DATAVISOR

Essential Guide to Using Machine Learning for Fraud Protection in Financial Services

How machine learning identifies suspicious transactions and applications in real time and stops financial fraud at the gate

Fraud crimes: $42 billion in 2019

Fraud is at a record high, with crimes racking up a collective $42 billion in costs in 2019. That money comes straight from companies' bottom lines.

Source: PwC Global Economic Crime Survey 2020

Financial Fraud Is on the Rise

Financial institutions have always been a favorite target for fraudsters, and their allure only seems to be increasing as more transactions, loans, and banking are done outside of the branch office.

As Banking Customers Go Online, So Do Fraudsters

In-person banking transactions are declining, while online transactions and credit applications are increasing. As a result, visual methods of verification are being removed and forcing financial institutions to rely on other means to verify customer identities. Many fraudsters are able to bypass typical security questions because they can find information on the dark web that allows them to fake the system.

By the time a customer becomes aware that they may be a victim of fraud, it's too late; the fraud has already occurred and the bank is left to pay the bill.

In a recent KPMG report on global banking fraud, more than half of respondents have experienced increases in external fraud, both in volume and in value. Specifically, these increases include identity theft, account takeovers, card not present fraud, cyber-attacks, and authorized push payment scams. What's more, more than half of respondents said they recover less than 25% of their fraud-related losses.

It's time for financial institution security and risk leaders to look beyond reactive fraud detection methods in favor of real-time fraud tools that can stop fraud at the gate.

In this guide, we'll review some of our insights based on multiple financial institution implementations and success stories that will help you assess, evaluate, and strengthen your fraud management strategy.

IN THIS GUIDE, YOU'LL RECEIVE:

+ A comprehensive set of criteria to evaluate your financial institution's fraud prevention vulnerabilities and needs
+ A closer look at the hidden costs of fraud detection and how to determine your return on investment (ROI)
+ What to look for to ensure your fraud solution can protect against the risk of a data breach and evolving fraud attacks
+ Resources needed to deploy your fraud solution
+ An overview of strategic business initiatives and how your fraud solution supports them

Consider the following criteria when evaluating solutions for financial fraud detection and prevention:

Protect Against Unknown Threats

Does the solution only safeguard against previously discovered fraud patterns and ongoing data training, or can it also detect new, unknown fraud patterns? In either case, what data does the tool need to detect fraud with high accuracy and fewer false positives?

Extensible Across Use Cases

Does the fraud detection tool apply to all channels and business areas where fraud could occur (e.g. new applications, new accounts, etc.)? Will the fraud tool address and support key business initiatives? Does the tool adhere to financial industry compliance requirements?

Total Cost of Ownership

Are there hidden costs to owning the solution, such as ongoing fraud modeling? How quickly will the new solution begin to add value to your financial organization? How much will the ROI timeline and total value offset the total cost of ownership?

Time to Implement

How long will it take to deploy the new solution? What are the costs and timeline of implementation, including training your employees on how to use the new tool?

Required Resources for Deployment

What does a successful deployment require from internal and external resources? Upon deployment, will the tool free up additional resources or remove responsibilities, such as administrative tasks?

Protect Against Unknown Threats

Financial fraud prevention isn't limited to known threats. Cybercriminals are continually evolving their attacks to bypass fraud prevention tools, seemingly as soon as new solutions are in place. This requires financial institutions to constantly update and refine their fraud models, keeping them one step behind fraudsters with no chance of getting ahead. A better approach is to prioritize tools that will evolve with the fraud landscape and scale your detection and prevention efforts without constant retraining.

Proactive Fraud Prevention

Compared to traditional reactive models, proactive fraud prevention does not rely on traditional data labeling and ongoing data training. By being proactive, financial institutions can mitigate losses simply by stopping fraud in its tracks instead of continually retracing their steps and trying to recoup losses.

Large-Scale Coordinated Attacks

Traditional fraud tools that only review isolated behaviors are missing the large-scale coordinated attacks that make up a sizable portion of financial fraud. Today's fraudulent financial activities aren't conducted by petty thieves looking for personal financial gain. Modern technology has made it easier than ever to organize large crime rings and coordinate attacks using emulated devices, money mules, and even machine learning. Viewing these activities on a broader scale gives banks a clearer picture of fraud that may otherwise seem authentic when viewed case by case.

Bulk Decision Making

The time it takes to create an account and complete a fraudulent transaction is narrowing. Now more than ever, financial institutions must be prepared to take immediate action to prevent fraud from occurring. The ability to make bulk decisions allows FIs to take action on groups without the need to retrain data models.

Using machine learning, it's possible to see emerging attacks forming and then stop them before they launch, no matter how new or unique the techniques may be.

-Yinglian Xie, CEO and Co-Founder, DataVisor

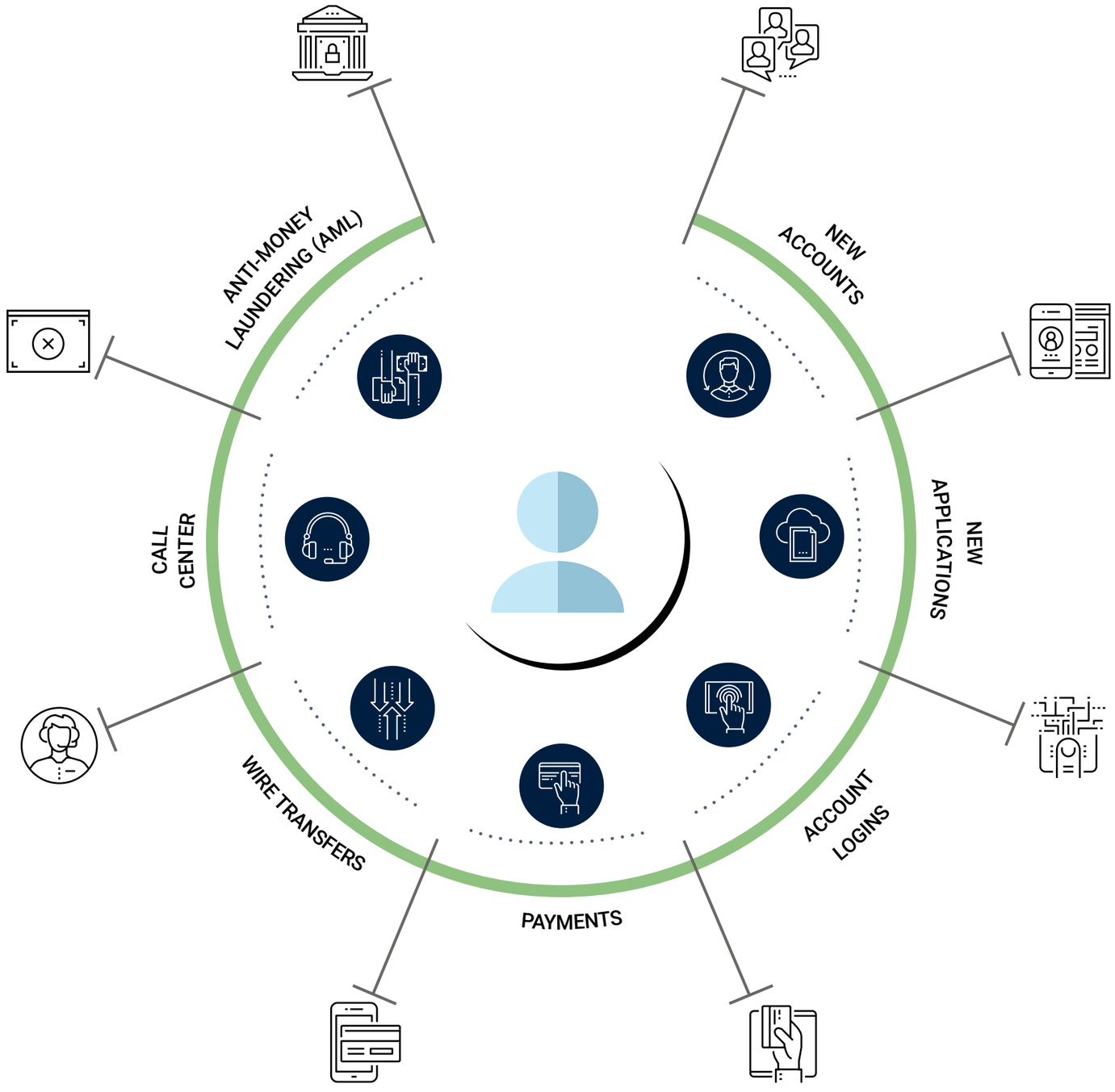
Extensible Across Use Cases

Financial institutions' variety of services and channels leave them vulnerable to fraud in many ways. Like other industries, financial companies are increasingly turning to the omnichannel to connect with and serve their customers, from website live chats to call centers to social media and more. A strong fraud detection strategy must take each of these use cases into account and address fraud across the enterprise for the best protection.

One Tool - Any Type of Fraud
Continuous Customer Lifecycle Protection

A comprehensive fraud detection solution addresses multiple potential stages of the customer account lifecycle where different types of fraud can occur including:

- Fake accounts
- Application fraud
- Account takeover
- Payment fraud
- Wire transfer fraud
- Call center fraud
- Internal fraud
- Money laundering



Total Cost of Ownership

The total cost of ownership refers to all upfront costs and ongoing expenses of owning a solution over time. These costs include but are not limited to the initial purchase price, annual licenses and user seats, training costs, infrastructure investments, operating costs, customer support, and user training.

Initial Investment

Starting a new fraud solution requires an upfront investment, including infrastructure, hardware, and the cost of the platform itself. For rules-based solutions, financial institutions must take into account the cost of collecting the appropriate data, creating fraud models, and training and testing the data.

For on-premise solutions, you'll need to take into account the required hardware, as well as the IT expertise needed for deployment and ongoing maintenance. If you choose a cloud-based solution, upfront costs may include computational bandwidth and per-user licensing.

Ongoing Costs & Maintenance

License renewals are often the biggest ongoing cost for cloud-based solutions that don't require rules training and extensive data labeling. If you're deploying an on-premise solution, factor in the costs of server maintenance, IT personnel, and physical data center security.

For supervised machine learning, you'll also need to allocate resources for ongoing data training. Rules-based platforms typically need re-training every 3-6 weeks. For every retraining session, data models go through lengthy variance and validation. As you add or remove services or channels, you'll also need to retune your data models.

Unsupervised machine learning (UML) holds an advantage over supervised machine learning when it comes to ongoing costs. Because UML is self-adapting, many of the data training costs are eliminated.

Support

Ongoing vendor support can vary in cost and scope. One thing to ask your solutions provider is the cost of ongoing support and what the cost includes. It's also a good idea to find out how support is delivered (e.g. live chat, web resources, phone) and whether this level of support fits your needs.

User Training

Onboarding new users is typically considered an upfront cost, but new hires will also need to learn how to use your fraud prevention tools. A user-friendly interface and the ability to avoid ongoing data training and retuning can help to shorten the learning curve and allow users to ramp up quickly.

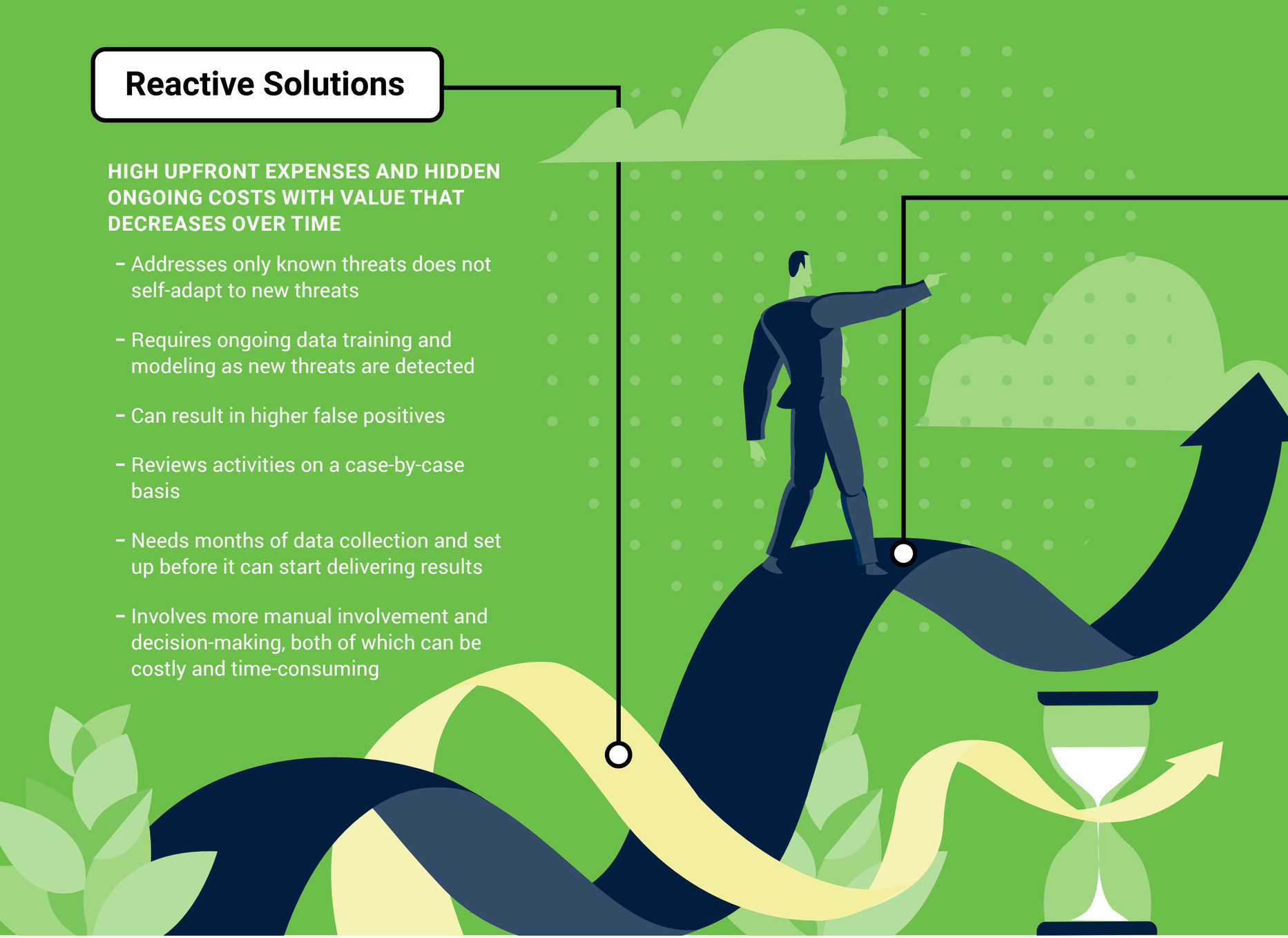
Using fraud detection as a path to increase revenue is a smart growth strategy. By reducing losses associated with fraud, you're automatically adding to your bottom line.

-Claire Zhou, Product Marketing Manager, DataVisor

Reactive Solutions

HIGH UPFRONT EXPENSES AND HIDDEN ONGOING COSTS WITH VALUE THAT DECREASES OVER TIME

- Addresses only known threats does not self-adapt to new threats
- Requires ongoing data training and modeling as new threats are detected
- Can result in higher false positives
- Reviews activities on a case-by-case basis
- Needs months of data collection and set up before it can start delivering results
- Involves more manual involvement and decision-making, both of which can be costly and time-consuming



Proactive Solutions

HIGH VALUE THAT BUILDS OVER TIME

+ Doesn't require data labeling or training
+ Detects fraud across the enterprise in real time
+ Reviews all data and transactions holistically to detect large-scale patterns
+ Enables bulk decision making with greater confidence and fewer false positives
+ Can be deployed on-premise or via the cloud
+ Predictable costs that scale with your financial institution
+ Integrates with existing data architecture and other third-party solutions

Time to Value

Time to value refers to the time between when a solution is selected and purchased to the day the solution begins to deliver value. This window of time can vary drastically between solutions, depending on how much data training, labeling, and modeling is required, the ease of use, and user adoption rates. The shorter this window, the faster your organization will see a benefit from the new implementation.

Influence the time to value in the following ways:

Proof of Concept

Map out how you want your fraud detection tools to look and function. From there, you can set up a pilot testing program across a small group of users before deploying to the enterprise. This allows you to catch and fix any errors early and see what works or doesn't work before training users.

Platform Deployment

Walk through what the deployment process will look like: Who is involved? What are the costs associated with deployment? How long will it take? What obstacles might you encounter? For faster deployment, a cloud-based solution is ideal because it won't require additional hardware or IT expertise to get up and running.

Onboarding & Training Users

One of the biggest time investments during deployment is adding, onboarding, and training users. The initial process of adding users can be a tedious task. Look for a vendor that offers bulk enrollment to save time and costs. If this isn't an option, you may need to allocate IT man-hours and other resources to this step.

Training will also be a critical deployment step. Though DataVisor solutions do most of the heavy lifting when it comes to detecting and preventing fraud, users need to understand why red flags appear and how to respond to them.

A fraud detection solution should include an easy-to-use API or SDK to integrate with existing systems quickly. You should be able to deploy the fraud prevention solution where needed, which could be in the cloud, on-premises, or on both.

-Hao Li, Head of Customer Success, DataVisor

Resources for Deployment

Fraud detection and prevention platforms work independently for the most part, but they require resources and hands-on involvement during the initial deployment. You'll need to consider the timeline, personnel, data infrastructure, and other resources to build a strong foundation that will deliver optimal results for your organization. Consult with your vendor to learn more about what's required for the initial setup.

Deploying a financial fraud solution requires the following resources:

Data & Hardware Infrastructure

Different solutions will require different hardware and types of data for implementation. Work with your vendor to determine your unique requirements, as well as the necessary IT expertise to complete the deployment.

Internal Fraud Team

Having your own internal fraud team designed to monitor and manage your new platform allows them to become the go-to experts. This team will be responsible for training new users, responding to suspicious activities, and tweak and refine your fraud strategy and models over time.

Data Scientists

Part of your internal fraud team should include data scientists that can help make sense of the data you collect and analyze. Their expertise allows you to make more sense of how your fraud tools are working and the ROI they deliver.

Your ability to identify fraud is entirely dependent on whether you have the infrastructure in place to collect and compile relevant signals from various data sources.

-Fang Yu, CTO and Co-founder, DataVisor

DataVisor's Comprehensive Detection Platform

Financial fraud takes many forms and occurs on a variety of channels across the enterprise. DataVisor delivers a comprehensive fraud and risk management platform that protects FIs from all types of fraud.

DEVICE INTELLIGENCE:

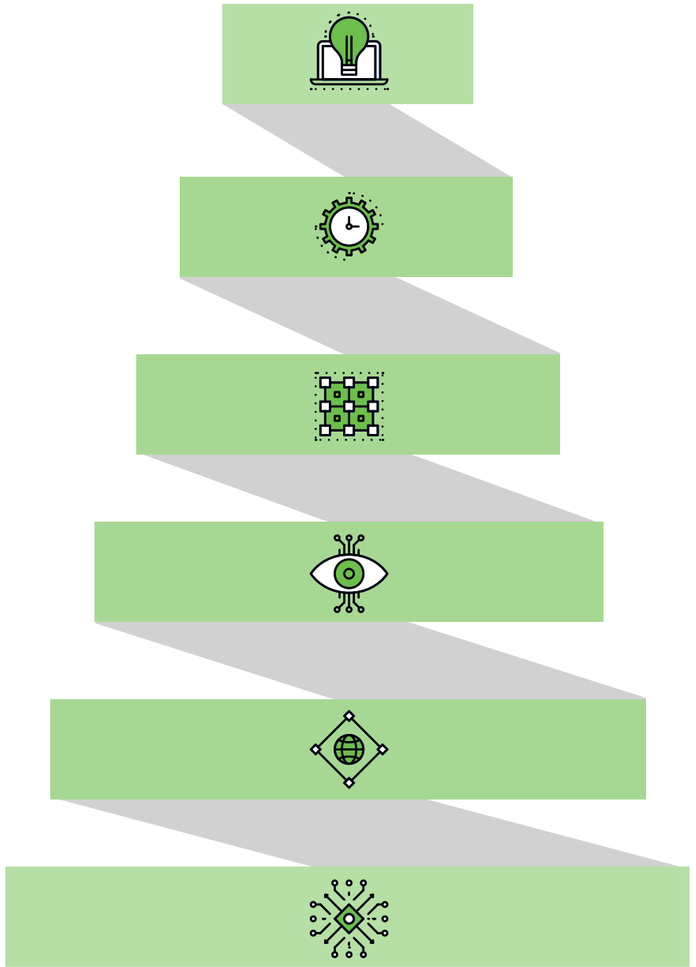
The DataVisor platform leverages device fingerprints to stop fraud before it occurs. Financial institutions can detect fraud on emulated or spoofed devices and prevent transactions from being completed.

REAL-TIME OPERATIONS

With real-time insight into known and unknown threats, risk leaders can take immediate action on suspicious activities without the need to hand off responsibilities to IT. DataVisor assesses activities across the entire customer lifecycle in real time to detect patterns and new threats.

UNSUPERVISED MACHINE LAERNING

Without the restrictions of known threats and data labeling upon which supervised machine learning depends, DataVisor can detect hidden fraud patterns and evolving attacks. This allows financial institutions to be proactive in locating and stopping fraud instead of trying to do damage control after the fact.



ANALYTICS AND REVIEW

Advanced analytics takes a visual approach to showing why certain activities have been flagged as suspicious and how they relate to potential threats. Leaders can quickly review data and make bulk decisions with confidence, resulting in fewer false positives.

GLOBAL INTELLIGENCE NETWORK

DataVisor's Global Intelligence Network includes data from more than 4.2 billion accounts from around the world, including IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains and more. This data pairs with the machine learning algorithms to enhance overall detection.

CENTRALIZED INTELLIGENCE

Taking a centralized intelligence approach to fraud allows you to use the same tools for multiple use cases. Historically, financial institutions attempt to centralize data using repositories and data lakes, but these attempts are far from perfect. A better way to accomplish data centralization is to use derived attributes and calculated data rather than sharing just the data itself. Data that exists in silos make it harder to locate and deter fraud across the enterprise.

The DataVisor Advantage

DataVisor takes a unique approach to financial fraud detection and prevention through the use of unsupervised machine learning. Without the restrictions of rules-based systems, the platform can not only protect against known threats, but also identify and prevent new attacks and patterns before they can create financial and reputational damage.

Here's how DataVisor holds an advantage in each of the above criteria:

Protect Against Unknown Threats

ML-DRIVEN PLATFORM

Bypassing the need for data training, labeling, and on-going retuning, UML looks at data on a holistic level to detect large coordinated attacks and unknown patterns. The platform collects and analyzes data in real time so financial institutions can take action quickly and mitigate threats before they crash the gate.

BULK DECISION MAKING

Because DataVisor looks for larger patterns beyond individual cases, fraud teams can make bulk decisions to decrease response time. This not only reduces internal operating costs, but also helps to prevent fraud from slipping through the cracks.

Extensible Across Use Cases

CENTRALIZED DATA REVIEW

DataVisor works across the enterprise to view data on a holistic level in real time. The same fraud tools are being used on all channels to prevent fraud from slipping through the cracks.

IMPROVED VISIBILITY & CONTROL

Because DataVisor can be deployed throughout the organization, fraud teams gain better visibility and control over fraud detection. Expect a higher accuracy with fewer false positives and deeper insight into your overall fraud profile.

Total Cost of Ownership

MORE VALUE OVER TIME

DataVisor eliminates the need for historic labeling, time-consuming data training, and ongoing retraining, giving financial institutions more value almost immediately and over time.

NO HIDDEN COSTS

Traditional solutions are ripe with hidden costs, but DataVisor's proactive approach helps to keep costs to a minimum. Tools that are self-adapting and require less retuning automatically deliver a lower total cost of ownership.

Time to Value

EASY INTEGRATION

DataVisor works with your existing data architecture for a faster, seamless integration. We follow a three-phase process to simplify implementation and allow you to start seeing the benefits as soon as possible:

1. **Integrate data.** Start with a few samples to test the data quality, then stream data to DataVisor's integration endpoint.
2. **Implement DataVisor's detection system.** Review DataVisor's detection results and reason codes, then create systems to parse in and take actions on the results.
3. **Start using results.** Define the criteria for automated actions based on DataVisor's detection results, and learn how to leverage the case management consoles to streamline responses and boost efficiency.

FROM ZERO TO ROI WITHIN TWO WEEKS

The streamlined integration and intuitive interface contribute to a shorter onboarding and user training period. Upon implementation, financial institutions may start seeing an ROI in as little as two weeks.

Resources for Deployment

SIMPLIFIED IMPLEMENTATION

For deployment, financial institutions will need to provide basic data fields and user events, and the DataVisor team will do the rest. If you've selected a cloud-based solution, implementation is shortened because additional hardware is not required.

DEDICATED SUPPORT

DataVisor includes ongoing support to help financial institutions get the most from their investment. Receive a dedicated Technical Account Manager that provides support 24/7 during and after deployment without expensive support contracts.

DataVisor analyzes all customer touchpoints and data in real time to provide thorough defenses against financial fraud.

CUSTOMER TESTIMONIAL

DataVisor's comprehensive fraud solutions put a stop to financial fraud and prove that crime doesn't pay.

DataVisor takes your financial institution out of the chore of constantly retraining and fine-tuning fraud models so you can deliver better service to your customers and stamp out fraud before it occurs. A scalable platform works in the background to reduce friction for good customers and identify known and unknown threats, including large-scale coordinated attacks that can easily look authentic when viewed individually. Our real-time, holistic approach to identity fraud, account takeovers, application fraud, money mules, and money laundering across the enterprise allows financial institutions to prevent reputational and financial damage instead of trying to repair damage after the fact.

"DataVisor's machine learning solution is the most critical component of our fraud defense as we grow in the digital space, helping us minimise customer friction while defeating fraud risk."

Richard Cooney,
Director of Fraud Strategy at Axcess Financial

Put your trust in DataVisor and let us help you protect what matters most. Request a demo today.

REQUEST A DEMO

DATAVISOR

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