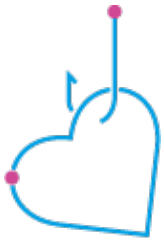
How to protect your account holders from scammers

celebrus

Scam losses are increasing

Scam tactics are being used at an increasing rate to dupe banking customers into transferring funds to fraudster-controlled accounts. Banks, who have traditionally offered customer awareness and education programs to combat these threats, are searching for stronger methods to differentiate their service offerings and better protect their customers.

But catching scammers is highly challenging. Fraudsters choose scamming strategies because they're hard to detect – scams involve sophisticated deceptions which result in customers voluntarily transferring money to fraudster-controlled mule accounts. The money lost is effectively unrecoverable in these situations. So, how can a bank identify and prevent a scam when the victim has failed to do so?



⇧ 62%
romance scams

⇧ 123%
impersonation scams

⇧ 95%
investment scams

Banks and financial organizations can protect their customers from scams, online fraud, and financial crime by using the unique behaviors of fraudsters to identify them. Despite their evolving techniques, fraudsters can't replicate the way genuine users behave when they access online platforms and make payments. When a customer is drawn into a scam they behave differently, and this real-time data provides a unique opportunity for the bank to detect and stop the scam. By leveraging automated behavioral insights which work seamlessly with your existing fraud management tools, you can shut down scams instantaneously.

Organizations who proactively work to protect account holders from scammers differentiate themselves in the market and build long-term loyalty.

Although the debate rages on whether banks and financial institutions should be responsible for customer losses suffered due to their own negligence, the reality is that by helping to protect your account holders from scammers you are building trust, authority, and strong loyalty with your customers. And don't forget the direct financial benefit – eliminating hours upon hours of unnecessary support calls when a customer realizes they've been scammed and contacts your organization for assistance.

Using a real-time solution that delivers frictionless, invisible, and continuous authentication you can transform the customer experience and provide seamless protection from scams. Real-time detection is a critical component of fraud solutions because the key is instantly flagging anomalous customer behaviors which indicate they're being scammed, enabling you to take immediate action.

Key takeaways

- Scam losses are increasing, and enterprises who protect customers will differentiate themselves
- Leveraging data to identify fraudsters by their unique behaviors helps prevent scams
- Helping prevent scams builds customer loyalty and reduces fraud management costs
- Frictionless authentication improves the customer experience while providing protection from fraud

Protect your account holders from common scams

Let's take a look at the four most common types of scams, and how modern fraud detection can prevent them in real time.

Impersonation scams

Impersonation scams are one of the more creative attacks, as fraudsters pretend to be a seemingly legitimate person or company and often create emails, accounts, and other assets with copied information. In early stages, this may be executed simply to collect information for later use in committing the scam. Once the fake profile is established, it's used to collect funds from the scam. In the UK alone, impersonation scams more than doubled in the first half of 2021 as fraudsters continued to expand their scam tactics.

These scams can target both consumers and businesses as fraudsters can also take over or spoof the email of a company's employees, customers, or vendors. This is especially powerful when the "request" is coming from a higher-level manager or executive. For vendor impersonation, it can be as simple as changing the account details on an invoice using a spoofed email. In any case, the fraudster disappears after the scam – never having interacted with a banking system directly.

Let's dive into what this might look like:

Impersonation scams

1. The fraudster obtains some of the victim's bank, contact, and other key details

2. The fraudster then contacts the victim, claiming to be from a trusted source like the police or the victim's bank

3. The victim is convinced of legitimacy because the fraudster has key privileged information

4. The victim is told their savings are being attacked, or that a fine is due and they must make a payment

5. The victim clicks on a link, or calls a fraudster-operated hotline, to make the "urgent" payment

6. The victim makes a payment to the fraudster and remains unaware of the fraud for many hours or even days

Investment scams

Investment scams typically involve promises of big payouts, quick money, or guaranteed returns in exchange for investing money – often for little or no risk. While this may seem like the classic "if it's too good to be true it probably is" situation, investment scams can be very sophisticated and convincing. The rise of cryptocurrency has also spurred an increase in investment scams since it's easier for fraudsters to take advantage of the less regulated environment.

Mule accounts are typically used to move and extract money with investment scams. While it's hard for financial institutions to track mule accounts independently, advanced fraud solutions tap into the power of fraud intelligence networks to identify and track compromised accounts and identities. This means that when a consumer attempts to make a payment to a mule account it is instantly marked and can be prevented.

1. The fraudster sets up a series of mule accounts for the purpose of extracting funds from victims without detection

2. The victim is contacted by the fraudster or responds to an advertisement for a very attractive investment opportunity

3. The fraudster induces the victim to transfer money to a fictitious fund or to pay for a fake investment, creating urgency with a time limit or bonus for investing before a set date

4. Many victims don't discover the scam for weeks or even months

Romance scams

Romance scams are one of the most common frauds in the market – in the US alone a whopping $1B in losses were reported in 2021 according to the FBI.

These scam artists take advantage of victim's emotions and have various approaches to conning their targets. Here's a typical romance scam lifecycle:

1. The fraudster establishes a number of fake online dating or social media accounts

2. Potential victims are contacted by the fraudster with the intention of establishing a fake relationship

3. When a victim responds, the fraudster uses a range of malicious tactics to establish a strong bond over a long period

4. After a relationship has been established, the fraudster requests a small payment, weaving a story of financial hardship

5. The victim sets up the fraudster as a new payee and makes several small payments over time

6. The fraudster convinces the victim to make a much larger payment, often claiming a medical or family emergency, or wanting to meet the victim in person

Imposter scams

In an imposter scam, a dishonest person lies and tricks the victim into sending money to them. They might call on the phone or send an email or text. Imposters may try to get payment by asking the victim to buy a gift card or wire money. There are many varieties, but they work in the same way – a scammer pretends to be someone you trust to convince you to send them money. This can be in the form of a cloned social media account of a close friend or relative, making it appear it's someone known, or from a familiar organization such as a government association or charity. More than $2.3B of losses reported by US consumers in 2021 were due to imposter scams, almost double what it was in 2020.

1. The fraudster obtains a list of social media contacts

2. The fraudster creates a duplicate social media account of one (or many) of the victim's contacts

3. The fraudster reaches out to the victim with the fake account, asking the victim to send money

4. The victim sends the gift card or transfers the money, believing they're helping a known individual

5. The victim may not be aware of the scam for hours, days, or even weeks

How to protect your account holders

Flagging new payment destinations, recipients, and accounts is standard operating behavior for fraud detection, but without context it's difficult to decipher which are legitimate versus prompted by a scammer. The usual rules of fraud prevention don't quite apply, because in most scam cases a real, authenticated customer is logged into their account in order to make the payment. The goal is to rapidly identify high-risk activities, so contextualization is key for detecting possible victims of a scam attempt. Considering whether the activity is in line with typical interactions from the customer, identifying and tracing flagged mule accounts, and layering behavioral biometrics on top of it all creates a recipe for success in identifying and preventing scam attacks on your account holders.

With an advanced fraud data platform, enterprises can protect valid account holders by weeding out the imposters. There are 7 key areas where a comprehensive data platform enables proactive fraud prevention:

1. Compare user interactions with historical profile
2. Compare user interactions with known good or bad profiles
3. Collect real-time signals & scores from fraud detection
4. Gain added insight from data model for investigations, AI, rules, and reporting
5. Incorporate cognitive signals such as shortcuts, typing patterns, response time, memory/recall, and pasting data into the identity profile
6. Capture payee PII in real-time to enable further tracking and investigation
7. Use behavioral biometrics and cognitive signals to identify fraudsters instantly

Behavioral biometrics are the secret ingredient in detecting and preventing scams. With a data platform that incorporates behavioral biometrics, enterprises can consistently build profiles of legitimate user behavior. For example, a typical banking customer likely doesn't request wire transfers on a regular basis, if at all. When that customer attempts to initiate a wire transfer, at the request of a creative scammer, they'll often hesitate and take extra time to find what they're looking for, fill out the information needed, etc. This is a data point for the fraud data platform to incorporate along with all other data points. A victim's biometric behavior signals are also very different when they log into their account if they're panicking or in a hurry. Users who are worried about losing their life savings, or rushing to take advantage of a limited time opportunity can't help but translate these emotions into their typing speed, gestures, etc. Likewise, a romance or imposter scam victim may hesitate, worrying whether this new person (or known person) will pay them back. These behavior anomalies are collected, detected, and sent as signals to fraud management systems and teams in milliseconds.

A modern fraud solution can also automatically detect behaviors that are commonly exhibited by scammed individuals, based on hundreds of thousands of interactions tracked over time. Advanced scoring and artificial intelligence (AI) can further contextualize known behaviors of scam victims, for example in the case of romance scams where fraudsters often escalate their requests for money or gifts.

How Celebrus for Fraud helps protect your customers from scammers

Celebrus for Fraud, the leading live-time fraud defense solution, enables you to catch the fraudster before the fraud by leveraging the rich behavioral data captured by our platform. Celebrus captures all customer interactions on your website, mobile App, and IOT devices. Our pre-configured, analyst-friendly technology automatically detects behaviors commonly exhibited by scammed individuals. Sophisticated scorecards and integrated AI deliver instant insights to shut down scams before your customers are conned out of their money.

Celebrus defines events and signals for fraud detection, flags behavior anomalies, and captures new payee information including PII in milliseconds. The detailed data and signals are then sent to fraud management systems and teams for further investigation and/or real-time payment blocking.

For example, defined signals can trigger a message on the victim's screen saying "Stop and think – do you know this person? You may never get this money back! Please call us immediately", then the payment is blocked or stopped for further investigation in real-time.

Celebrus' real-time behavioral analytics provides your organization with the tools you need to stay one step ahead of scammers. And there's no need to replace your existing Fraud Management, Identity Proofing, or Authentication systems - Celebrus perfectly enhances these applications to deliver next-level fraud prevention. We also provide comprehensive support, and managed services if you're looking for a full solution.

Learn how Celebrus can help you track, contextualize, and identify fraudulent behaviors to protect your valuable customers from scams.

CONNECT NOW

Connect now and book a demo

celebrus

www.celebrus.com