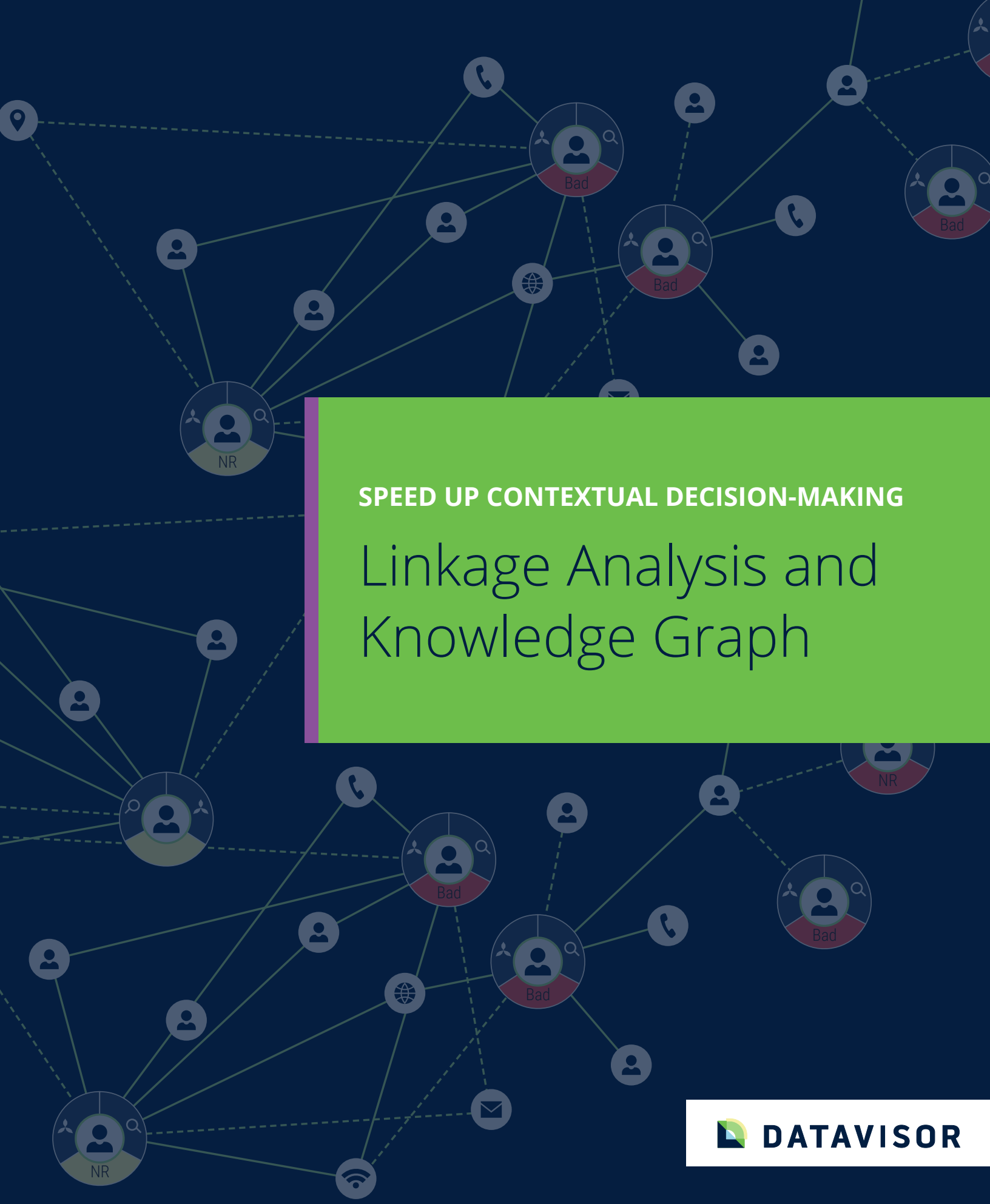


SPEED UP CONTEXTUAL DECISION-MAKING

Linkage Analysis and Knowledge Graph

DATAVISOR

Table of Contents

Introduction

Context is at the heart of every decision you make. You cannot effectively answer questions and make decisions without knowing why you're choosing that answer. AI technologies can help solve the problem of making data-driven decisions, but you still require context into how AI arrived at a particular solution. That's why DataVisor's Knowledge Graph is such a valuable component of its AI-driven fraud prevention solutions.

In times past, fraudsters set the pace for fraud detection and prevention technology. They found creative ways to carry out their activities and leave companies scrambling to catch up and adapt their strategies to fill the gaps. It was a never-ending game of cat and mouse, and too often, the mouse got away with enough cheese to cause serious financial damage to the cat's bottom line.

Today, new threats are evolving faster than ever. Gone are the days when fraudsters carried out their activities in a linear, single-channel fashion for their own personal gain. Many fraudsters are no longer acting alone, but rather as part of organized crime rings whose activities are interconnected and therefore might evade fraud detection on an eye-to-eye level.

Effective modern-day fraud prevention requires a holistic approach with a bird's eye view into the context of potential fraud. Seeing connections between activities helps to uncover patterns that may appear normal or unrelated on the surface, allowing teams to capture more fraud and take faster action. DataVisor's Knowledge Graph provides visual insight into potential fraud activities to deliver a better understanding into the context of activities. For more confident decision-making, linkage visualization is a critical piece in your fraud prevention strategy.

> Fraudsters often act as part of the organized crime rings whose activities are interconnected and hard to detect without a way to link activities. DataVisor's Knowledge Graph provides visual insight into potential fraud activities to deliver a better understanding into the context of activities.

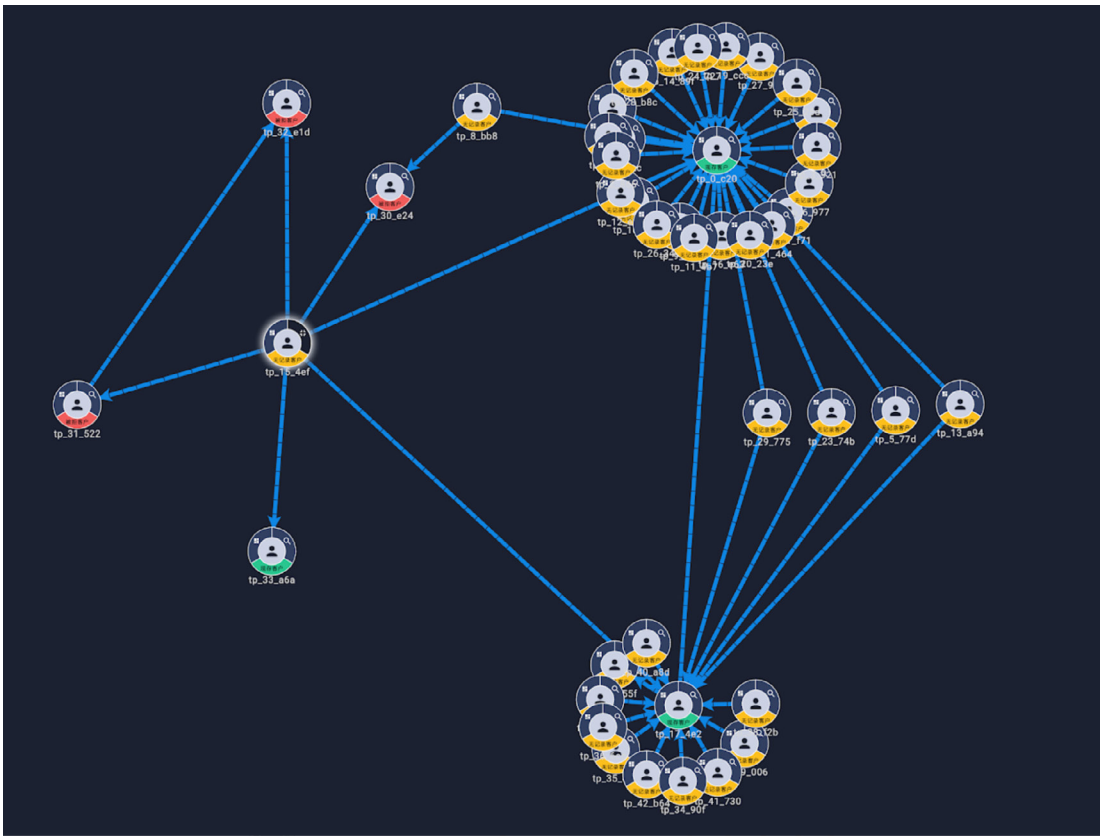
1 Why Knowledge Graph Is the Future of Fraud Prevention

Imagine you are an online retailer offering an attractive incentive for new customers. You quickly notice 100 new customer accounts that take advantage of your incentive. On the surface, you might be elated to see your advertising working, as new customer accounts potentially mean more loyal customers moving forward.

But if you dig a little deeper into the context of those new accounts, you might find that the majority were created using the same IP address or device, or share some of the same personal identifiable information (PII). Suddenly, you realize that someone is trying to commit fraud, and without a way to quickly shut them down, your business may have to foot the bill.

Scenarios like that are why Knowledge Graph is useful in fraud detection. While fraud tools investigate actions, Knowledge Graph works to discover how those actions might be related.

> DataVisor analyzes links between activities and displays them in a visual Knowledge Graph. It augments omnichannel data, rather than relying on siloed data that may bypass traditional fraud detection tools. The Knowledge Graph is automatically generated using AI technology to speed up the fraud review process.



Knowledge Graph of money laundering activity in action

As a result, Knowledge Graph gives you a holistic view of your customers by connecting the dots between them. Users can conduct contextual fraud analysis and make faster decisions based on a better understanding of how activities are related.

2 Knowledge Graph Use Cases

> Knowledge Graph can be used across a variety of industries to uncover fraud patterns in real time. As an essential tool in fraud management, Knowledge Graph enables teams to review links between multiple customers and activities and take bulk actions to eliminate large threats.

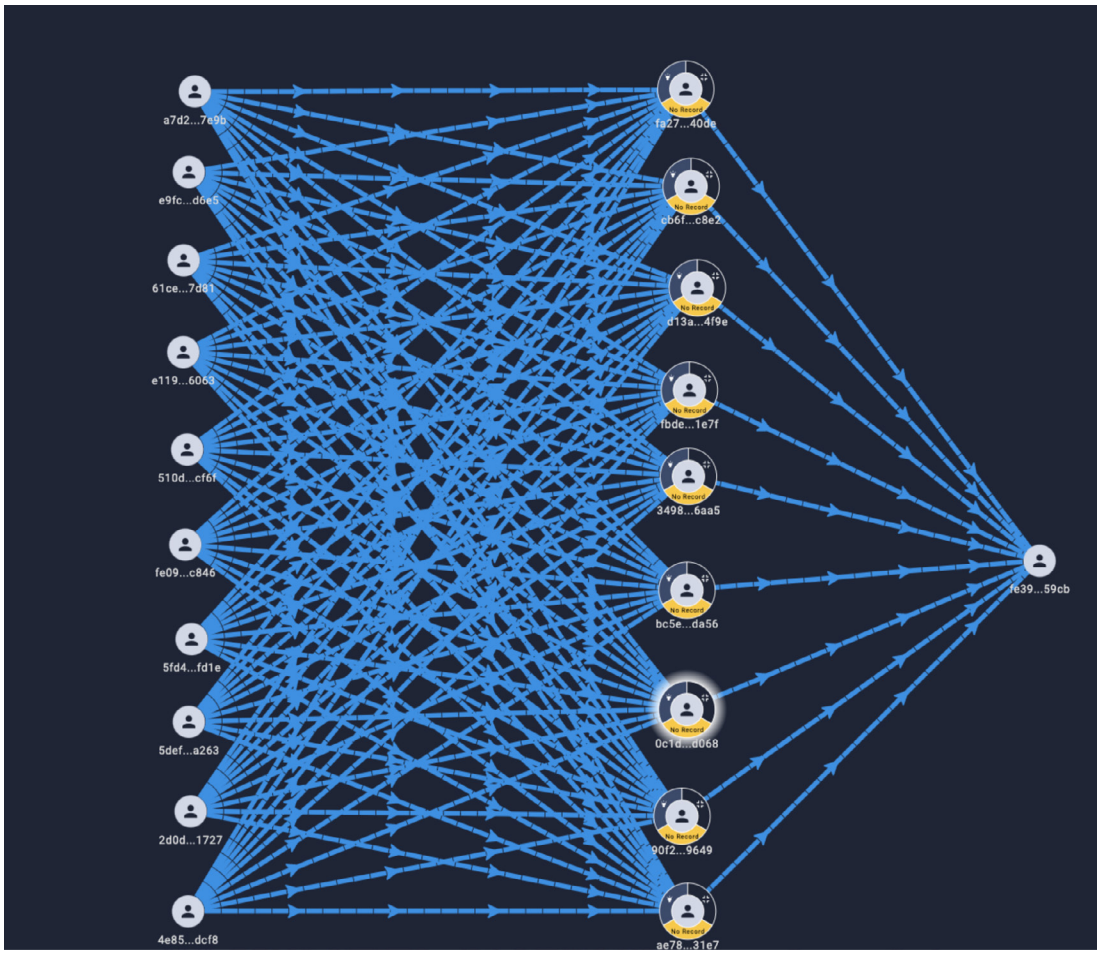
Fraud Detection

Knowledge Graph detects multiple types of fraud, including application fraud, transaction fraud, identity fraud, account takeovers, and even internal fraud. The contextual fraud analysis approach looks beyond isolated activities to see the "big picture" behind them. The result is a faster path to fraud detection and prevention, allowing companies to take action sooner and mitigate the negative effects of fraud.

AML and KYC

Complex money laundering rings are hard to detect because many crime rings employ money mules that may be unaware they're doing anything wrong. On the surface, their activities may seem legitimate. Gaining a holistic view into activities can help teams uncover money mule and money laundering activity faster.

Even with Know Your Customer (KYC) processes in place, identity theft and synthetic identities can go unnoticed. Knowledge Graph helps to discover multidimensional connections that can slip through manual review methods.



Knowledge Graph of mule network in action

Investigation

Knowledge Graph offers intelligent fraud review and fraud case management. With all detections imported from various systems into a central platform, fewer acts of fraud can slip through the cracks. You can customize linkages based on any dimensions, including exact/fuzzy matches and strong/weak links. Boost investigators' efficiency with the AI-powered interface to spot emerging attacks in real time.

3 Knowledge Graph Differentiations

> DataVisor's breadth and depth in uncovering fraud patterns, combined with intuitive fraud analysis and real-time functionality, separates it from other fraud detection and prevention solutions.

Some of the key characteristics that make DataVisor stand out from the crowd are:

- High level of scalability
- Automatic identification of suspicious entities
- Flexible integration that facilitates rapid actions

High Level of Scalability

As your business grows, existing fraud prevention tools and teams will need to adjust to accommodate increased demand. AI-driven Knowledge Graph offers high scalability and real-time computation, allowing it to accommodate any size demand on an ongoing basis.

DataVisor's Knowledge Graph is the most scalable solution compared with other analysis tools. It can build hyper-scalable graphs in real time across billions of events as data comes in, thanks to a hyper-modern data infrastructure and distributed systems. Graphs, entities, and linkages are stored and calculated over a distributed network with the ability to achieve 10K+ QPS with real time graph updates. DataVisor's Knowledge Graph can process several years of data, while other solutions cannot.

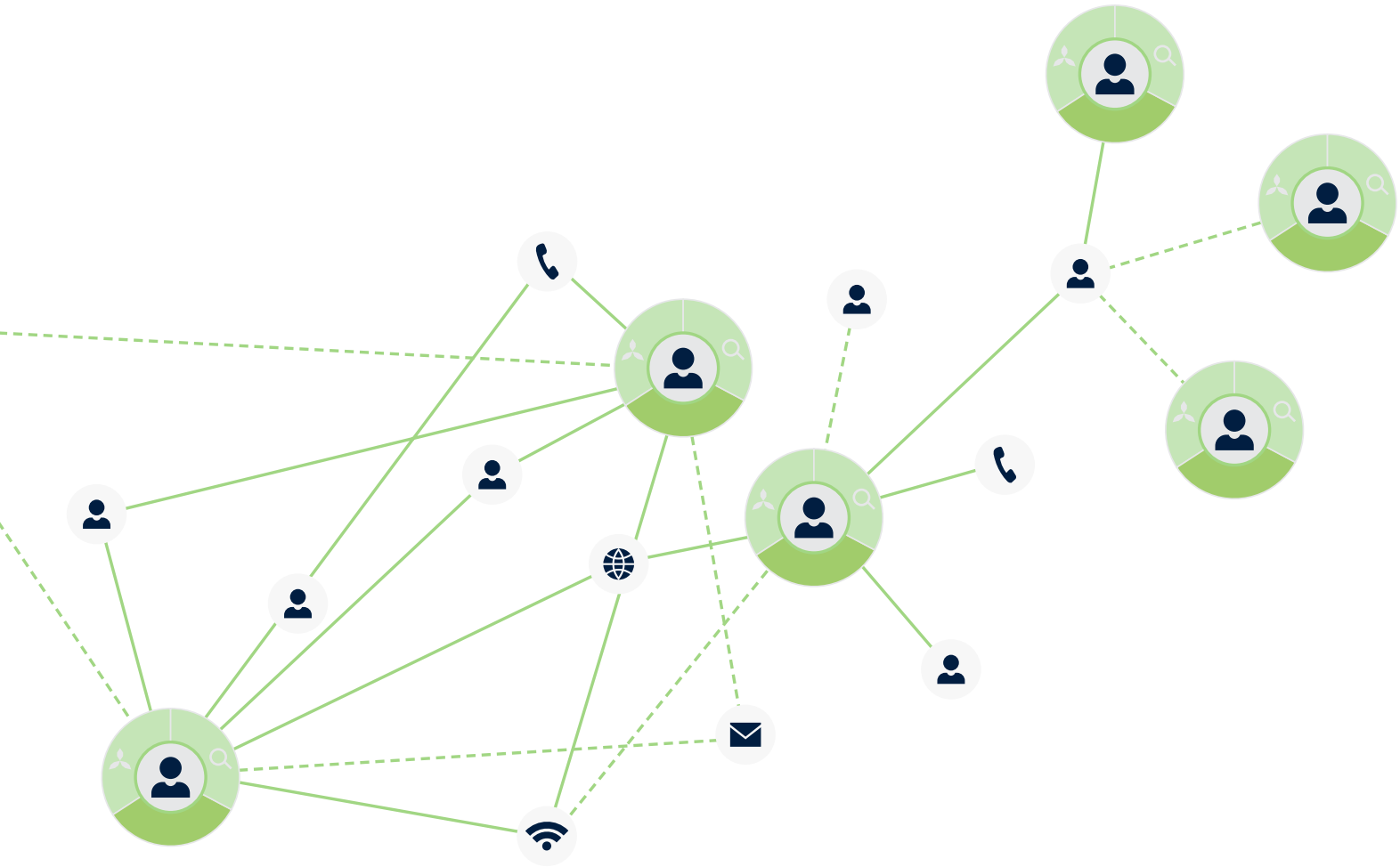
Automatically Identify Suspicious Entities

Knowledge Graph automatically identifies the most suspicious entities to streamline the investigation process. Since linkages are created in real time, fraud teams can conduct one-click investigations to learn more about relationship patterns without the need for manual searches.

Flexible Integration to Take Rapid Actions

When fraud is confirmed, teams can take multiple rapid actions to improve their knowledge base and prevent the threat from spreading, including:

- Update white list/black list by directly marking on the graph
- Set flexible ingest alerts from external systems
- Ingest internal and external heterogenous data
- Load, store, and search through years of data



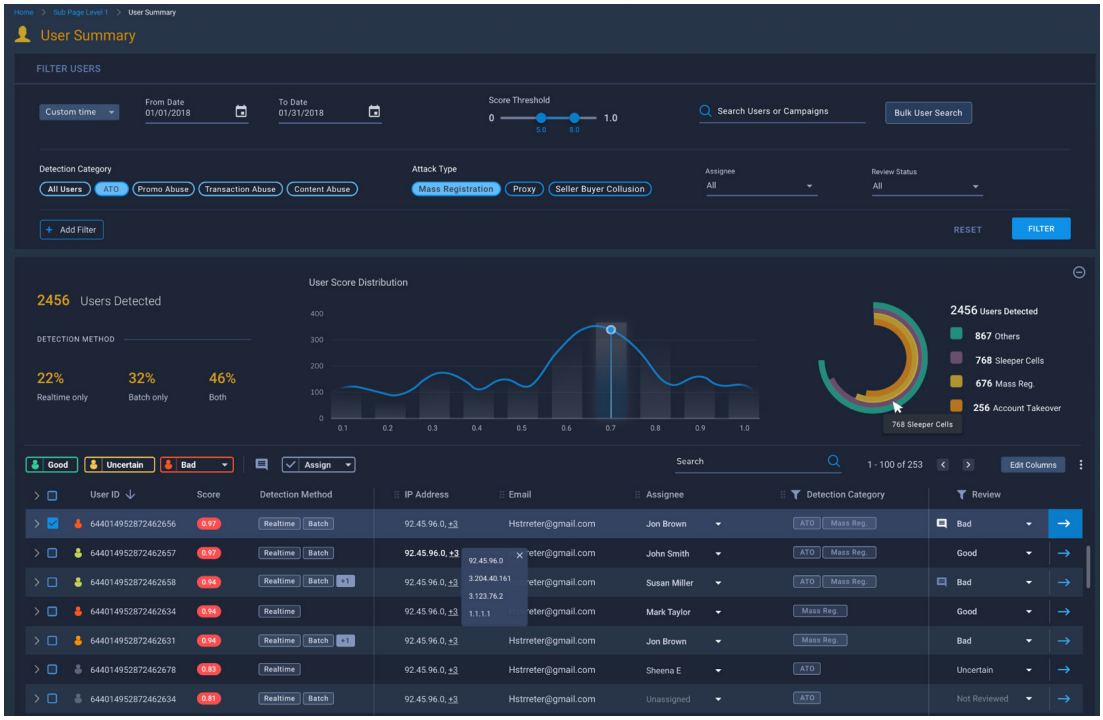
4 Knowledge Graph Capabilities

> DataVisor's Knowledge Graph is part of a comprehensive suite of AI- and ML-driven fraud detection tools. Its inherent capabilities make it a valuable component of an overarching fraud strategy.

Dynamic Integration

DataVisor supports the real-time ingestion of internal structured and unstructured data along with third-party heterogeneous data to spot bad actors, both individually or as a group. This data can come from a variety of sources, including but not limited to cloud and on-prem databases, local files, and third-party signals and databases, either via API or user uploading.

DataVisor integrates seamlessly with internal case management, rules engine, and machine learning engines to streamline the workflow. A distributed storage system supports loading and searching through years of data.



Entity Resolution

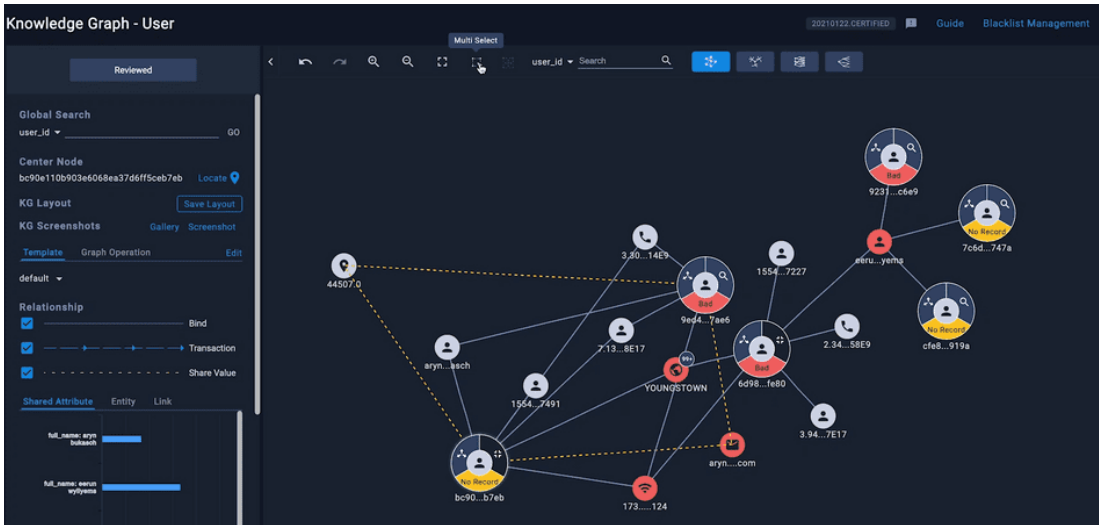
One person could be using multiple entities to carry out fraudulent activities. To understand, identify, and match entities, DataVisor's platform offers the utmost flexibility, including fuzzy matching abilities when some information is missing.

For digital attributes, DataVisor looks for exact matches in device IDs, IP addresses, and email addresses. Non-digital attributes, such as tax IDs, driver's license numbers, and credit card numbers, are also reviewed for exact matches. DataVisor is also flexible in reviewing user text input, such as names, addresses, ZIP codes, phone numbers, and other details that can be cross-referenced. The platform compiles these insights (including custom specifications), finds the links between them, and translates it into a visual explanation.

Real-Time Linkage Analysis

Knowledge Graph allows for real-time graph building and deep fraud analysis between links. AI builds multi-dimensional connections between groups, entities, money flows, IP addresses, email addresses, and other attributes in real time to uncover hidden connections and patterns. Fraud teams can make contextual decisions based on the relationships between users and activities.

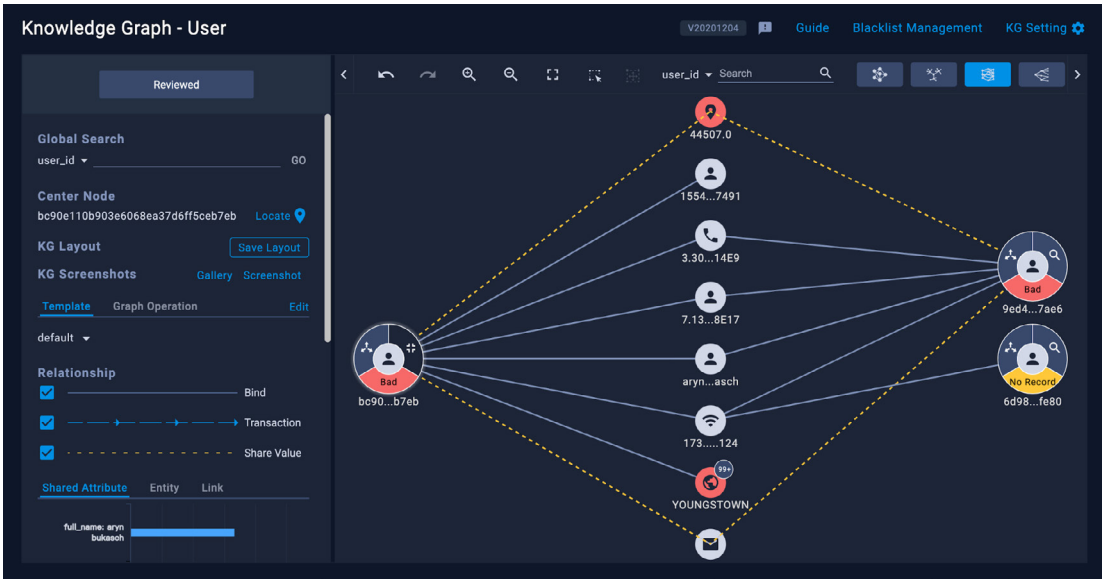
Data in the Knowledge Graph is displayed in a Smart Layout with an intuitive view and shows critical connections based on different fraud scenarios. This gives users the most valuable insights and limits the amount of trivial details to avoid information overload.



Smart Investigation

Smart investigation features allow you to adapt DataVisor capabilities to your needs. Drill deep into as many layers of detail as you need to gain granular insights and build context into your decision making.

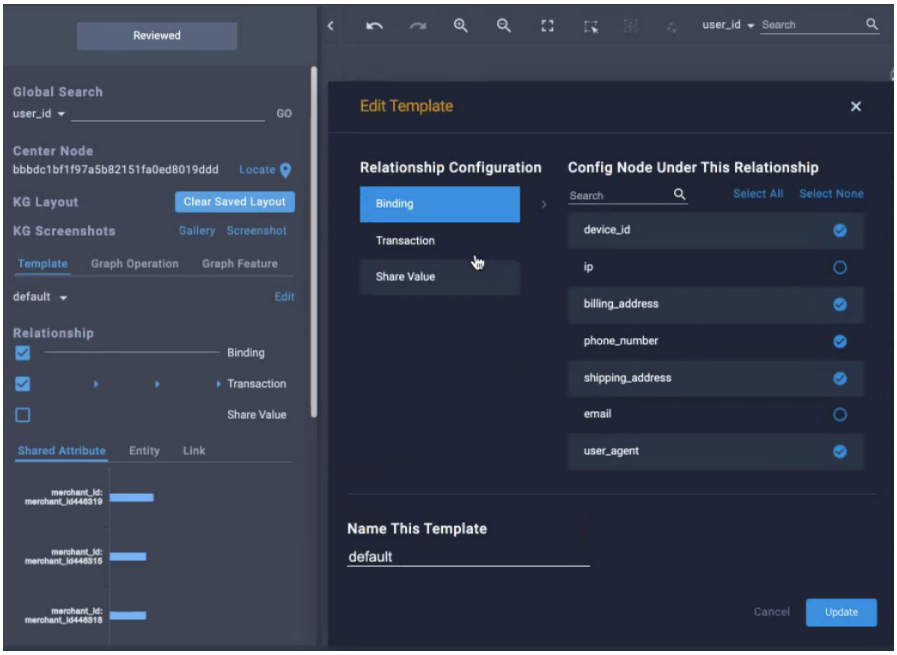
For example, Knowledge Graph's one-click investigation allows users to click their way through multiple layers of detail without extensive searching. Exploring these layers enables teams to easily connect new entities or events with previously detected fraud rings or activities. Users can also search beyond basic entities and events to customize their searches for specific data (e.g., all transactions greater than $500 in the last 7 days, etc.).



Full Customization and Configuration

Knowledge Graph users have full control in defining linkages and setting volume and time windows to generate insights. Within the graph itself, all edges and nodes are fully customizable to give you the most important information for your investigations.

Users can create and leverage customizable templates according to their role to give them the most important information they need to make a decision. Templates combine human expertise with AI research and data collection, and make it easy to share insights across the enterprise. Once created, the templates can be reused and shared with other users and teams to save time.



Rapid Actions

Once fraud teams have made a decision, they can act on those decisions with just a few clicks. For example, entire groups can be blacklisted or whitelisted in seconds, thereby increasing operational savings and reducing fraudulent threats.

Fraud teams can mark groups directly on a linkage graph, saving time compared to identifying and adding them individually. Bridge the gap between investigation and action with just a few clicks. All actions are updated in real time so that teams using the same blacklists or whitelists will receive the same information.

5 Knowledge Graph Case Study

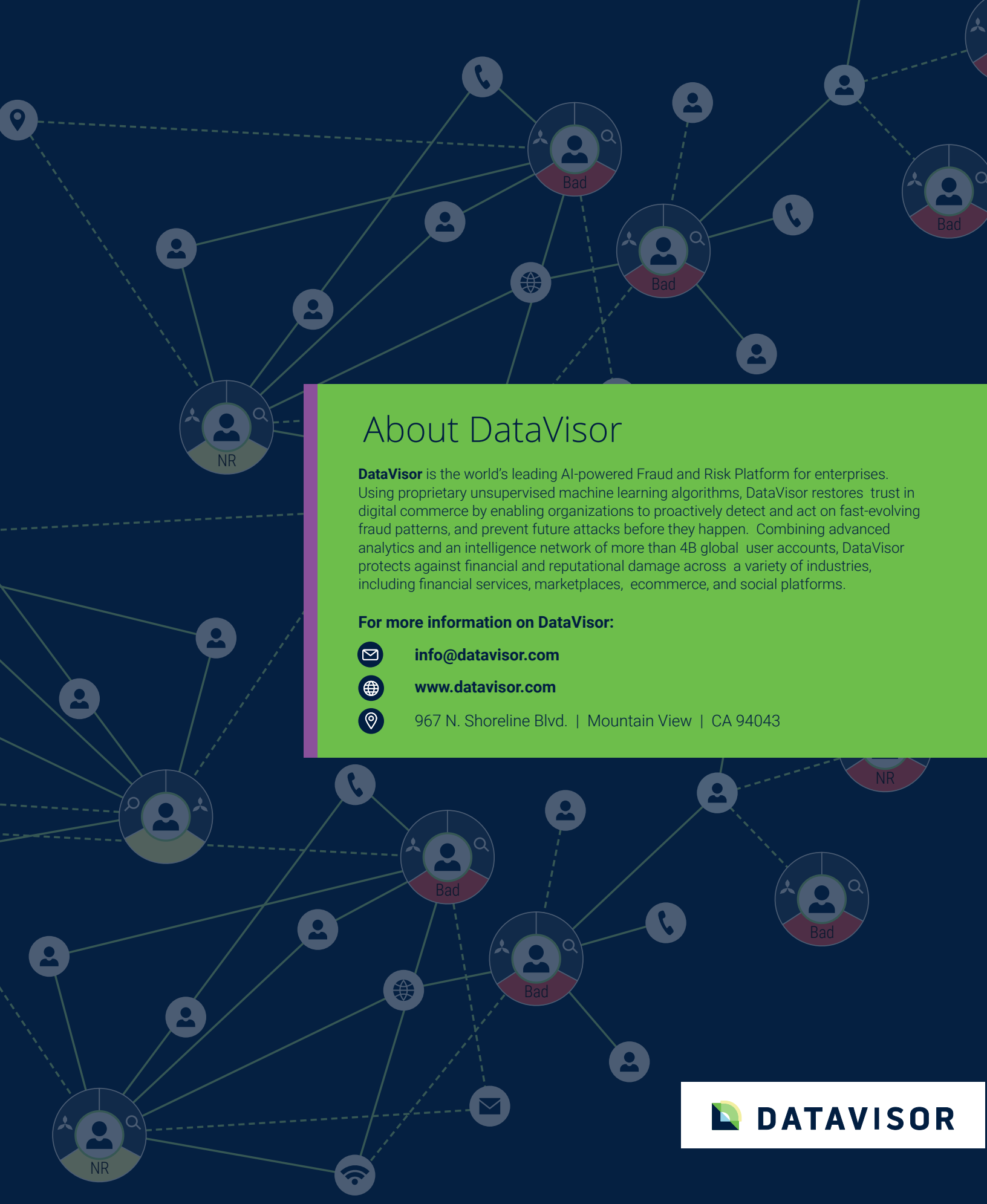
One quick-cash lender in the U.S. deployed DataVisor's Knowledge Graph to overcome significant customer experience and operational challenges.

Because the lender had no way to look holistically at transactional data, each potential fraud case had to be processed individually, which allowed undetected attacks to slip through and triggered high false positive rates. Long processing times caused by manual fraud review led to higher operational costs and lower customer satisfaction.

By leveraging Knowledge Graph in combination with case management, the lender is now able to get a holistic view of the data in real time and make contextual decisions more easily. Knowledge Graph has enabled the lender to achieve a lower false positive rate, detect 20% more fraud, and improve operational efficiency by 500%.

"Our analysts enjoy hunting for hidden bad cases using Knowledge Graph. That brought us 20% more uplifts and has saved us an additional $1.2M after the COVID outbreak," noted the lender.

Knowledge Graph is part of a powerful, AI-driven fraud detection and prevention solution. Discover more about how Knowledge Graph works to uncover more fraud in real time.
Schedule a free 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