The ultimate guide to identity verification and real-time fraud prevention

celebrus

The ultimate guide to identity verification and real-time fraud prevention

Increasing consumer dependence on tech-forward digital banking options provides ripe opportunities for digital fraud – and fraudsters are taking advantage. Every type of fraud has increased dramatically over the past two years, both human and automated. At the same time, attacks and scams are becoming more complicated and harder to detect and prevent.

According to the latest LexisNexis Cybercrime Report, global transaction volume increased 44% year-over-year (YoY) in the second half of 2021, and automated bot attacks rose 32% YoY.

Fraud goes beyond borders or industries, it's widespread and highly interconnected. Financial, insurance, healthcare, telecom, retail, and even gaming industries are at increasing risk of attack by cybercriminals.

Enterprises need to be prepared by taking steps to prevent fraud and protect themselves and consumers. The first step is to tackle identity verification. From digital ID and verification options, to building comprehensive profiles to quickly detect and prevent fraud, this guide explores multiple authentication methods to tackle fraud in real-time.

Contents:

celebrus

The basics of digital identification

Fraud is increasing at an alarming rate. Organizations across all sectors are struggling to stay ahead of threats to themselves and consumers. Businesses are tasked with handling fraud while providing legitimate customers with a frictionless experience.

Less than 25% of all fraud losses are recovered – identity verification is critical to prevent fraud before it happens. Enterprises are looking for ways to reduce fraud in real-time. Digital identification (ID) has become a front-runner to combat fraud; however, it has its pros and cons.

Here's the rundown:

What is a digital ID?

A digital ID is an electronic version of an individual's physical identification card, such as a driver's license or passport. It can be used to digitally verify or authenticate the individual's identity and/or to grant access to a service online. Ultimately, the digital ID verifies the person is who they say they are when trying to access a digital channel. It provides the consumer with an easy way to digitally prove their identity, rather than presenting physical documentation. This became especially important during the pandemic and is often sold by vendors as part of a fraud, authentication, and verification product suite.

Digital ID is often discussed in relation to civic or government needs, as a literal digital version of government-issued identification. But there's a strong use case in the corporate world as well. Activities with the greatest value (and risk) are prime examples of where implementing Digital ID systems can be beneficial – such as healthcare, banking, government services, and education.

How does it work?

Using a mobile device, the consumer initiates the process on the business' website. The consumer receives a URL link via SMS that they must click to continue the process. The individual and phone are authenticated to prevent SIM swapping and confirm the consumer is in possession of the phone.

Next, the consumer takes a picture of both the front and back of the physical identification card (such as a driver's license, passport, or government issued identification card) using the same mobile device. The photo of the document goes through several forensic checks behind the scenes to determine if the identification card is legitimate (not a fake ID) or has been tampered with or altered in any way. The information from the ID card is matched against external data sources, such as a state Department of Motor Vehicles. Additional analysis and security checks are conducted using artificial intelligence (AI) and machine learning (ML), along with biometric technologies. These checks verify the bar code, holograms, and date of birth match, and that the photo print patterns and likeness check are consistent. A score is then provided to the business, along with reason codes, and a recommendation on whether to accept, reject, or conduct additional authentication of the consumer.

Pros and Cons of Digital ID

The primary benefit of digital identification is a reduction in fraud by providing businesses the capability to verify their consumers, reducing risk for both the enterprise and the consumer. For consumers, it's fast and convenient, and is usually completed within a few minutes, allowing

the verified consumer to continue to the business' website. For the business, it helps increase integrity and verifies the consumer currently using the digital channel is legitimate. A digital ID system streamlines what is traditionally a manual and clumsy process.

The biggest potential issue with expanding the use of digital identification is that not everyone has a mobile device or smartphone. According to Pew Research, more than 40 percent of people over 65 and 25 percent of people who make less than $30,000 a year don't own a smartphone. Another concern is the possibility of having a data breach where the digital ID information is stolen. Enterprise data protection and security are therefore critical when integrating a digital ID system.

Alternatives for identity verification

Innovative technologies, such as behavioral biometrics, enable organizations to digitally verify customers and users, ensuring integrity and reducing risk.

Let's explore 5 modern solutions used by leading enterprises to authenticate users. When it comes to identity, there is no single perfect tool, but using a combination of solutions, layered on top of one another, increases the success rate and reliability of digital identity verification while maintaining compliance with legal and ethical responsibilities.

Behavioral biometrics

Behavioral biometrics analyzes a consumer's physical and cognitive behavior such as mouse movement, swipe patterns, and touch pressure. Fraudsters have less probability of mimicking these

behaviors because every individual has a unique way of moving around a phone app or a website. By comparing user interactions with historical customer behavioral profiles, businesses can use behavioral biometrics to make a clear determination whether interactions are a real consumer or an imposter (fraudster).

Behavioral Analytics

Behavioral analytics (BA) solutions compare user interactions with known "good" or "bad" profiles. User profiles are stored and analyzed to understand the interactions and behaviors of hundreds of thousands of users over time and are constantly evolving. This enables the system to continuously authenticate users and identify suspicious activity.

BA uses this intelligence to detect unique behaviors displayed by cybercriminals. Suspicious activity is immediately flagged to existing access management and fraud detection solutions to stop account attacks as they happen.

Mule detection and tracking

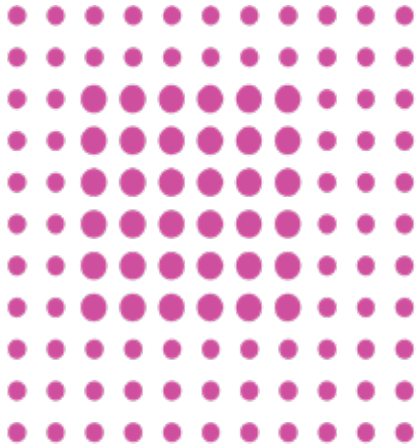
Mule accounts are a critical piece of the fraud pie – cybercriminals need a way to move and extract money, or there's no point in stealing it. Unfortunately, most financial institutions don't track mule accounts due to resource strain and the need for continuous monitoring.

Using a "sense and trace" approach, modern fraud prevention solutions perform real-time scanning of fraud intelligence networks to identify and track compromised accounts. They can also trace compromised identities to mule accounts to uncover additional compromised accounts and identities. This spiderweb of buried connections, illustrates why technology-enabled fraud solutions are best equipped for the job.

Anomaly Detection

With anomaly detection, organizations can automate the recording and measurement of aggregated data points such as customer behavior and page load times across all digital channels. This data is then used to build analytics models that compile information across data structures and platforms, searching for inconsistencies in data patterns.

Discovering hidden data patterns such as login failures, DDoS attacks, username or password harvesting, application failures, and bot attacks, empowers organizations to recognize fraud before it occurs. Every business has unique parameters and criteria that indicate abnormal activity, as well as tolerable risk levels. This may also vary by segment or business unit. Advanced anomaly detection enables enterprises to determine their own acceptable ranges and outcomes to alert risk management teams of potentially fraudulent activity. Enterprises can then customize alerts to their unique needs, striking a balance between reducing fraud losses and maintaining a positive customer experience.



Actively prevent fraud by running forensics before it happens

Many organizations, including banks, typically engage in "fraud management" rather than fraud prevention. They set an "acceptable" limit of fraud to avoid interrupting the customer journey. Unfortunately, this also means their thresholds allow numerous fraudulent transactions before recognizing they're fraud. Likewise, chasing fraud after the fact results in huge losses for financial and other organizations because only about 25% of losses are ever recovered.

The key to reducing these losses, and protecting consumers, is strong identity verification and authentication processes.

While many enterprises think their authentication practices are sufficient, most solutions start with authentication during sign-on which isn't soon enough. To truly prevent fraud, authentication must start the instant a user joins a website and continue throughout the session until they leave - not just when they're signed on. Behaviors exhibited by a fraudster before logging in can provide valuable context and signals that may indicate fraud early on.

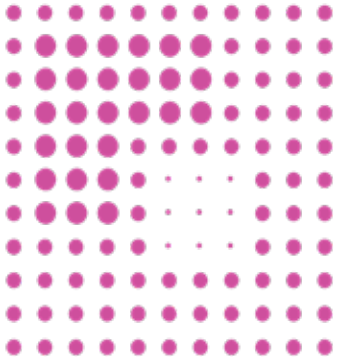
Think of a criminal investigation. Forensics begins with the crime (just like with typical fraud detection), they gather evidence and try to match it to suspects they identify later. Imagine if investigators had millions of individual comprehensive profiles, complete with DNA, fingerprints, behavioral patterns, and activities. They could use these to match the crime – or even predict it before it occurs. Sounds like a movie, right? In terms of digital fraud, it's actually possible to do this.

Behavioral analytics and biometrics enable real-time fraud prevention by monitoring every single interaction at an individual level. This occurs for 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 so that for every visit the enterprise can determine whether it's a legitimate user or not.

Advanced fraud prevention solutions also use 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 buyer journey disruption – focusing on detection and prevention - by "holding" accounts of 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 are shut down.

By layering behavioral biometrics and pattern analysis on top of robust identity profiles and PII you can make a transformational shift from detecting fraud after the fact, to actively preventing it in real-time.



4 steps to modern fraud prevention

1. Capture contextual behavior of each transaction and merge it with existing customer data to create comprehensive customer profiles

2. Apply machine learning in real-time to assess the fraud risk of each transaction

3. Decide if an intervention is required to stop the transaction, and what that should be

4. Deliver a message or other action to prevent the fraud

Critical questions to answer to inform identity

Enterprises must create clear and structured insights to inform fraud decisions with accuracy and efficiency. This includes solving for questions like: “Is the applicant behaving like a regular customer? Is the transaction in context? Is the customer behaving differently today? Is the quote pattern unusual?

A modern fraud data platform will capture, contextualize, and consolidate this information by considering the following:

WHO is interacting?

Are they a known customer or an anonymous visitor? This provides the starting point for connecting and analyzing identity. Beginning with a user profile - known or unknown - every interaction, behavior, keystroke, and action should be captured and resolved against other known data.

WHY are they here?

Is the user trying to open a new account, make a payment, or simply check their balance? Actions often dictate the path and triggers used in fraud detection and prevention - higher risk activities have stronger checks in place and activate more serious actions.

WHAT are they doing?

Are they changing credit limits or adding new payees? Updating profile details? Requesting password changes typically flags additional scrutiny, while other activities require behavioral and interaction context to accurately assess.

WHEN are they visiting?

Is this their first visit or are they a repeat visitor? Is the time of day consistent with previous activity or out of the norm? If a known customer always visits their banking app during business hours, account access at 2am is suspicious.

WHERE are they?

Consider the users location, device or network, and IP address. Advanced fraud data platforms can identify ISP, connection type, and even screen resolution to match behavior and interactions across multiple sessions.

HOW are they behaving?

Are their actions consistent with known behaviors and profile history? Behavioral signals such as mouse and swipe gestures, keyboard entry, touch pressure, and orientation as well as cognitive signals such as response time, pasting, and using shortcuts provide behavioral clues that can’t be overlooked. For example, a known user may always use their tablet in portrait mode, while a fraudster uses a mobile device in landscape orientation. In fraud prevention, every detail matters.

By assessing these questions, and building profilea for fraud detection, enterprise fraud prevention solutions can uncover clues to help analyze and assess fraud risk – and ultimately prevent it in real-time.

About Celebrus FDP

Celebrus FDP is the world's most advanced, comprehensive solution that captures real-time, first-party behavioral biometrics and PII across the entire customer journey – not just on the payment page. Instant availability to contextualized data transforms the prevention of scams and financial fraud such as new account creation, account takeover, and payment fraud. The ability to intervene to catch the fraudster before the fraud provides a more seamless customer experience, streamlines resource management, and reduces fraud expense to the organization.

Learn how Celebrus FDP enables you to catch the fraudster before the fraud by instantly activating contextualized identity and biometric data.

CONNECT NOW