DATAVISOR

EVALUATING FRAUD PREVENTION VENDORS: BEST PRACTICES FOR A KILLER RFP

AND A BONUS TEMPLATE TO GET YOU STARTED

Your enterprise payment fraud detection vendor should make life easier and bring more confidence to your business. But as you're comparing solutions and their many features and benefits, clarity and simplicity are often left out of the conversation. Finding the best fit for your organization can be challenging, which is why many companies require a request for proposal (RFP).

Best Practices for Writing an RFP

The goal of the request for proposal isn't to arrive at a final decision, but rather to create a shortlist of potential vendors that can make the exploration process easier and more focused. When developing an RFP template, keep the following objectives in mind:

Gain Insight from Multiple Perspectives

Collect input from all impacted business stakeholders. These may include legal, marketing, customer support, IT and cybersecurity, fraud and risk teams, data scientists, finance, and leadership.

Understand Your Most Important Business Outcomes

Define the key business KPIs by which a fraud detection solution can be considered successful. Focusing solely on vendor capabilities may distract from the business outcomes the vendor is being asked to achieve.

Take Features a Step Farther By Differentiating Their Functions

Seek to differentiate each fraud prevention solution when defining feature requirements and benefits. Ask vendors to specify how those features work to support the desired business outcomes and KPIs.

RFP Template for Choosing a Fraud Prevention Solution

Developing an RFP to support the fraud detection solution selection process can simplify comparisons, encourage healthy competition, and put the focus on performance, not features. Using the best practices above, we've designed an RFP template you can use when vetting a new fraud detection solution:

Fraud Prevention Solution KPIs

KPI	Definition	Why It's Important
Auto accept Rate	% of transactions or applications that are automatically accepted with no manual review	Most companies want to maximize this.
Auto reject Rate	% of transactions or applications that are automatically declined with no manual review	Most companies want to minimize this.
Manual Review Rate	% of transactions or applications that are automatically flagged for manual review	Ideally, this is minimized to reduce manual efforts.
Postreview Acceptance Rate	% transactions or applications that were manually reviewed and become accepted	If this figure is >60%, it suggests that the tool is causing too many good transactions or applications to be reviewed that should be auto accepted.
Postreview Reject Rate	% of transactions or applications that were manually reviewed and become rejected	If this figure is >60%, it suggests that the tool is causing too many fraudulent transactions or applications to be reviewed that should be auto rejected.
Authentication Pass Rate	% of customers that pass authentication challenges	Helpful in understanding if customers are being inconvenienced with additional authentication
Fraud Rate	% of accepted transactions or applications that turn out to be fraud	Indicates the effectiveness of fraud prevention solution
False Positive Rate	% of rejected transactions or applications that aren't fraudulent	Represents lost revenue and eroded consumer trust

RFP Fraud Prevention Solution Differentiation Questions

Model Development & Management

- Describe how your fraud model outputs can be audited to determine how decisions were made.
- How does your fraud detection solution avoid bias?
- What are the different sources of data your models use? How are each weighted and leveraged to improve model performance?
- How can you help us to achieve model governance?
- How can our data scientists create and run their own models on your platform?
- How does your solution support model comparison and validation?
- Can machine learning models be configured to meet our specific needs?
- Can our existing machine learning models be combined with your solution?
- Are machine learning models self-training or do they need to be retrained over time?
- How does your fraud solution discover new fraud or patterns without model retraining?
- Explain how you identify previously unseen fraud patterns.
- How does your solution measure false positive rates?

Rules Management

- Does your fraud solution include a rules engine?
- Can rules be created, altered, deleted, and tested within the platform?
- Can our internal data scientists back-test rules using extensive historical data within the rules engine
- How are rules used in the fraud detection decision process?
- Who holds the responsibility of retraining the rules with fresh data — you or our internal team?
- How scalable is your rules engine?
- Can out team forward test rules before deploying them in production?
- Can your rules engine auto-suggest new rules to adapt to fast-changing fraud attacks?

Data & Analytics

- How does your fraud solution ingest various types of data?
- Can you solution ingest unstructured data?
- How can you streamline data integration?
- Are there limits to the types of data that your platform can ingest? If so, describe the limitations.
- Describe the types of data your solution looks at to analyze fraud activities and patterns (e.g., device intelligence, behavior analytics, biometrics, etc.).

Case Management

- Explain how third-party services integrate with your case management tools, why you chose them, and how they have improved outcomes for your clients.
- How does your case management reduce the time it takes to investigate transactions?
- How can your case management tools fit into a broader workflow?
- Can alerts be automatically routed to specific case managers based on rules?
- How can case management features be combined with other channels for a more comprehensive, unified case?
- How does your solution prioritize alerts based on risk scores or other factors?

Link Analysis

- Does your solution have visual entity linkage analysis?
- Can your solution allow the analysts to investigate the graph, i.e., click on an entity to expand the graph further?
- Can your solution automatically discover the criminal/mule network and visualize it?
- How can your solution pull all the historical information and events of the cases? For example, the account's registration information, historical transaction and login events.
- Can your solution allow analysts to reconfigure the graph layout and save the graph for manager review?

Authentication

- How does your fraud prevention solution balance the need to authenticate customers while also reducing customer friction?
- Explain the authentication measures you offer, why you have chosen them, and the outcomes they have produced for your clients.

Other Questions to Consider

- Briefly describe the types of fraud your solution is designed to detect (e.g., account takeovers, AML, digital payments, check fraud, etc.)
- How does your solution work across channels to provide comprehensive coverage?
- What ongoing support do you provide?
- What is the average timeline to fully implement the fraud solution and start seeing an ROI?

Discover how DataVisor helps you connect your fraud prevention solution to real business outcomes. Get a demo to experience proactive AI-powered fraud detection.

About DataVisor

DataVisor is the leading fraud and risk management platform powered by transformational AI technology. Using proprietary machine learning algorithms, it restores trust by enabling organizations to stay ahead of even the most sophisticated forms of fraud. DataVisor protects clients across financial services and digital commerce against economic losses and reputational damage by combining advanced analytics and an intuitive SaaS interface with terabytes of data enriched by an extensive partnership network of identity providers.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

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