Out of the (black) box

Unleash the power of real-time fraud prevention

celebrus

Unleash the power of real-time fraud prevention with a platform fraud solution

Most fraud solutions only address one type of fraud, maybe two. The reason is simple – it's easier. But easy doesn't mean best. While there are different approaches to the different types of fraud, there's also a lot of crossover.

In addition, these single-serve fraud solutions live in a "black box", meaning they're completely separate and distinct from the organization, from each other, and they don't (in fact CAN'T) pass data back and forth. We'll get into that later, but first let's look at the most common types of fraud causing pain for fraud professionals today.

Contents:

The four key types of fraud banks needs to address

While there are as many variations of fraud as there are fraudsters, the schemes can be grouped under four key types. Understanding the mechanisms behind them is the first step in a proactive fraud prevention strategy.

Scams – when a fraudster employs a scheme directly targeting individuals or groups and convinces (aka tricks) them into making a payment or transferring money.

While other types of fraud can be more hands-off, relying on technology, scams typically include heavy personal involvement on both sides. And scams are part of every other type of fraud – a scam will often collect or augment the information needed to create a false identity, take over an account, or launder stolen funds after the fraud has been executed. Common examples include impersonation scams, romance scams, investment scams, and money mule scams.

Scams are the most difficult fraud type to combat because of the people factor - the owner of the account legitimately sends their money to someone who's tricked them into doing so. When a victim unwittingly provides their information to a fraudster, makes a payment to a fake account, or transfers funds from a legitimate account, it's not as obvious as a fake application or suspicious transaction. As a result, fraud solutions targeted at identifying scams will typically make use of behavioral analytics, including biometrics, to detect behavior that can signal a potential scam situation or a customer acting out of the ordinary.

RAT (Remote Account Takeover) fraud – when an unauthorized person takes control of an existing account.

Typically, fraudsters steal consumer account information and credentials such as username and passwords, which they use to access the account and steal funds. The information can be collected by purchasing on the dark web, mining social media sites, and through scams by directly contacting the account owner. The fraudster will often attempt to modify the account information, password, and notifications so the actual owner isn't aware of the malicious activities in their account.

A fraud solution targeted at identifying account takeover will look for activity like multiple requests for a password reset or unsuccessful login attempts, changes to key information like email address or phone number, and fraud-related behavior like erratic mouse movements.

Payment fraud – when a fraudster either steals someone's payment information or opens a fake account to make a purchase with no intention of paying for it.

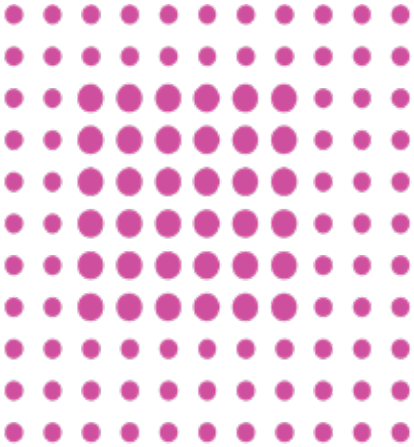
In general, it's any false or illegal transaction completed by a criminal. This includes BNPL fraud, which is growing in reputation and more difficult to detect. Payment fraud can also occur when a legitimate customer initiates a false chargeback by disputing a charge or claiming the product wasn't received, when in fact it was.

A payment fraud solution will look for signs of identity theft, multiple suspicious transactions, change in delivery address, usage anomalies, etc. but they're typically focused on transaction monitoring. Risk-based scoring and authentication/verification are also often part of payment fraud solutions.

Application fraud – when a fraudster uses a stolen or synthetic ID to apply for a loan or line of credit with no intention of paying back the lender.

This type of fraud also includes legitimate customers falsifying their application information. It can refer to insurance application fraud as well, when someone falsifies their information, or creates a fake identity to either obtain insurance or add as a loss payee for a future insurance scam.

A fraud solution aimed at identifying application fraud is literally analyzing the information on an application and looking for red flags. Behavioral analytics can supplement by identifying fraudulent behavior such as cutting and pasting while identity resolution can uncover multiple applications using the same or similar name, email, or address.



Why black box fraud systems aren't enough

As stated, fraud, in its many forms, doesn't live in a silo or black box. Different types of fraud deploy multiple methods that work together to execute the larger fraud. Scams are a perfect example of the crossover between fraud types because they're regularly used to gather information that enables account takeover, identity theft, creation of false identities, and authorized push payment (APP) fraud – including money mule scams.

For example, leading up to RAT fraud, fraudsters will often execute a scam to collect an account number, fill in missing information like security questions, or bypass security checks by having the victim provide their password or verification code to complete the account takeover. They may then transfer funds from the hijacked account to a fraudulent account created via application fraud. Then they use a money mule to complete that transfer.

Likewise, application fraud can use scams to collect information to create a fake identity that's used to set up new accounts, credit cards, or insurance policies. Speaking of insurance, scams are often the final play in insurance fraud – setting up a false scenario (or false payee) to get a payout.

In fact, it's highly unlikely – if not impossible – to have one type of fraud be completely standalone. The success of fraud is dependent on many of these approaches working together. Which is exactly why your fraud solution needs to do the same.

The other glaring issue with most fraud solutions is they're black box because they're third-party. When dealing with banks and financial institutions, there's so much exposure to risk they must massively encrypt the information from the bank and CAN'T transfer PII (personal identifiable information). The amount of encryption and extra steps that would be required to then send all that information back to the bank is unrealistic. Instead, they operate in a black box environment which means the bank never gets the actual data - all they get is a score with no context, no explainability, and no sharable intel. And because security overrides timeliness, it's impossible for third-party fraud systems to get real-time data to actively prevent fraud. Finally, this simplistic scoring method creates a lot of false positives due to the lack of context, with no insight into why. Not a great experience for legitimate customers.

The result of this single-serve approach is that every bank has multiple fraud systems, running in multiple departments, addressing multiple fraud types – completely INDEPENDENT of one another. Not only is this costly and inefficient, it stops the organization from building complete identity profiles that stitch together activity data, behavioral data, and contextual data for a 360-degree view of the customer to prevent fraud in real-time. They can't see that user123 browsed four of their subdomains and submitted a credit card application on each, with slightly different information, but the same IP address and same behavioral biometrics. They can't tell that a legitimate customer is logged into their banking app on their desktop at the same time as they're in the mobile app and one of those may be under the influence of a fraudster. They can only see that a legitimate customer is making a payment to a new account they just added. And since the payment fraud system is disconnected from the application fraud system, they have no idea the account that was just added is the same one that just got flagged by the application fraud department.

How to combat all fraud types with a first-party platform fraud solution

To effectively combat fraud – and more specifically prevent it – financial institutions need a comprehensive solution that detects all types of fraud in real-time and builds comprehensive identity graphs that increase their ability to prevent all types of fraud. Capturing and consolidating data across session, device, domain, and over time multiplies the power of a platform fraud solution and reduces false positives.

Using a first-party fraud solution, all data is captured and contained in-house, protected within the organization's robust security protocols so banks can activate all their data to use across the organization – for every fraud use case. They can also build their own fraud models, applications, and intellectual property and ensure privacy and regulatory compliance. It can even be used to enhance existing fraud management systems and deliver real-time decisioning to effectively prevent fraud.

Every bank has a fraud team, with data scientists building fraud models. Every one of those teams is using a plethora of different technologies like FICO, SAS, Quantexa, BAE, and others - and each has their own models (RAT fraud, application fraud, scams, payment fraud). Every single one of those models can benefit from better data.

Better data means better results. By connecting a full customer view with all data points within a protected environment, these solutions can maximize the efficiency of technologies like behavioral biometrics, Machine Learning (ML), and link analysis to not only detect and prevent fraud in real-time, but also to identify known mule accounts and trace them to other connected accounts and profiles.

A true platform solution is the gold standard in combatting all types of fraud and overcoming the challenges of traditional black box fraud systems to actively prevent fraud in real-time, across the organization.

Meet the gold standard

Celebrus FDP is a first-party platform fraud solution that solves for all fraud types in real-time. With connected, compliant data capture, organizations can stitch users together across channel, session, device, and time for a full identity view that can be used across the organization – say goodbye to silos forever. Doing all of this within milliseconds enables instant decisions for intervention. The value impact of this is enormous – instead of looking back to see what happened (like most fraud solutions) the organization can see what's happening NOW, in the moment. When you prevent losses in the first place, you don't have to spend time recovering them. Your customers and your organization are protected.

The level of data produced by Celebrus is unmatched in the industry. Because Celebrus FDP is first-party, contained within your organization, you have access to the real data and can load it into any system you choose, in parallel. It supplements your other fraud solutions, so they can work optimally. The data is captured seamlessly and not only can it be fed into your existing fraud management systems and data models, it can also receive data from other systems to contextualize and send it back – forming a valuable two-way information sync.

Since Celebrus FDP is embedded directly within your organization's websites and mobile apps, it also provides the ability to intervene in real-time – i.e., displaying a pop-up warning for a suspected mule account or taking over the entire session to actively prevent the fraud from being executed.

Example: a customer is on their phone at the exact same time they're logged into their bank account. This is classified as atypical behavior, but most fraud solutions wouldn't be able to identify those signals because they can't persist identity across channels. And while this could be a perfectly legitimate occurrence, it can also be indicative of a scam where the fraudster is on the phone convincing the customer to provide their login details, perform a verification, or transfer funds to an account under the fraudster's control.

Celebrus CDP can capture this comprehensive data simultaneously and match it to the identity profile, while also comparing to known mule accounts or fraudulent behaviors, and instantly alerting to high-risk signals. It can also push an intervention, such as placing a hold on the transfer and delivering an in-app message advising the customer to contact their bank directly.

To defeat fraud and prevent it in real-time you must stop looking back at what happened and be able to see exactly what's happening NOW, in real-time.

Meet Celebrus FDP

Celebrus FDP is the world's most advanced, comprehensive first-party platform fraud solution that captures real-time behavioral biometrics and PII across the entire customer journey – not just on the payment page.

Instant availability to contextualized data transforms the detection and 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 and frictionless customer experience, streamlines resource management, and reduces fraud expense to the organization.

See how Celebrus FDP enables you to prevent all fraud types in real-time.

CONNECT NOW