Early Warning®

# Five Best Practices for **Preventing Account Opening Fraud**

# Introduction

## What do credit card fraud, money laundering and first-party check fraud have in common?

**They are all facilitated by account opening fraud.**

Account opening fraud is booming—and its impacts are far reaching. In fact 81% of financial institutions say it increased in the wake of the pandemic and the upward trend is continuing.[1]

On first glance, account opening fraud may seem relatively harmless. But the act of falsifying an application to open an account is rarely the end game. Rather, it's a gateway crime that enables bad actors to commit more costly and dangerous offenses down the road. A 2022 Datos Insights report highlights a variety of concerning downstream trends:[2]

82%

of FIs report that first-party check/deposit fraud resulting from application fraud is up year over year

63%

of FIs report that mule activity (using a bank account to launder money) resulting from application fraud is up year over year

44%

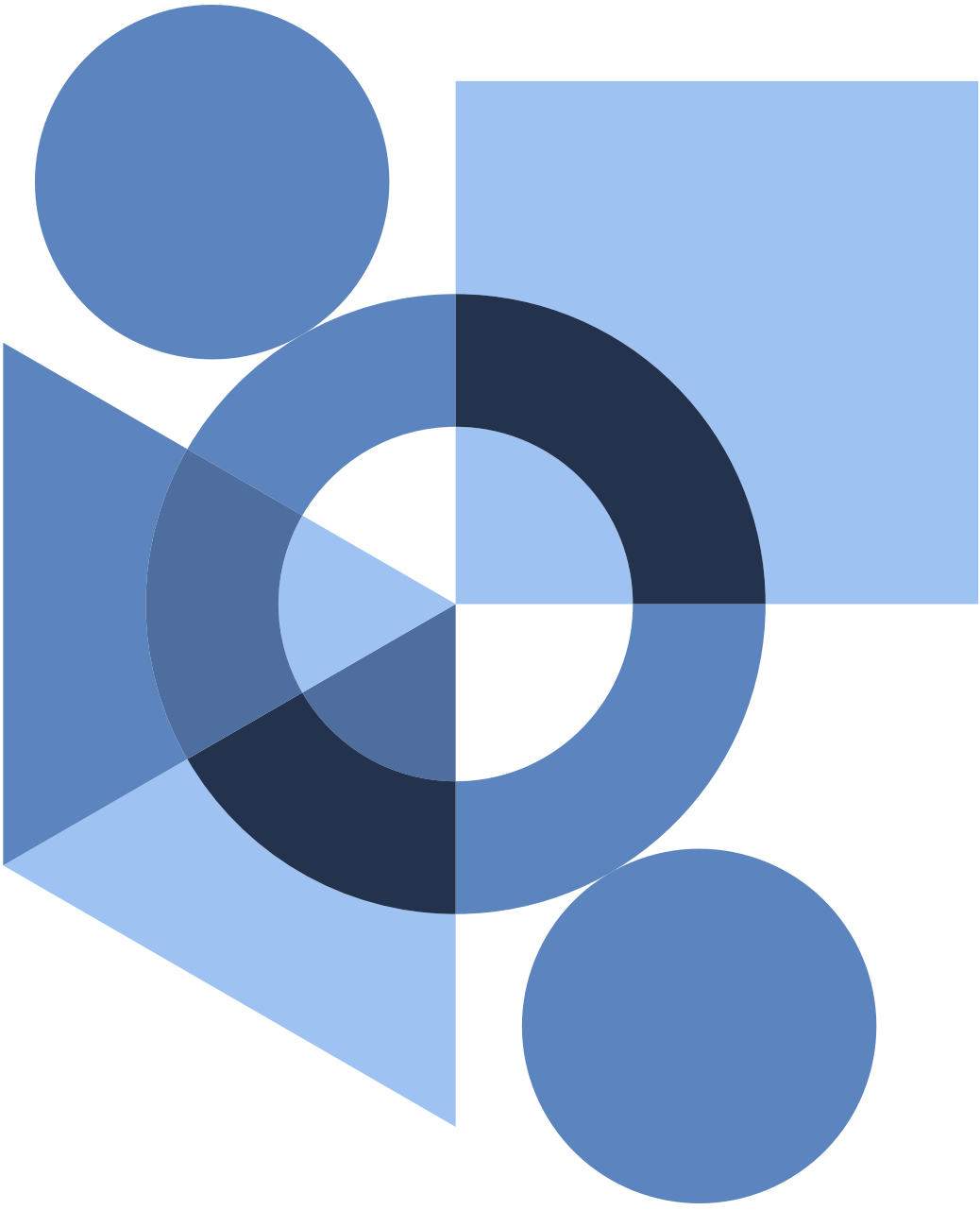
of FIs report that first-party lending fraud (including credit cards and loans) resulting from application fraud is up year over year



CLICK HERE TO LEARN MORE

To prevent massive downstream losses and reputational damage, banks and credit unions must be able to spot and stop criminals at the point of account opening.

In this guide, we examine the unique challenges FIs face in preventing account opening fraud—and we share best practices for overcoming them.





CLICK HERE TO LEARN MORE

# Identity plays a central role in account opening fraud

When a bad actor provides false information on a new account application, the goal is always the same: to trick the FI into opening the account. To accomplish this, however, the fraudster may use their own identity, a stolen identity or a made-up identity.

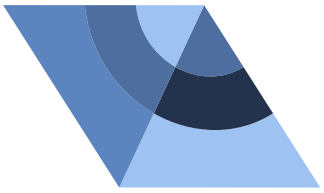
**Here's how each tactic works:**

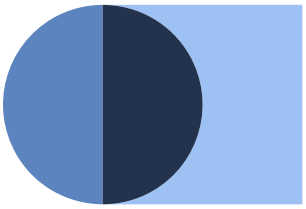
## FIRST-PARTY ACCOUNT OPENING FRAUD

A person provides their own personally identifiable information (PII) on the application, but misrepresents other potentially qualifying information (e.g., income, employment history).

## THIRD-PARTY ACCOUNT OPENING FRAUD

An individual (or a crime ring) steals another person's PII and opens the account in that person's name. Third-party fraud is considered "true identity theft" because the stolen identity is that of a real person.





## SYNTHETIC IDENTITY ACCOUNT OPENING FRAUD

Unlike first-party and third-party fraud, the criminal in this case does not use a real person's identity. Instead, they use a made-up identity, which has been created using a mix of real and/or fabricated PII.



CLICK HERE TO LEARN MORE

The pandemic-driven shift to digital services increased the risk of data breaches, making it easier for fraudsters to access consumers' PII, manufacture sophisticated identities—and commit account opening fraud.

In the current fraud landscape, FIs are prioritizing funding for identity verification controls.[3]

## In 2022, traditional identity fraud totaled $20 billion and impacted 15.4 million victims.[4]

## Synthetic identity fraud is the fastest growing financial crime in the United States.[5]



CLICK HERE TO LEARN MORE

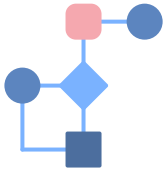
# Account opening fraud challenges extend beyond identity verification

Effective identity verification is essential in the battle against account opening fraud. But it's only the first line of defense. After ensuring an applicant is who they say they are, FIs must determine the risk of doing business with them.

**Below are two additional challenges FIs must overcome.**

## Reducing fraud risk and ensuring compliance—without sacrificing the customer experience

Traditional account opening systems provide "yes" or "no" approval decisions derived from limited, internal data sets. Because these binary tools err on the side of caution, FIs often turn away potentially viable applicants. What's more, when FIs update their systems to stay compliant and/or reduce risk, the new controls can slow down the approval process—frustrating consumers who expect fast and easy digital experiences.



## Detecting and quantifying account opening fraud

To successfully combat account opening fraud, FIs need to know where their systems are failing. But account opening fraud is hard to detect because the act itself doesn't result in an immediate loss or raise red flags. To the contrary, it often appears like legitimate customer behavior. And once the account has been opened, distinguishing between first-party fraud, third-party fraud and synthetic identities isn't easy. For FIs, however, differentiating between these forms of fraud is critical for understanding the scope of the problem and tailoring prevention strategies.



CLICK HERE TO LEARN MORE

# Best practices for preventing account opening fraud

**Preventing account opening fraud may feel like a complex and daunting challenge.** But it doesn't have to be. Here are five best practices to level up your fight against account opening fraud:

1

## ASSESS YOUR CURRENT SOLUTIONS

To stay compliant and reduce fraud losses, it's important to regularly evaluate your new account fraud prevention solutions and make updates where needed. One way to avoid disruptions as fraud trends evolve is to adopt a holistic solution that gives you the flexibility to align new capabilities with your business goals and threshold for risk.

2

## LEVERAGE ADVANCED ANALYTICS

Embrace predictive analytics and machine learning tools. These advanced analytic models can process massive amounts of data instantly—to predict risk in real-time and speed up the onboarding process.

3

## USE CONSORTIUM DATA

Analytics, no matter how sophisticated, are only as good as the data they're fed. Consortium data (sharing data across institutions) is critical for accurate risk assessments. When you combine advanced analytics with pooled data, you can make more informed approval decisions, based on deeper data intelligence.



CLICK HERE TO LEARN MORE

4

## ENHANCE IDENTITY VERIFICATION

To effectively prevent account opening fraud, you must be able to quickly and accurately verify the identities of potential customers. You can expedite customers through the application process without letting bad actors enter your system by using an identity intelligence solution that determines the likelihood that an applicant is who they claim to be in real-time.

5

## CUSTOMIZE CUSTOMER ACCOUNT PRIVILEGES

Once you've confidently verified a customer's identity, the next important step is to evaluate what types of services, privileges, and limits you should offer. Use a predictive analytical scoring tool to make tailored account privileging decisions, reducing the risk of first-party fraud or account default and enabling faster account funding.



CLICK HERE TO LEARN MORE

# Early Warning® is your ally in the fight against account opening fraud

As the Trusted Custodian® of the *National Shared Database*℠ resource, Early Warning collects account data from thousands of financial institutions on a recurring basis. Verify Identity and Predict New Account Risk leverage this vast data pool, using predictive analytics and machine learning models to provide the deep data intelligence you need to make fast, confident account opening decisions.

When a customer begins the account opening process, Verify Identity gives you insights to determine the likelihood that their identity is valid in real-time, as well as an improved ability to identify synthetic and manipulated identities.

Early Warning®
**Verify Identity**

**Verify Identity provides the following outputs:**

- **Identity Confidence Score:** assesses the likelihood that a person is presenting their true identity credentials with a predictive, analytical score.
- **Identity Attributes:** a bundle of attributes on each identity element, depth and velocity of the identity. Identity attributes add context to scores, enabling more informed risk assessments.
- **Synthetic Indicator:** indicators that help to detect synthetic or manipulated identities by pinpointing anomolies in the data, preventing bad actors from entering the system.
- **Verify SSN*:** confirms if an applicant's name, SSN and date of birth combination matches a legitimate database record. Early Warning® is one of the first and largest providers of SSN cross-checks.

*Verify SSN does not verify identities, eliminate synthetic identity fraud or reduce fraud. Verify SSN is only available to financial services organizations. Visit earlywarning.com/products to learn more.

After an applicant has completed the identity verification process, Predict New Account Risk provides a transparent view into their deposit account history and behavior. Based on these insights, you can customize the services and privileges you offer to align with your institution's risk appetite and protect against losses from first-party fraud and/or account default.



CLICK HERE TO LEARN MORE

Early Warning®

# Predict New Account Risk

**Predict New Account Risk provides the following outputs:**

- **First-Party Fraud Score 2.0 (available as of May 2024):** Predicts the likelihood that an applicant will commit fraud within nine months of account opening.

  Available as of February 2024, it leverages the latest machine learning technology and boasts an additional 19 fraud attributes, ensuring greater precision in risk determination. It delivers an estimated 63% improvement at predicting fraud compared to our original 1.0 model, providing a significant reduction in false positives and further minimizing friction in the customer experience.

- **Account Default Score**: Gives insights into how an applicant manages their accounts and predicts the likelihood of account abuse within nine months of account opening.
- **Key factors & summarized attributes:** Dozens of data elements enable more nuanced risk assessments—by providing insight into the behaviors from which the risk scores were derived. Examples include:
  - Number of fraud records identifying previous nefarious behavior
  - Number of days accounts have ever been in high-risk status
  - Average daily balances across owned accounts
  - Number of days an account has been open
  - Charge off loss amount across accounts
  - Number of account abuse records



CLICK HERE TO LEARN MORE

**With Verify Identity and Predict New Account Risk, you can expect greater precision to inform your decision-making. By leveraging unbeatable data and insights from Early Warning®, you're able to maximize approval rates while minimizing losses from synthetic or stolen identities, first-party fraud and account default.**


## Sources

1 *Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise*. Datos Insights, Feb. 2021
2 *What's Top of Mind for Fraud Executives: Trends, Scams and Talent*. Datos Insights, August 2022
3 *Trends in Fraud for 2023 and Beyond: Everything Old is New Again*. Datos Insights, Feb 2023
4 *2023 Identity Fraud Study: The Butterfly Effect*. Javelin, March 2023
5 *Market Trends in Fraud for 2022 and Beyond*. Datos Insights, Feb. 2022

## ABOUT EARLY WARNING

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial system with cutting-edge fraud and payment solutions for more than three decades. We are also the company behind Zelle®, and the soon-to-launch Paze℠, a wallet that reimagines e-commerce payments. Early Warning partners with more than 2,500 banks and credit unions to increase access to financial services and products and protect financial transactions. Learn more at www.earlywarning.com and connect on LinkedIn.