalate.

Evolved fraud detection to stay ahead

Behavioral analytics and biometrics are essential: both enable swift fraud prevention by monitoring every single digital interaction at an individual level. This applies to all visits, sessions, devices, etc.—not just ones that have been identified as fraudulent. This data is used to map the individual and create a profile, making it possible to identify whether each visit is from a legitimate user or not.

The captured digital identity data is also used for pattern analysis to look for similar patterns with other users. For example, when a user is attempting to open a new account, behavioral signals provide insight into the validity of the attempt. A legitimate user knows their password and quickly answers verification questions, while a fraudster may paste information or hesitate when entering responses. Likewise, a new customer will likely take a bit longer to navigate a new account setup process, while a cybercriminal will be very familiar with the process and move through it relatively quickly.

With this insight, businesses can do a soft and personalized buyer journey disruption—focusing on detection and prevention—by "holding" accounts with similar buying patterns while checking flagged accounts. This provides a low-friction experience for legitimate customers, allowing them to complete the action while still protecting the organization. If the flagged accounts confirm fraud, all of them can be shut down. Layering behavioral biometrics and pattern analysis on top of robust identity profiles and PII ensures fraud prevention is happening right away, rather than detection after the fact.

Outfoxing Fraudsters with Celebrus

Customers that deploy Celebrus typically see an initial uplift in identifying fraud by over 20%, while also seeing a significant decrease in false positives as the system builds evidence profiles to the tune of 25-30% in the first year.

Our ability to do this lies within our frictionless data capture and the completeness of that data contextualized in our data model, combined with our machine learning, scorecards, and consumer evidence profiles.

1. **Granular Data Collection:** Celebrus captures every interaction a user has with a website, mobile app, or other digital touchpoints in real time:

- Keystroke Dynamics: Tracks typing speed, patterns, and corrections (e.g., changes to name, income, or address fields).
- Mouse Movements and Touch Gestures: Monitors hesitations, erratic movements, and abnormal interaction styles.
- Form Submissions: Captures and analyzes data inputs to detect unusual or manipulated information.
- Session Metrics: Measures session length, navigation patterns, and time spent on specific fields or pages.

Use Case: A user frequently alters financial details (e.g., income) during loan applications, indicating a potential attempt to manipulate approval criteria.

2. **Behavioral Biometrics:** Celebrus applies behavioral biometrics to build a unique profile of each user based on:

- Typing Rhythm: Analyzing patterns that remain consistent for genuine users but differ for fraudulent ones.
- Navigation Habits: Detecting unnatural browsing flows, such as jumping directly to key sections without typical exploration.
- Device and Environment Analysis: Identifies if a genuine user is on their usual device in their usual environment or if they've switched to suspicious setups (e.g., new devices, VPNs).

Use Case: A legitimate customer rarely changes their home address, but a fraudster trying to exploit their identity alters the address repeatedly during the session.

3. **Identity Validation:** Celebrus integrates with third-party data sources and fraud detection tools to cross-check user-provided information:

- Anomalies in Personal Information: Flags mismatched or implausible details, such as a newly created email address or a high-risk IP location.
- Behavioral Deviations: Identifies changes in interaction style (e.g., slower typing speed) that may indicate falsification of claims or inputs.

Use Case: A customer claiming a fraudulent charge shows interaction patterns consistent with someone who completed the original transaction.

4. **Contextual Machine Learning Models:** Celebrus uses machine learning models trained to detect fraud typologies specific to first-party fraud including:

- Profile Building: Creates detailed customer profiles based on historical behavior.
- Anomaly Detection: Flags behavior deviating from the baseline, such as: unusual transaction disputes, excessive refunds or chargebacks, or frequent use of specific excuses (e.g., "item not received").
- Pattern Recognition: Identifies trends, like repeated fraudulent claims by the same individual across different accounts.

Use Case: A user has a consistent history of dispute claims after high-value purchases, which signals potential refund abuse.

5. **Real-Time Alerts and Actionable Insights:** Celebrus provides actionable insights to businesses in milliseconds:

- Fraud Scoring: Assigns a risk score to each session or interaction based on the likelihood of fraud.
- Immediate Alerts: Sends notifications for high-risk behaviors, enabling businesses to block or investigate further.
- Evidence for Decisions: Provides a detailed audit trail of user behavior, aiding in fraud investigation and regulatory compliance.

Use Case: If a user triggers a high fraud score during an application, the system can halt the process, request additional verification, or escalate for manual review.

In addition, we have a variety of instant interventions that can be enabled on Day 1 to watch for common behaviors that would signal potential fraudulent activity.

First-Party Fraud Key Patterns and Indicators:

- Behavioral Inconsistencies: Includes but not limited to frequent edits to income, employment, or address fields during application forms; hesitation or repeated attempts when filling sensitive fields (e.g., salary details or loan amounts).
- High-Risk Behaviors: Excessive chargebacks or disputes on what we demonstrate as legitimate transactions or requests for refunds or compensation shortly after high-value purchases.
- Unusual Patterns Over Time: Consistent abuse of promotional offers or refunds; high velocity of claims or applications across multiple channels (e.g., online, in-store).

How Celebrus helps customers to detect it:

- Session-Level Analytics: Tracks user behavior during interactions to flag signs of manipulation or dishonesty.
- Historical Comparisons: Cross-references current behavior with the user's historical patterns (e.g., sudden changes in financial details, age, employment details, and many more).
- Anomaly Detection: Identifies behaviors that deviate from genuine user patterns, such as unusually fast or slow typing during form submissions.

Third-Party Fraud Key Patterns and Indicators:

- Device and Network Signals: Use of new or unrecognized devices, proxy servers, or VPNs; inconsistent geolocation (e.g., logins from different countries within a short time frame).
- Behavioral Biometrics: Unnatural typing patterns or navigation behavior inconsistent with human users (e.g., bots).
- Identity Mismatches: Discrepancies in personal details compared to known databases (e.g., SSN, date of birth).
- Rapid and Repetitive Actions: Submitting multiple applications or transactions within seconds or minutes; attempting to brute-force login credentials or exploit vulnerabilities.

How Celebrus helps customers to detect it:

- Behavioral Profiling: Identifies whether a user's interactions match the expected profile of a genuine consumer.
- Device Fingerprinting: Tracks and flags suspicious device usage, such as emulators or multiple accounts on a single device.
- Real-Time Alerts: Detects high-risk behaviors and triggers actions like multi-factor authentication or account lockdown.

Genuine Consumer Behavior Key Patterns and Indicators:

- Consistent Historical Behavior: Typing speeds, browsing habits, and interaction styles remain stable over time; device usage and geolocation align with the customer's known patterns.
- Natural Navigation: Exploration of content, natural pauses between actions, and predictable browsing flows.
- No Red Flags in Verification: Personal information matches trusted databases, and no anomalies are detected during application or transaction processes.

How Celebrus helps its customers to confirm it:

- Baseline Profiling: Establishes a detailed behavioral profile for each user over time.
- Cross-Channel Continuity: Monitors user behavior across channels (e.g., web, mobile, call centers) for consistency.
- Risk Scoring: Assigns a low fraud risk score to interactions that align with genuine consumer behavior patterns. Our differentiation approach combines behavioral insights, environmental data, and historical patterns to distinguish between fraud types and legitimate actions.
- Behavioral Biometrics: Tracks unique user behaviors (e.g., typing rhythm, mouse movement) to detect anomalies.
- Session Replay and Analytics: Analyzes how users interact with applications or forms in real time, revealing fraudulent intent.
- Machine Learning Models: Identifies patterns specific to first-party fraud (e.g., refund abuse) versus third-party fraud (e.g., credential stuffing).
- Data Enrichment: Integrates third-party data (e.g., credit bureaus, phone companies, IP validation resources, fraud consortiums, fraud bureau/CIFAS, and many more) to verify identity and behavior.
- Velocity Monitoring: Flags excessive or repetitive actions that suggest automation or fraud.

Choose a solution that stays ahead of fraud!

When it comes to fraud prevention, Celebrus is your missing lynchpin. Trusted by 4 of the top 10 global banks, Celebrus delivers advanced digital identity resolution, frictionless first-party data capture, and instant fraud detection and prevention solutions at scale.

Each Celebrus installation is built and managed specifically for each individual brand as a single-tenant, private cloud solution, and we ensure organizations remain compliant with privacy regulations such as GDPR and CCPA, while maintaining full ownership of their data. Celebrus integrates seamlessly with fraud prevention platforms, customer relationship management (CRM) tools, and risk management solutions to enhance existing fraud detection workflows and improve decision-making to support collaboration between fraud, risk, and compliance teams.

Contact Us

celebrus.com

moreinfo@celebrus.com

Chosen by industry leaders

More than
300M
Individual customer records...and counting

~100ms
Average response time — this is real-time

8
Weeks
Average time to value

citibank ally UBS HSBC BANK OF AMERICA