How to beat creative fraudsters:

Moving from fraud detection to prevention

celebrus

How to beat creative fraudsters: Moving from fraud detection to prevention

Consumers are racing to adopt digital alternatives to in-person interactions, especially since COVID-19 disrupted the status quo. Unfortunately, fraudsters are also stepping up their game. Volatile economic and political markets, inflation, and increased travel provide even more opportunities for cybercriminals to exploit – and they do.

Digital fraudsters are an innovative bunch – they adapt and evolve their techniques continually to outsmart current fraud technology and maximize their success. It's time for enterprises to adapt in-kind and go on the offense.

The trends are increasing, across all industries. According to the 2022 State of Fraud & Account Security Report, the majority of industries saw a 400% increase in attacks, with those in travel seeing a major reappearance – a shocking 45% of traffic on travel sites is reported to be from scraping attacks.

Recent news shows that one in five logins is an account takeover attempt, with an overall 85% increase in attacks on logins and sign-ups.

In addition,

- 70+% increase in reported fraud losses in 2021 (FTC)
- 98% increase in credential stuffing attacks (using automation to try different usernames and passwords at scale) – predicted to double in number in 2022 (Arkose Labs)
- 85% increase in login & registration attacks in 2021 (Arkose Labs)
- 2/3 of technology, media, and telecommunications companies experienced some form of fraud in 2021 (PwC)
- Fintechs have an average fraud rate of around 0.30%, double that of credit cards that average 0.15-0.20%. (Experian)

Synthetic identity theft, one of the more creative types of fraud, is spiking as fraudsters create fake identities to defraud businesses, especially in financial services and insurance. New fintech categories like buy now pay later (BNPL) are expanding and providing increased opportunities for retail fraud. And the list goes on. As quickly as fraud experts can detect and impede one type of fraud, another emerges. At the same time, increasing privacy and compliance regulations are making it more difficult for fraud and security professionals to differentiate between "good" and "bad" actors.

This guide explores the rise of digital fraud, and how to beat fraudsters at their own game.

Contents:

The digital fraud landscape at-a-glance

Digital fraud is on the rise. Fraudsters have quickly developed new strategies to exploit digital channels leading to skyrocketing financial losses. With the emergence of real-time payments, losses happen fast and the ability to recover is low.

With increasing pressure from regulators for banks to act, detection and prevention have become a top priority for financial services.

Most current fraud solutions are inadequate and don't have the sophistication needed to activate all data—both transactional and digital. New and traditional solutions are reactive, not preventative. They're designed to identify fraud after it's already happened, when it's too late to do anything about it.

Traditional fraud solutions are transactional and backward focused. They only look at completed single transactions and historical transaction patterns. These solutions ignore behaviors detected around each transaction and instead rely on decisioning rules that are rigid and difficult to adapt.

Newer fraud solutions only focus on behavioral detection and are often a black box. They offer behavioral biometrics analysis, but don't incorporate transactional knowledge. These solutions are low in precision and accuracy, typically lacking explainability .

The majority of fraud solutions, both new and traditional, provide capabilities to detect and investigate fraud after it's happened, but aren't able to prevent fraud in real time. In a world of real-time digital payments, these solutions are falling behind.

You don't need more data – you need perspective.

Data on its own can't provide the perspective needed to activate real-time fraud prevention. When it comes to data in context, perspective is key. Context is essential for detecting and preventing fraud - and so is speed.

New and traditional fraud solutions can't keep up with the rapidly evolving strategies that fraudsters are using to evade detection. A contextual, future-proof, scalable fraud solution requires 5 key capabilities:

1. Combine transactions and interactions:

Combining conventional transactional information with behavioral data to describe digital interactions can provide valuable contextual intelligence that empowers richer insights, including detection of fraudulent behaviors.

2. Match identities to detect customers:

As customers move across channels, multiple systems capture customer data in different formats. The fraud solution must be able to match and link customer profiles across various data sources.

3. Enable increased accuracy with millions of models:

Training and deploying a personalized AI or machine learning model for every customer makes it possible to more accurately detect if interactions are from legitimate customers, or imposters.

4. Act in real time to drive intervention:

With millisecond, real-time response times, organizations can not only detect fraud, but also drive an intervention that prevents loss.

5. Continuously learn and evolve:

Leveraging artificial intelligence (AI) and machine learning methods to continuously train on user behaviors delivers the ability to detect new types of fraud tactics as they emerge, providing a scalable solution.

Advance from detection to prevention

To stop fraud, you need a solution that enables you to understand bad actors and intervene in their journeys with preventative action in real-time. The intervention itself can be defined by the severity and probability of fraud and can range from a warning message to blocked payment.

To actively prevent fraud, your solution needs to:

Listen

Build a contextual view of each transaction, combining detailed information about the transaction and digital behaviors that illustrate how users navigate, move, and interact with digital channels.

Understand

Profile and compare an individual customer with their expected behavior by applying real-time, hyper-personalized AI and machine learning models to quantify the fraud risk.

Decide

Use your decisioning process to determine if an intervention is required, and if so the severity. Aim for a balance between minimizing losses, maximizing experience, and reducing fraud management cost.

Act

If the threat is assessed as fraud, deliver the appropriate intervention in real-time to prevent it. If it's assessed as genuine, allow the transaction to continue.

Contextual decisioning enables real-time fraud prevention at scale

Generating data that is more accurate, timely, and contextualized provides insights that simplify investigations and improve efficiency. By reducing fraud investigations and case management your organization can eliminate overhead and improve overall efficiency.

Capturing multiple data points across multiple channels, for millions of users, and contextualizing transactional data with behavioral data requires a massive amount of work and insight. Automating this process and making use of intelligent technology greatly streamlines the process to execute at scale. Although fraudsters are becoming more sophisticated, the same rules apply in reverse – financial and other enterprises must become more sophisticated in their fraud prevention solutions.

By intervening in fraudulent transactions in real-time you can not only reduce fraud losses, but also reduce false positives. This improves the customer experience because you only stop fraudulent transactions, not genuine ones, which greatly reduces customer friction. Proactively intervening to protect at-risk customers also creates better customer experiences.

With a forward-focused fraud solution you can address evolving threats and stay ahead of new fraud types and strategies.

For example, one of our clients, a top 5 global bank, was struggling with Remote Access Takeover (RAT) fraud, which grew 15% during COVID. The bank was experiencing over 2,000 fraud cases per month, and losses of $2,700 per fraud case. With losses and pressure from regulators escalating, the bank needed to act fast. They needed a real-time solution to detect fraud and prevent losses before they happened.

The bank deployed Celebrus for real-time, comprehensive data capture and cross-channel user identification, along with Teradata Vantage for data configuration and enterprise analytics. They established a hyper-personalized behavioral fraud solution to prevent fraud, improve the customer experience, reduce losses, and improve business efficiency.

With 250K unique customer journeys per hour at peak times, there was a lot of data to process. The combined solution began with capturing digital interactions in real-time, then analyzing the data for transactional and behavioral patterns. They were able to run millions of micro models to assess behaviors and deploy insights in sub-second response times.

The results were impressive:

- 70% of the bank's fraud cases are now detectable and preventable
- $100M In fraud detected and prevented

Enabling contextual decisioning and actioning while the user is live on a digital channel is critical to preventing fraud.

Behavioral biometrics and the scam technology arms race

Over the years, financial institutions have developed ingenious ways to root out fraud and scams.

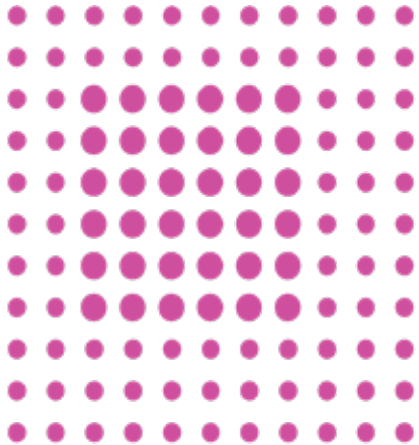
Banks and card issuers have spent millions implementing algorithms to analyze transaction activity for anomalies that uncover compromised accounts or credentials for fraud analytics teams to investigate. Their data models look at global patterns, such as time spent on specific web pages or device location, to verify the credibility of transactions or transaction amounts. However, these rules-based systems are easily infiltrated by enterprising fraudsters, typically detected too late to catch fraudsters in the act.

Behavioral biometrics technologies provide a superior alternative to help identify behavioral anomalies and better protect against fraud. Behavioral biometrics uses multiple data points, such as how someone holds, touches, or taps their device, to guard against known and unknown attack types.

The data collected can be used to follow the activity of scam victims across devices and systems to find associated identities coerced by scammers, and set alerts based on those activities. When combined with traditional anti-fraud prevention systems, behavioral biometrics enable organizations like financial institutions to detect and prevent a range of scams in real-time, at scale, in an automated way and with a very high degree of accuracy. They give fraud teams an extra layer of data to revolutionize fraud prevention by connecting fraudulent activities to uncover scam networks.

While in theory it's possible for scammers to trick identification technology and mimic a real person, the reality is that would only be effective with a one-off approach. It takes a lot of time, resources, and programming to effectively bypass behavioral biometrics at scale. Most attackers simply don't have these resources, which is why it's such an efficient shield against fraud.

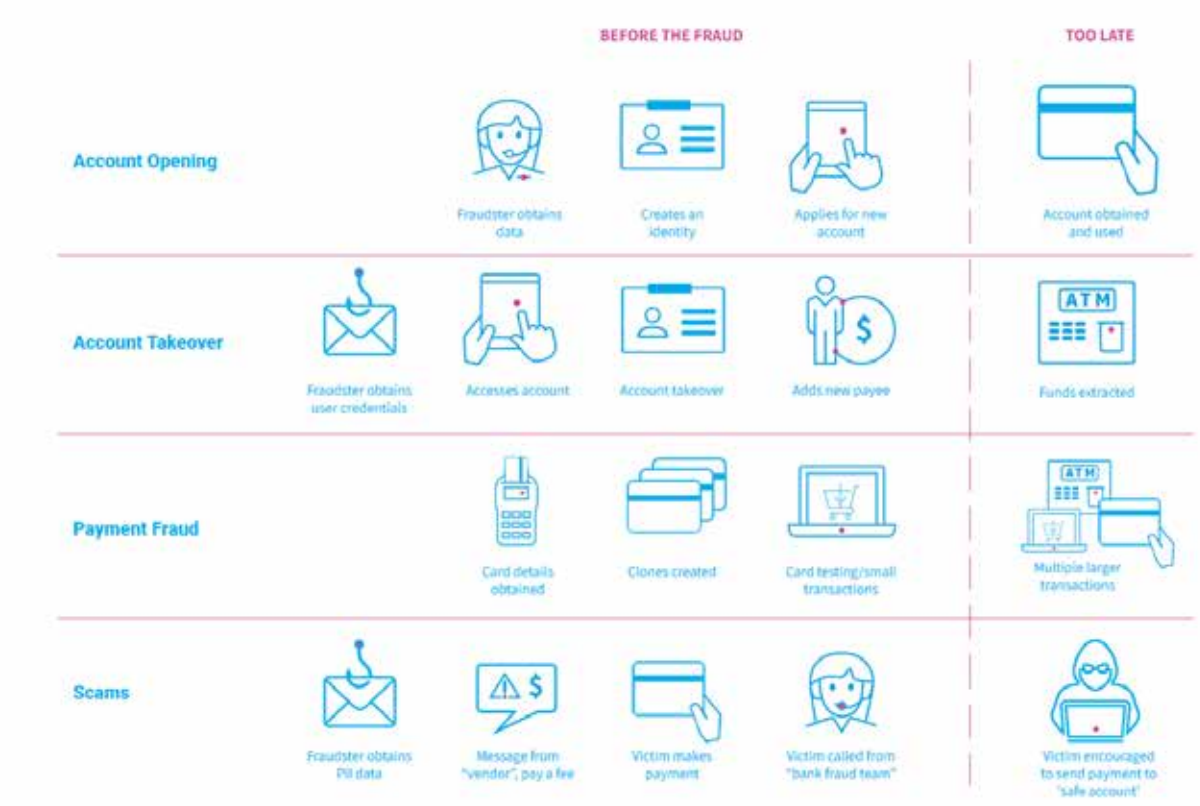
Although scams have become an accepted societal nuisance, digital technology has made it too easy for scammers to begin and expand quickly, only to disappear behind technology buffers. Organizations can shift the power dynamic by turning criminals' own digital "fingerprints" against them, using behavioral biometrics to gain the advantage.



The power of prevention

There's a fine line of distinction between where fraud can be prevented, and when it's too late. Considering only about 25% of fraud losses are ever recovered, this thin line is the equivalent of millions, even billions, of dollars per organization. If you can move that line just one step in the process, the rewards are extraordinary. Consider four common types of fraud – New account, Account Takeover, Payment, and Scams. Each has several steps before it's too late, to identify and prevent fraud.

A fraud prevention platform identifies and halts fraudulent activity before it's too late. With account opening fraud, the identity and behavior of the user when completing their application will give valuable data points to assess validity. With account takeover, there can be indicators during the account access point in addition to signals when a new payee is added, or information is changed. An increase in activity such as a series of small transactions can flag potential payment fraud, while payment behavior contextualized with customer behaviors can indicate a potential scam.



Real-time is key

The term “real-time” is used exhaustively these days, especially in the tech space, and everyone has their own definition. According to the Oxford dictionary, real-time means “relating to a system in which input data is processed within milliseconds so that it is available virtually immediately as feedback”. To be clear, a millisecond is 1/1000 of a second. So, customer data platforms (CDPs) who claim “real-time” data capture but only offer 30 or 60 second timing, aren’t providing a real-time solution. To compete in the real-time fraud prevention game, we’re talking milliseconds.

Let’s put this in perspective:

- The human eye takes 300 milliseconds to blink
- The average human reaction time (the time it takes to react to input) is 250 milliseconds
- The interval between swiping a card and transaction approval is measured in a few seconds
- It takes 7 milliseconds to snap your fingers

When it comes to fraud prevention, speed is critical. The longer a buyer’s journey takes, the less likely they are to complete checkout. When looking at fraud prevention solutions, remember to account for both the data capture and the data processing (how long it takes to deliver to your decisioning platform). Data captured in milliseconds doesn’t do much good if it takes 30 minutes to deliver actionable insights to your downstream applications.

Equally time-sensitive is the user experience in terms of false positives. The faster you can differentiate legitimate users from bad actors, the faster you can allow the transaction to continue without interrupting the buyer’s journey. And, of course, the ultimate goal is to beat the fraudster BEFORE they’re able to complete the fraud – protecting both your organization, and your customers.

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 beat creative fraudsters by moving from fraud detection to prevention.

CONNECT NOW