A GUIDE TO

Fight Synthetic Fraud with a Multi-Layered Detection Platform

DATAVISOR

Introduction

The most damaging threats are the ones you don't see coming. For financial institutions, synthetic fraud falls firmly into that category.

The Federal Reserve and **additional McKinsey research** have deemed synthetic fraud as the fastest-growing type of financial fraud in the United States, with an estimated impact of **$6 billion in annual losses**. What makes this type of fraud so threatening is that most traditional fraud tools fail to detect it. In fact, fraudsters can fly under the radar for months or even years before they "bust out" — suddenly maximize their credit and refuse to pay.

A report by ID Analytics found that, to further complicate matters, models designed to detect traditional fraudulent activities missed as much as 95 percent of synthetic fraud applicants.

That is a compelling reason for financial institutions to look beyond conventional fraud protection and explore the benefits of a comprehensive fraud platform that can fight synthetic fraud at the gate.

Synthetic fraud results in

$6 billion

in losses annually

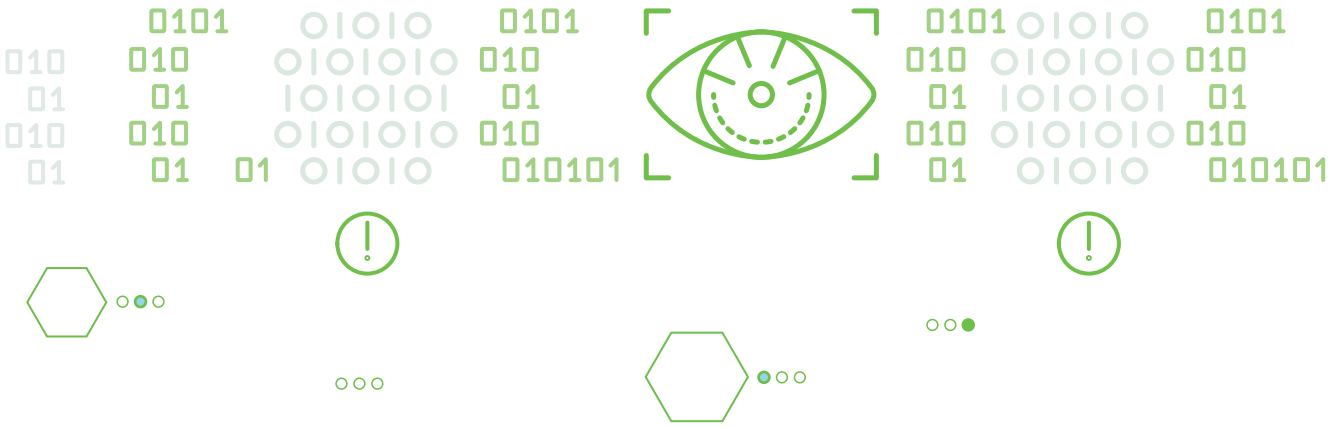
Traditional fraud detection models missed as much as 95% of synthetic fraud applicants.

What Is Synthetic Fraud and Why Is It Difficult to Detect?

Synthetic fraud occurs when scammers pair real customer data with fake information to create entirely new identities. These identities are then used to create fake accounts, apply for credit, and conduct transactions with no intention of repaying the debt, leaving financial organizations to cover the loss.

Thanks to advancements in fraud tools, banks have generally become more effective in fraud detection. But synthetic identity fraud creates a whole host of new challenges that evade conventional fraud protection measures. Because some pieces of data in a synthetic profile are legitimate, it's not easy to separate fake accounts from real ones.

McKinsey likens the problem to a hidden time bomb. The longer these fake accounts build up credit under the radar, the greater the potential losses to the lender. Once fraudsters reach their credit limit, repayments are halted and the scammer disappears. Since some of the personal information they provided is fake, it can be impossible to track them down and recoup the losses.

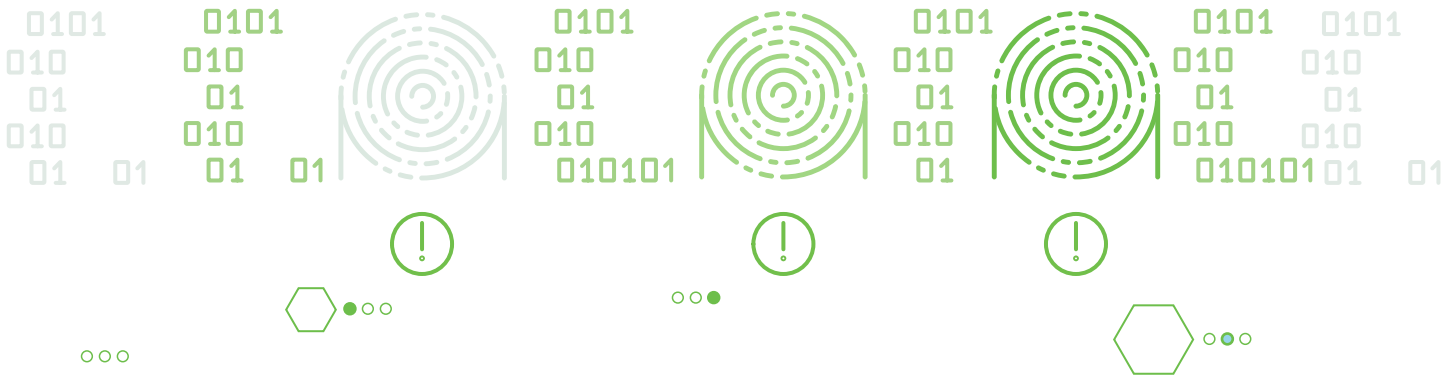


How Are Synthetic Identities Created?

Fraudsters can obtain personally identifiable information (PII) in a number of ways, then use that information to forge synthetic identities. **Experian reveals** that a Social Security number on the dark web costs as little as $1. Or, scammers can purchase full packages of personal data that include SSNs, addresses, phone numbers, names, and other details. Once a criminal has enough information about a person, they can use false information to fill in the missing links and commit financial fraud.

A **report from the Federal Reserve** notes that addresses near international airports or shipping facilities are common in synthetic identities. Many accounts may also share details like the same phone number or address while using different names and Social Security numbers. Some will even go as far as creating fake social media profiles and other documentation to further support their claims.

The goal of a synthetic identity is to appear valid so that activities are not picked up by fraud protection measures. In some cases, fraudsters will make small purchases and pay them off to build credit over time. As their credit portfolio grows, they have a better chance of getting approved for larger loans or lines of credit. Without proper fraud protection, financial institutions could be left with a large bill.



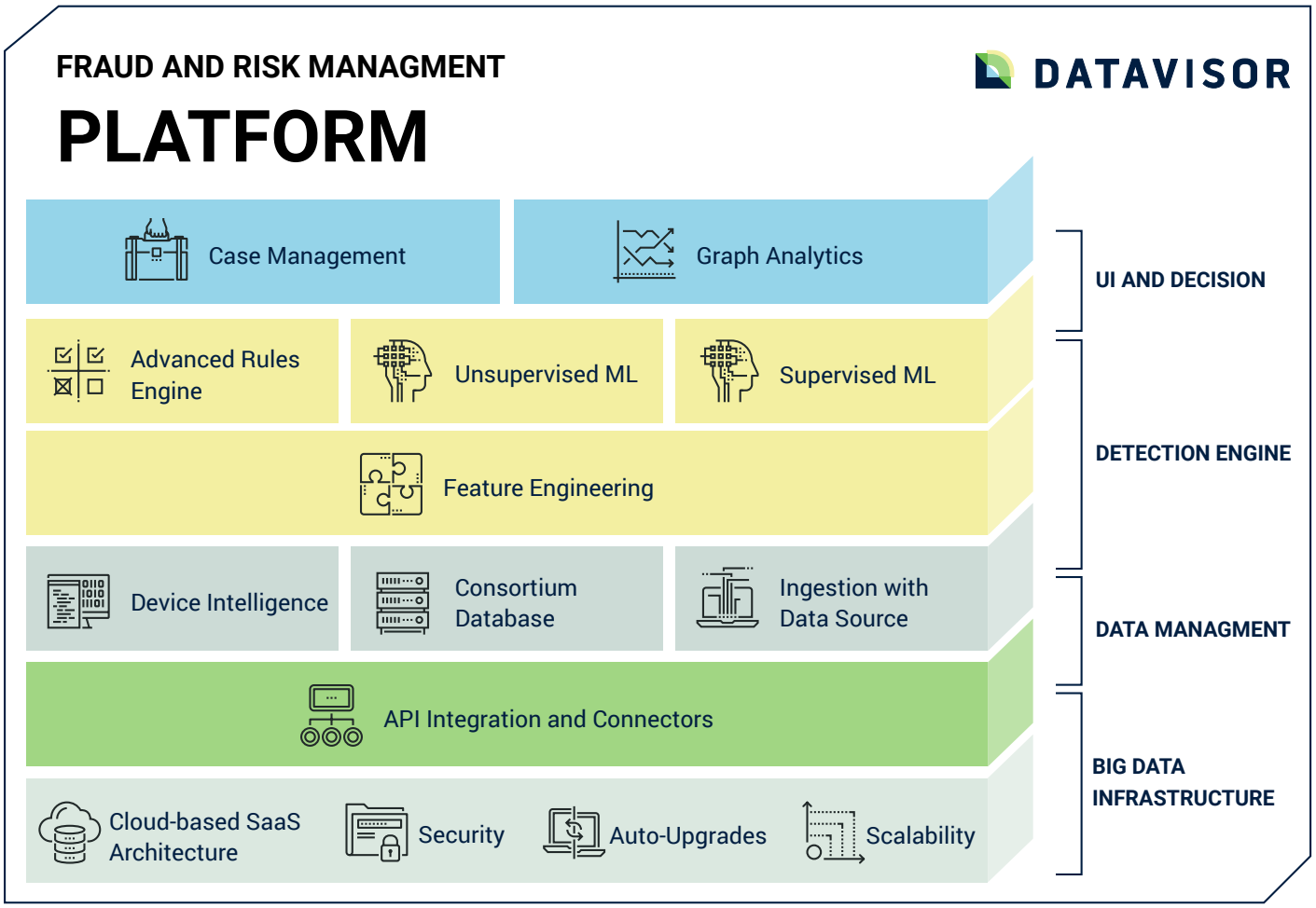
6 Common Characteristics of Synthetic Fraud

1. Repeated use of the same Social Security number
2. Accounts created using the same IP address
3. The same personal details being used to create multiple accounts
4. Credit file depth does not align with the customer profile
5. Addresses are near large airports or shipping destinations
6. Multiple authorized users on the same account

Taking a Multi-Layered Approach to Synthetic Fraud Prevention

The U.S. Federal Reserve warns against using a single piece of data to make decisions related to synthetic fraud. This is because not having a holistic picture could lead to higher false positives, which creates friction for good customers and ultimately leads to customer attrition.

DataVisor helps financial institutions to lead the good fight against synthetic fraud. With a comprehensive fraud protection platform, our layered approach provides a 360-degree view that leaves no stone unturned in the fight against fraud.



Machine Learning

Fraud is evolving as quickly as the tools used to fight against it. DataVisor leverages supervised machine learning (SML) to detect known fraud patterns, thereby helping organizations get the best from their existing data. Then, DataVisor's multi-layered approach goes a step further, using unsupervised machine learning (UML) to detect unknown and emerging fraud patterns in real-time with no need for data labels and constant model retuning. This allows financial organizations to evolve alongside threats and take a proactive approach to fraud detection. Leveraging both SML and UML, DataVisor provides comprehensive, best-in-class protection.

Device Intelligence

One of the telltale signs of synthetic fraud that often goes overlooked is the device that fraudsters are using to create mass fake accounts. For example, fraudsters could use emulators to control hundreds of devices and use botnets to create and register massive numbers of accounts and hide their tracks carefully by changing IP addresses or geolocations to avoid detection. DataVisor's device intelligence enables financial institutions to trace activities back to the device, providing another key piece of information that can help fraud teams identify synthetic fraud with greater confidence.

Feature Platform

DataVisor's Feature Platform automates the feature engineering process by producing thousands of auto-derived features based on user-imported raw data and mapped fields. These features are created using attributes—such as device IDs, user agents, email addresses and more–to provide more powerful features for advanced fraud detection. The platform can also recommend select features optimized for specific fraud types, enabling fraud teams to generate thousands of high-quality features in minutes.

The platform also offers fraud teams the ability to custom engineer unique features tailored to the specific organizational needs with just the UI or a bit of simple coding, with no additional need for IT support. This level of customization helps fraud teams infuse feature creation with their own internal expertise, optimizing fraud detection efforts accordingly.

Real-Time Graph Building and Deep-Link Analysis

Link analysis is a particularly helpful tool in the fight against synthetic fraud. DataVisor's real-time graph building and deep-link analysis capabilities enable organizations to build multi-dimensional connections among entities, groups, money flows, IP addresses, emails, and other attributes in real time to quickly uncover hidden patterns and empower contextual decisions.

One-click investigations connect new entities or events with previously detected fraud rings without the need for manual searches, speeding up detection and decision-making and improving accuracy at the same time. By visually highlighting fraudulent relationships in the network, DataVisor makes it easier for fraud teams to quickly see and act on synthetic fraud patterns as they emerge.

Case Management

DataVisor Case Management offers a centralized place for reviewers to efficiently assign and receive tasks, prioritize what to review, and analyze reason codes to accurately identify malicious activities. Teams can review detailed detection reasons, user profiles, and suspicious patterns, and benefit from investigating correlated accounts all together at the group level. Teams are empowered to make accurate bulk decisions that apply for the entire fraud ring, and significantly improve review efficiency with more cases reviewed in less time. The complete review and action histories are automatically recorded and fully traceable.

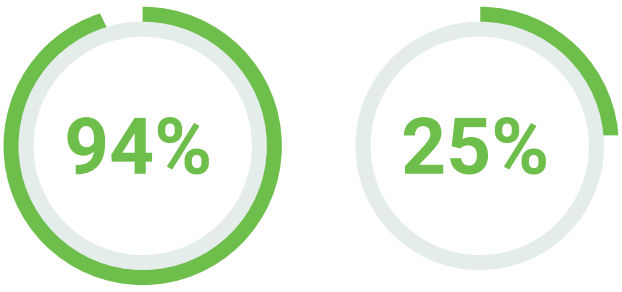
Global Intelligence Network

DataVisor's Global Intelligence Network leverages deep learning technologies to provide real-time, comprehensive digital intelligence culled from over 4.2 billion protected accounts and 1 trillion events across global online services in finance, E-commerce,marketplace, social, telecom, mobile gaming and other industries. This significantly enhances machine learning with fine-grained digital intelligence from rich digital fingerprints such as IPs, locations, email domains, devices, and more.

Success Metrics

How well does DataVisor's comprehensive fraud detection platform work in finding synthetic fraud. **Consider the case** of a leading U.S. credit card issuer that was struggling to reduce application fraud losses caused by third-party and synthetic fraud. The company was able to fully integrate the DataVisor solution within a matter of weeks and began to see results right away, as the new system was able to detect fraud immediately and provide real-time scores that were highly accurate.

With 94 percent detection accuracy and 25 percent additional fraud identified and captured, the credit card issuer was about to realize over $15 million in fraud loss savings and operational savings in a single year. At the same time, DataVisor was able to balance providing exceptional fraud detection and prevention with also providing a frictionless application experience for customers of the U.S. credit card issuer. By delivering on the promise of both cutting-edge fraud detection and seamless customer experience, the card issuer was able to conquer two of its major challenges with DataVisor's comprehensive solution.



Fight Synthetic Fraud with DataVisor

Synthetic fraud is one of the fastest-growing types of fraud in the United States, and financial institutions are tasked with finding ways to fight the rising tide of synthetic fraud in this sector. Traditional methods of fraud detection based on rules engines on their own are simply not up to the task of ferretting out synthetic fraud and stopping it in its tracks.

A multi-layered approach to fraud detection is needed to fight the increasing sophistication of synthetic fraud. DataVisor's comprehensive fraud detection platform takes a multi-layered approach that includes supervised and unsupervised machine learning, device intelligence, a feature platform that automates the feature engineering process, real-time graph building and deep-link analysis, case management, and a 4.2 billion-account-strong Global Intelligence Network.

To learn more about how DataVisor enables synthetic fraud detection at scale, **request a demo**.

See DataVisor Fight Synthetic Fraud.

DATAVISOR

REQUEST A DEMO

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform for enterprises. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR