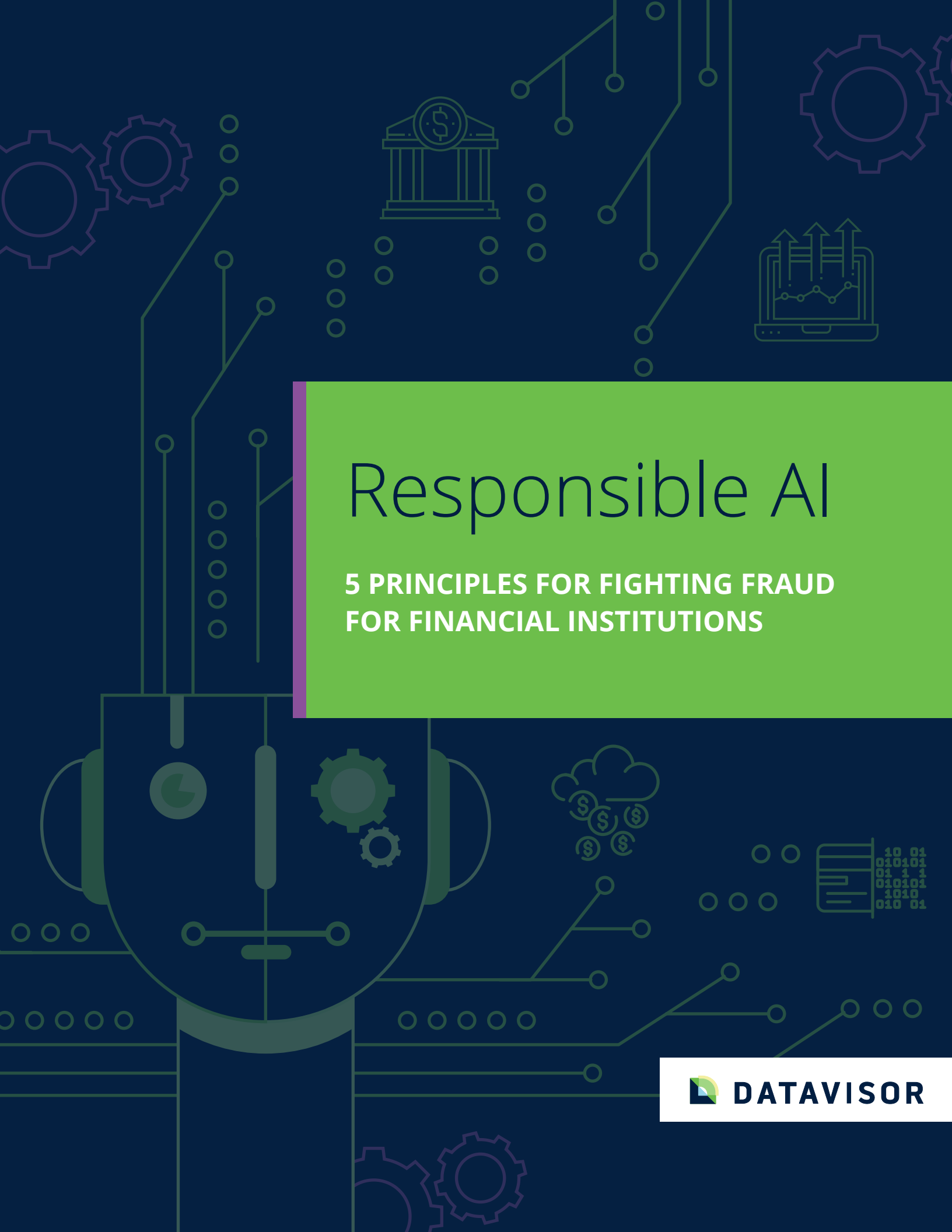


Responsible AI

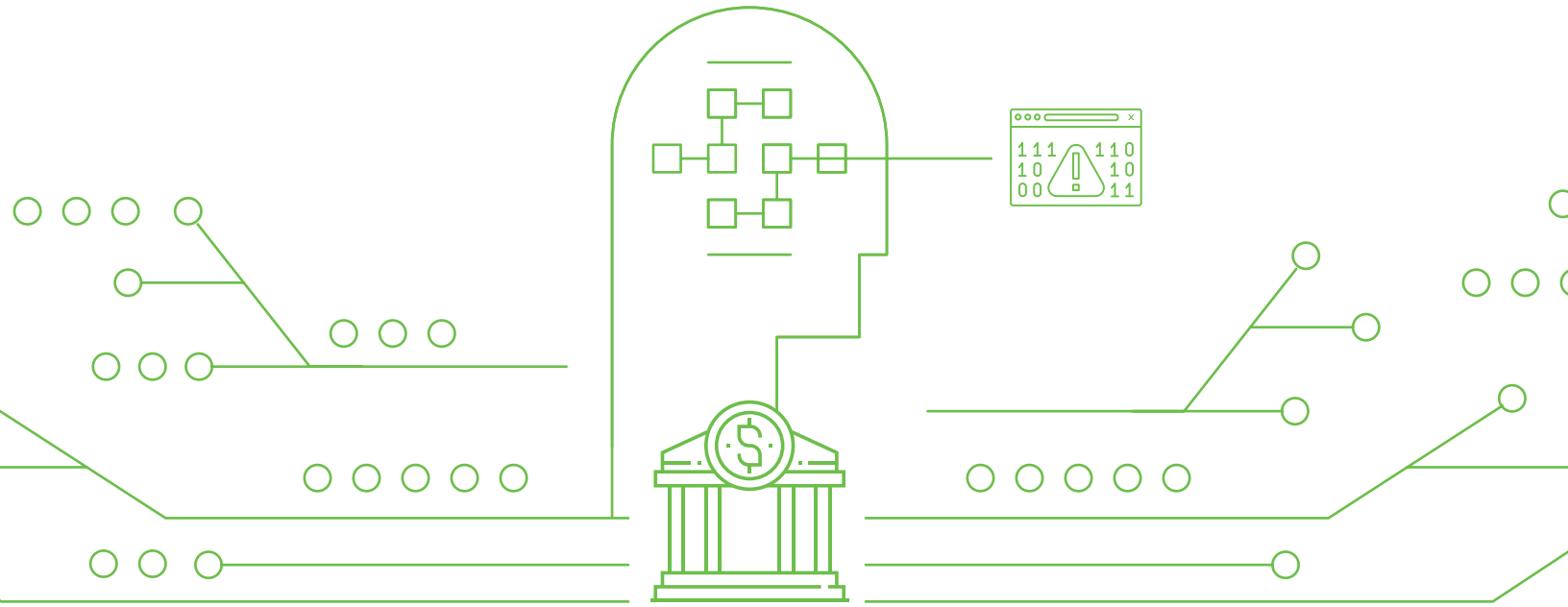
5 PRINCIPLES FOR FIGHTING FRAUD FOR FINANCIAL INSTITUTIONS

DATAVISOR

Introduction

Artificial intelligence (AI) is increasingly making its way into the financial sector, offering financial institutions more tools to scale their fraud and risk management programs. However, as with any new technology, it's important to be able to trust the results that AI-powered technologies deliver, as well as understand how they work and whether they align with corporate ethics and values.

> This is the foundation of Responsible AI—the practice of ensuring AI is leveraged in a safe and meaningful way while protecting the financial institution's brand and its customers. When used with a focus on responsibility, financial institutions stand to improve customer relationships, lower their risk of discriminatory decision-making, and reduce the threat of regulatory or reputational damage.



5 Principles of Responsible AI

The five principles of AI—fairness, privacy, transparency, reliability, and accountability—should align with technical and people processes. By assessing ethical risks on an ongoing basis, FIs can work to remove as much bias as possible from their fraud and risk management programs.

1. Transparency

In the past, building transparency into fraud detection models often meant creating a custom solution from scratch. Today, fraud detection models built on open platforms make it easy to consolidate and enrich data upon which models can be built, evaluated, and deployed.

Reason codes then indicate why certain activities are flagged as fraud, how they relate to other users or behaviors, and provide more context into decision making to help avoid bias. Transparent AI gives organizations more insight into when and why AI algorithms make mistakes, which enables them to make adjustments to their models.

2. Mitigating Bias by Nature

Data bias and algorithm fairness are imperative to ensure responsible AI, and are misconceived as being costly endeavors to implement. The reality is that bias reduction techniques can be applied during AI model training to improve fairness. The first step is to define fairness objectives and requirements, and then look for signs of bias in the datasets.

It is here that unsupervised machine learning shines. Because these models are looking at suspicious clusters and linkages among various entities rather than looking at individual transactions, unsupervised machine learning is more effective in eliminating bias in the data. For example, unsupervised machine learning won't look at gender or specific zip codes that have a high priority toward the target. Instead, it treats all zip codes and genders the same, only focusing on detecting the suspicious clusters and linkages. A male or female value won't affect the model because the model is not based on any prior labels.

3. Explainability

Explainability affects all parties involved in the financial institution ecosystem, including customers, fraud teams, regulatory bodies, and stakeholders. For this reason alone, the importance of this element of Responsible AI cannot be overstated.

For years, AI has seemingly lived in a black box, where outcomes were prioritized above the how, what, and why. But for financial institution, a black box solution does not offer confidence in how fair and inclusive decisions are made. Rather, financial institutions require a solution that produces decisions that are understandable, transparent, and fair so they can hold their teams accountable for the outcomes and ensure safety and privacy for their customers.

4. High Confidence Results

Reliability is a driving factor behind every fraud solution. Users need to be able to trust the results, but Responsible AI is somewhat erroneously believed to compromise model performance.

The truth is that some fraud models may sacrifice a small percentage of performance in favor of fairness, but improved explainability that supports any red flags makes up for that easily.

5. Safety and Privacy to All Users

The safety, security, and privacy of user data are heavily scrutinized, and for good reason. The effects of a data breach can be costly to financial institutions, not just in terms of stolen funds, but also in terms of the expense of fixing errors, filling gaps in defense, and repairing reputational damage. What's more, recent research shows that an organization's likelihood of a data breach within two years is 31% greater than it was in 2014.

Any new solutions being brought into the fraud and risk management mix should be thoroughly examined for potential gaps in safety, security, and privacy. These solutions should also be able to leverage a combination of omnichannel data (e.g. call centers, web, login events, mobile app, etc.), client data input, and consortium data to detect more fraud in real time.

DataVisor's Approach to Responsible AI

DataVisor believes that Responsible AI isn't just part of an efficient and robust fraud and risk management program, it's also the right thing to do.

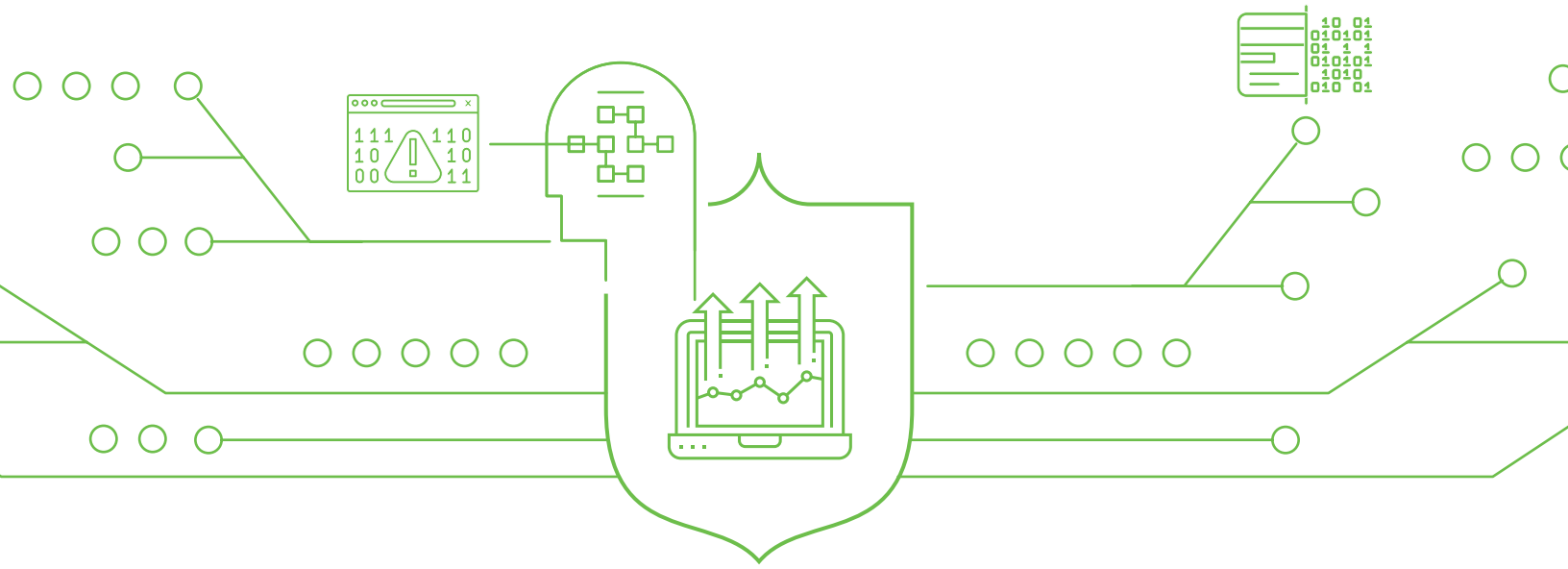
DataVisor's multi-layered approach to fraud helps financial institutions prioritize responsible AI principles in a scalable, efficient manner without compromising the effectiveness of its fraud detection and prevention. Here's how:

- **Transparency:** An open platform provides users with the ability to process data, create features and build, evaluate, compare, and deploy models.
- **Mitigating Bias by Nature:** DataVisor leverages unsupervised machine learning models, which do not depend on historical data and labels to make decisions. That means DataVisor captures evolving fraud by detecting abnormal behaviors among various entities, thus eliminating bias by nature.
- **Explainability:** DataVisor fraud detection results come with easy-to-understand reason codes to build confidence and ensure fairness and explainability.
- **High Confidence Results:** Models offer a 90%+ accuracy and less than 1% false positives.
- **Safety and Privacy:** DataVisor solutions can be deployed across public cloud, private cloud, and on-prem technologies to meet the security requirements of any financial enterprise.

Fair, ethical decisions are a cornerstone of the financial sector, ensuring legitimate customers have access to the financial services they need without regard to race, age, gender, and other factors. Automation can help to make fair decisions, but only if a fair framework allows it.

DataVisor's multi-layered approach to fraud detection is designed to inherently uphold the five Responsible AI principles so that bias doesn't get in the way of fraud-related decision making. What's more, because the platform takes a holistic approach to fraud, DataVisor can not only make a Responsible AI pursuit attainable, but also execute it with efficiency and confidence.

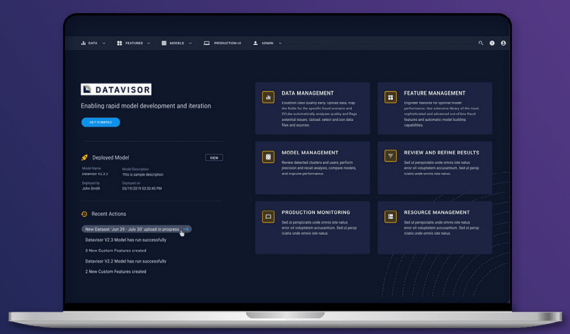
Learn more about how DataVisor upholds Responsible AI principles while fighting fraud; **request a demo**!



See fraud prevention with Responsible AI in action today.

DATAVISOR

GET 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