6 Questions to Ask

Before issuing a request for proposal (RFP)

Accertify

Executive Summary

Selecting an e-commerce fraud detection partner is not just a technology decision—it is a business-critical strategy that impacts **revenue growth, risk posture, and customer experience**. Before issuing an RFP, executives should ensure alignment on six strategic questions:

1. Does your strategy to stop fraud support revenue?

There are 3 dimensions to supporting revenue:

- The ability to minimize false positives, as they are the enemy of growth.
- The ability to scale to handle growth as well as peak selling times.
- The ability to optimize payments.

2. Are you addressing fraud across the entire customer lifecycle?

Fraud doesn't start and end at checkout. Account takeovers, returns abuse, and refund fraud demand a holistic approach.

3. What fraud model aligns with your business goals?

Understand partner models—liability shift, black box, or Service Levels Agreement (SLA) based—and choose one that aligns their incentives with YOUR revenue.

4. Does your RFP for Fraud integrate chargeback management?

Chargebacks are a feedback loop for fraud strategy. Integrated solutions bring more accurate machine learning models and improved dispute win rates.

5. Does your partner understand your vertical?

Industry-specific models and insights outperform generic solutions.

6. How strong is the fraud detection partner's data network?

Size and diversity of data matter. Partners with broad consortium networks deliver faster, more accurate fraud detection that guards your top-line.

Bottom Line

Issuing an RFP without answering these questions risks misalignment, lost revenue, and operational inefficiency. A well-prepared RFP sets out the foundation for measurable outcomes: **higher approval rates, lower fraud losses, and improved profitability**.

Introduction

Issuing a RFP for e-commerce fraud detection software is not just a procurement exercise—it's a strategic decision that will influence your company's risk posture, customer experience, and profitability for years to come. Yet many companies rush into the process without first asking the right internal questions. The result? Misalignment.

The **cost of misalignment** is significant and often underestimated. It manifests in several ways:

1. **Revenue loss**

   Your first priority should be to maximize sales while minimizing risk. Inaccurate fraud decisioning leading to too many false positives will result in lost revenue and degraded customer experience.

2. **Suboptimal fraud outcomes**

   When your fraud prevention approach only addresses checkout fraud—or fails to evolve with emerging attack vectors—you leave your business exposed. Fraud is dynamic, and is perpetrated well before and well after the checkout.

3. **Mismatch with organizational capacity and resources**

   Selecting a solution that doesn't match your in-house operational expertise – or lack thereof - creates inefficiencies and risk. Conversely, outsourcing everything without understanding the trade-offs of the various partner models can result in overpaying for suboptimal results.

Before you draft your RFP, step back and answer the following six questions. They will help you define what success looks like and ensure that your partner selection process generates the results you desire.

Question 1:

Does your fraud strategy support revenue?

Supporting revenue is every company employee's mission. That means a fraud strategy must also be aligned to maximizing company revenue – and this is important along three dimensions: a) maximizing sales acceptance through the removal of false positives (transactions that are legitimate but marked as fraudulent); b) scaling to support your growth as well as peak selling times; and c) optimizing payments.

Why This Question Matters

Reframing your fraud strategy as maximizing revenue means you would not make decisions that impair the top-line in the name of preventing fraud. With this outlook, you won't be tempted to over-decline transactions suspected of fraud just to lower your chargeback losses.

You will also be keen to find a partner who has shown themselves capable of scaling to handle your long-term growth, as well as during peak selling times like Black Friday and Cyber Monday, which have transcended the United States to become globally relevant. Systems availability during such times is critically important to revenue realization, and you'll want to make sure you understand your partner's uptime strategy.

And finally, evaluate your partner's approach to payment optimization. Will they help maximize success through proven techniques such as intelligent routing and best-practice use of 3-D Secure (3DS)? A strong payment optimization strategy ensures legitimate transactions are approved without adding unnecessary friction, thereby upholding your revenue-first fraud outlook.

RFP Implications

Your RFP should require clarity on how the potential partner supports revenue across these dimensions:

- False Positive Reduction: Request a detailed explanation of how the partner minimizes false positives and maximizes approval rates, including how these metrics are calculated. For example, clarify whether multiple attempts are counted as a single transaction.
- Scalability: Ask for evidence of the partner's ability to handle peak selling periods and long-term growth. This includes uptime strategy, system availability guarantees, and performance benchmarks during high-volume events like Black Friday and Cyber Monday.
- Payment Optimization: Require details on how the partner improves authorization success through best practices such as intelligent routing and 3-D Secure (3DS) implementation, while minimizing unnecessary friction for legitimate customers.
- Transparency in Decisioning: Confirm whether you can access transaction-level insights, such as scores, reasons for declines, and linkages to related transactions for historical context.

Question 2:

Are you addressing fraud across the entire customer lifecycle?

Before you even think about partners, you need clarity on the scope of your fraud prevention strategy. Fraud doesn't start and end at checkout. **Third-party fraud**—such as stolen credit cards purchased on the dark web—typically targets account creation and checkout. **First-party or friendly fraud**, where customers abuse return policies or request excessive refunds, often happens post-purchase.

Why This Question Matters

Most RFPs for e-commerce fraud detection software narrowly target payment fraud at checkout. While checkout is important, this approach ignores other high-risk areas such as account takeover, returns abuse, and refund fraud. *Today's e-commerce businesses need a holistic approach to assessing risk across the entire customer journey. To accomplish this, businesses need to perform event-based risk assessments on every customer touchpoint.*

Lifecycle Risks

Pre-Transaction Threats

- Fraudsters gain access to legitimate accounts through credential stuffing or phishing. Once inside, they can make unauthorized purchases or exploit stored payment methods.
- Event-based risks that need to be assessed: account creation, login, account changes.

Transaction Threats

- Fraudsters gain access to credit cards and use them to make fraudulent purchases.
- Event-based risks that need to be assessed: purchases.

Post-Transaction Threats

- Fraudsters and customers alike can manipulate or take advantage of return policies and refund processes, with fraudsters often using stolen payment credentials.
- Event-based risks that need to be assessed: returns, refunds, and chargebacks.

Blind Spots of Checkout-Only Focus

Many organizations only detect first-party abuse after purchase, but this reactive approach creates blind spots. Blocking an abusive account does not prevent the same individual from opening a new account and repeating the behavior. Holistic lifecycle fraud prevention requires visibility at account creation—identifying known fraudsters and abusers before they reach the purchase path—to mitigate both first- and third-party fraud.

Benefits of Holistic Prevention

- **Unified View of Risk:** Linking signals across the lifecycle—account creation, login, checkout, and post-purchase—enables better detection and decisioning.
- **Greater Flexibility that Disrupts Fraudsters:** When fraud signals are captured across the entire customer lifecycle, merchants gain strategic flexibility in how and when to act. For example, a merchant might detect risk at login but choose to intervene later at the point of purchase. This unpredictability makes it harder for fraudsters to identify which data point triggered scrutiny, increasing the complexity of evading controls and reducing their ability to adapt.
- **Stronger, More Predictive Models:** Machine learning models that incorporate multi-touchpoint data are more resilient to evolving fraud patterns.
- **Improved Customer Experience:** Holistic strategies reduce false positives and unnecessary friction at checkout, preserving revenue and brand loyalty.

Operational Implications

A holistic approach to fraud prevention isn't just about technology—it's about reducing complexity and risk. Many organizations unknowingly create operational and security challenges by deploying separate solutions for account protection, transaction screening, and returns/refund abuse. This fragmentation leads to:

- **Operational Inefficiency:** Teams waste time toggling between multiple systems, reconciling data, and managing inconsistent workflows.
- **Incomplete Risk View:** Disconnected tools make it harder to link signals across the customer lifecycle, leaving blind spots that can be exploited.
- **Higher Total Cost of Ownership—and Increased Security Risk:** Multiple partners mean multiple contracts, integrations, and support models. More importantly, they create multiple points of entry into your organization, increasing the attack surface and complicating compliance.

Organizational Alignment Matters

Fraud prevention isn't just a Chief Financial Officer (CFO) of Chief Operating Officer (COO) concern. The Chief Information Security Officer (CISO) plays a critical role in account protection and overall security posture. Too often, CISOs are only brought in to validate compliance. A converged approach—where the CFO and CISO jointly shape fraud strategy—ensures alignment between financial risk and cybersecurity AND generates better fraud prevention outcomes.

RFP Implications

Fraud cannot be considered in a silo. A holistic fraud strategy is not optional—it's essential. Limiting your approach to checkout-only solutions leaves blind spots that attackers and opportunistic customers will exploit.

Your RFP should explicitly require:

- Capabilities that address fraud across the entire customer lifecycle (account creation, login, checkout, and post-purchase returns, refunds, claims, and adjustments).
- Inbuilt integration of fraud prevention tools to reduce operational complexity and avoid toggling between applications.
- Alignment between financial risk and cybersecurity by involving both the CFO and CISO in shaping fraud strategy.
- Support for unified data and workflows to enable predictive models and better customer experience.
- An integrated platform that contains all customer events in a single solution, delivering your business a complete view of customer interactions across the journey.

This decision will shape partner selection, pricing models, and your long-term operational success.

Question 3:

What fraud model aligns with your business goals?

If you don't have fraud expertise in-house and don't want to build a fraud team, you will need to find expertise outside and partner with a trusted expert (and presumably, this is why you're issuing an RFP). In general, the partners that you will be outsourcing to have a few different approaches:

1. The Fraud Liability Shift (FLS) Approach

FLS means you pay a portion of your revenues to the fraud software vendor, and in return, they assume total liability for fraud-related losses. On the surface, this seems convenient—no more worrying about chargebacks.

However, the economics of this model can be challenging. Because 90+% of transactions are legitimate, you're effectively paying an insurance premium on good transactions – making this approach disproportionately expensive for most merchants.
In other words, you're overpaying for protection you rarely need.

Beyond cost, FLS creates a misalignment of incentives:

- The vendor is motivated to minimize chargebacks at all costs.
- To do that, they may decline more transactions, including legitimate ones.
- Result: lost revenue for your business, and frustrated customers.

Fraud liability shift has a place, but it should not be a standalone solution. To truly optimize margin, use the fraud liability shift on your highest-risk transactions only – otherwise, you could be overpaying for transactions that were never at risk.

2. The Black Box Approach

A black box vendor uses machine-learning models to generate a single fraud score or result for each transaction but doesn't allow you to understand the specific underpinnings of that score or result. A models-first approach is the right answer, but the problem here is not giving access or only giving minimal access to why the model scores the way it does, leading to a **lack of observability and explainability:**

- You can't see why a decision was made, so you can't easily adjust the inputs to the model.
- You also typically cannot add additional rules or thresholds at all.
- If they don't have an integrated chargeback/ dispute solution on the same platform, their machine-learning models are not going to be adjusted to the outcomes anyway, causing them (and you) to make poor decisions in perpetuity.
- Ultimately, all of the above limits your ability to optimize fraud strategy for margin, customer experience, or unique business needs.

3. The Profit Share/Revenue Incentive SLA Partner

This is a partner that provides you an SLA which ensures a minimum acceptance and chargeback rate that aligns with company goals. If they perform better than these guarantees, they take a profit share. If they perform worse than these guarantees, they take the loss. Having a fraud partner that offers an accept-reject model, but allows you to determine the thresholds that are acceptable to your organization means they are aligned with your overall revenue maximization strategy.

Why This Matters

Choosing the right fraud model means finding a partner who will be aligned with your company's desire to guard revenue while minimizing risk. Choosing a standalone fraud liability shift model may create incentive misalignment between your company and your fraud vendor. Choosing a black box vendor may mean ceding control entirely to a machine that may or may not be "learning."

Looking for an alternate or hybrid approach, such as a partner who offers SLAs and then receives additional incentives for better performance, may solve the incentive misalignment problem. And finding a partner who provides good model explainability and can demonstrate why decisions were made at the transaction level can alleviate the challenges that come with "black box" vendors.

RFP Implications

Ask about:

- Whether they offer alternate models to the fraud liability shift or otherwise create alignment with revenue maximization.
- Whether they offer transparency in decisioning logic. Ask to see examples of supporting detail.
- Whether they offer the ability to configure tailored rules and thresholds in combination with a strong machine learning basis.
- To what extent they provide human fraud decisioning support (to review those transactions which fall into the "grey" area.

Question 4:

Does Your RFP Integrate Chargeback Management?

Chargebacks are more than a payments nuisance—they're a critical component of fraud strategy because they're a natural and instantaneous feedback loop for your fraud strategy. This is why it's essential that fraud detection and chargeback management be considered together in the same RFP. Not including chargeback management or having a separate chargeback management solution can lead to suboptimal fraud outcomes and lower win rates.

Why Chargebacks Matter

Chargebacks represent both fraud and operational inefficiencies. They impact cash flow, incur fees, and damage relationships with payment processors.

Why Fraud Detection and Chargeback Management Are Better Together

Partners that handle both fraud detection and chargeback management create a powerful, real-time feedback loop that improves outcomes across the board:

- **Accelerated Model Improvement:** Dispute outcomes feed directly into fraud models, enabling real-time updates that make detection more accurate and adaptive to emerging patterns.
- **Stronger Fraud Signals:** Fraud insights inform dispute strategies, creating a closed loop that continuously strengthens both prevention and recovery.
- **Faster Identification of Friendly Fraud:** Integrated chargeback data not only accelerates model learning but also makes friendly fraud easier to spot and address—reducing unnecessary disputes and improving win rates.
- **Higher Overall Performance:** This rapid learning cycle reduces false positives, improves customer experience, and helps merchants stay ahead of evolving fraud tactics.

Only solution providers with integrated chargeback and dispute solutions on the same platform have access to the "truth" they need to update models in real time.

This is why combining fraud and chargeback management with the same partner typically results in higher dispute win rates. Why? A strong fraud strategy reduces fraud-related chargebacks (which are almost impossible to win), shrinking the denominator and boosting your overall win rate.

RFP Implications

Your RFP for e-commerce fraud detection software should also explicitly ask about:

- Dispute win rate.
- Chargeback ratio.
- Recovery timelines.
- Automated representment workflows.
- Chargeback win rate of customers who have the combined fraud detection and chargeback management solution.

Question 5:

Does your fraud detection partner understand your vertical?

Fraud patterns vary significantly by industry. A partner with deep vertical expertise can deliver tailored models and operational insights that generic solutions cannot. This matters because fraud tactics evolve differently in travel, retail, hospitality, gaming and digital goods businesses. A one-size-fits-all approach often leads to poorer results.

Vertical-Specific Expertise

Tailored AI/ML Models

Models trained on industry-specific data outperform horizontal models in accuracy and false positive reduction.

Operational Insights

Partners familiar with your vertical can anticipate seasonal fraud trends, regulatory nuances, and common abuse patterns.

People Expertise

Technology alone isn't enough. The best partners pair advanced models with teams who have lived the challenges of your industry. Colleagues who come from retail, travel, gaming, or digital goods bring practical insights that generic providers cannot match. Their experience helps anticipate seasonal fraud trends, regulatory nuances, and operational realities—ensuring your fraud strategy is grounded in real-world expertise, not just algorithms.

Why This Matters

Vertical expertise isn't just about better detection—it's about optimizing customer experience and reducing unnecessary friction. For example, a travel-focused fraud model understands last-minute booking patterns, while a retail-focused model accounts for gift card abuse and returns fraud. When combined with human expertise, these insights drive smarter decisions and faster adaptation to emerging threats.

RFP Implications

- Evidence of vertical-specific AI/ML models and how they differ from horizontal models.
- Examples of operational insights tailored to your industry (seasonality, regulatory compliance, common fraud schemes).
- Proof of people expertise, such as team members with prior experience in your vertical or specialized fraud practitioners.
- Case studies or benchmarks demonstrating performance in your vertical.
- Partner disclosure questions, such as:
    - Do you have clients in my industry? How many?
    - How do you customize models for vertical nuances?
    - Can you share case studies or benchmarks?
    - Can we speak to your clients who operate in our industry to learn from their experiences of working with you?

Question 6:

How strong is the partner's data network?

It takes a village to fight fraud. Partners with broad, diverse data networks—and the ability to share intelligence across merchants—offer a significant advantage and create powerful network effects: when one bad actor is detected for one merchant, others in the network benefit as well. This collective intelligence accelerates detection and reduces community exposure (similar to the concept of "herd immunity" in epidemiology) and truly highlights the meaning of being "better together."

Why This Matters

Because size matters! No matter how robust fraud detection models are, they all require data to get better. At its core, machine learning has a "cheat code" – the larger and more diverse the dataset it is trained on, the more focused it is on your vertical, and the more accurately marked feedback data it has, the better the model becomes. This is why vendors with narrow datasets struggle to detect emerging fraud patterns, while those with global, multi-vertical coverage adapt faster and deliver better protection.

RFP Implications

Your RFP should explicitly require:

- Evidence of consortium data sharing and how intelligence flows across merchants.
- Breadth and diversity of the partner's data network (geographic coverage, verticals, transaction types).
- Refresh frequency and mechanisms for updating fraud models with new data.
- Partner disclosure questions, such as:
    - How large is your network?
    - How frequently do you refresh data?
    - Do you share intelligence across clients?

Conclusion

Choosing a fraud detection partner isn't just a technology decision—it's a business-critical strategy that shapes revenue, risk posture, and customer experience. Issuing an RFP without addressing these six questions first risks adopting the wrong strategy – or settling for suboptimal results.

A well-prepared RFP should:

- Align fraud strategy with revenue goals by minimizing false positives, scaling for growth, and optimizing payment authorization.
- Require a holistic approach to fraud across the entire customer lifecycle to eliminate blind spots.
- Integrate chargeback management to create a real-time feedback loop that strengthens fraud models and improves dispute outcomes.
- Demand vertical-specific expertise—both in technology and in people—so your partner understands the nuances of your industry.
- Require a partner with a true consortium approach—where fraud spotted at one merchant is blocked across all clients, so you join a community that protects each other and fights fraud together.

When these elements come together, your RFP does more than solicit bids—it sets the foundation for measurable outcomes: higher approval rates, lower fraud losses, improved profitability, and a fraud strategy that is resilient, adaptive, and optimized for growth.

**In short:
Ask the right questions now, so you don't pay for the wrong answers later.**

Accertify enables commerce by doing one thing extraordinarily well: pinpointing fraud. The company's Predictive Yes Platform helps businesses say yes to more - more good customers, more revenue, and more growth - without getting burned. It's a precise, confident, data-backed yes, made possible by joining signals across the entire customer lifecycle through unmatched data volume, layered AI-powered models, and a consortium approach that protects clients from bad actors spotted anywhere in the network while unlocking business with good actors verified anywhere in the network. With more than 10 billion transactions and over $1 trillion in commerce processed in 2025 alone, Accertify delivers the intelligence and precision that fraud and payments teams need to say yes confidently and enable growth. That's the More Yes difference. Learn more at **accertify.com**.

Accertify