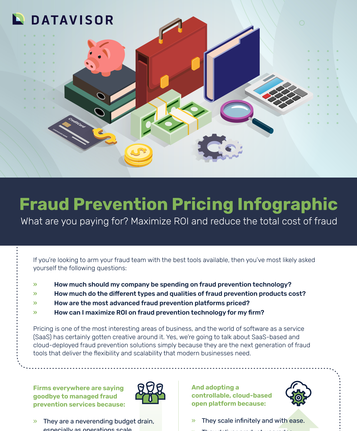
DATAVISOR



Fraud Prevention Pricing Infographic

What are you paying for? Maximize ROI and reduce the total cost of fraud

If you're looking to arm your fraud team with the best tools available, then you've most likely asked yourself the following questions:

- **How much should my company be spending on fraud prevention technology?**
- **How much do the different types and qualities of fraud prevention products cost?**
- **How are the most advanced fraud prevention platforms priced?**
- **How can I maximize ROI on fraud prevention technology for my firm?**

Pricing is one of the most interesting areas of business, and the world of software as a service (SaaS) has certainly gotten creative around it. Yes, we're going to talk about SaaS-based and cloud-deployed fraud prevention solutions simply because they are the next generation of fraud tools that deliver the flexibility and scalability that modern businesses need.

Firms everywhere are saying goodbye to managed fraud prevention services because:

- They are a neverending budget drain, especially as operations scale.
- They can't provide the agility and real-time response that modern businesses require.
- Working with them means handing control over the fraud strategy and customer experience.
- Fraud teams quickly realize that managing these service providers is hard work.

And adopting a controllable, cloud-based open platform because:

- They scale infinitely and with ease.
- They deliver product upgrades and innovation without lengthy installation cycles.
- They have lower total costs of ownership (TCO).
- They can be deployed faster for immediate protection.
- They allow for rapid response to real-time threats without depending on batch updates.

40%

The percentage of enterprise workloads that will be deployed in cloud infrastructure and platform services in 2024, vs. just 20% in 2020.[1]

58%

The portion of SaaS technology contracts among all those negotiated over 2020.[2]

[1]Gartner: How Cloud Adoption Will Increase Opex Budgets.
[2]Gartner: 2021 SPVM Leaders Survey.

How are SaaS-based fraud prevention products priced?

Let's cut to the chase. These are the main ways in which fraud prevention companies can price their products and services.

Flat rates
where fraud teams pay a fixed recurring fee per month/year regardless of their usage levels.

Pay-as-you-go
such as when fraud teams pay a fee per transaction monitored or per API call.

Tiered Prices
where vendors offer different packages based on the volume of events monitored (or other metrics) and often reduce the unit price as the customer enters a higher tier.

Pay-per-user
(AKA per-seat pricing), in which fraud teams pay based on how many employees have access to the vendor's fraud prevention software.

Pay-per-feature
(AKA per-seat pricing), in which fraud teams pay based on how many employees have access to the vendor's fraud prevention software.

How much can my firm expect to pay for a fraud solution?

The world of SaaS fraud prevention is quite varied, from relatively simple signal providers to comprehensive platforms that tackle multiple use cases. The first risk that teams need to take before shopping for fraud solutions is to decide on the various factors that need to be considered - from resource to infrastructure requirements. We have this buyer's guide ready for you!

Once you define the type of solution your firm needs, use this table as an illustrative guide of what you can expect to pay. Please note that actual costs will vary depending on many factors.

How do fraud leaders get the most out of their budgets?

1st Quantify the fraud problem and set a realistic budget to solve it.

How much is your firm's total financial impact of fraud (AKA total cost of fraud)? Here are some concepts that you should include:

Direct Losses
- Funds stolen from accounts
- Successful payment fraud
- Chargeback management costs

Cost of Tools and Headcount
- Costs of detecting and preventing fraud
- Cost of maintaining in-house systems
- Cost of vendor-provided tools
- Human resources

Impact on the Customer Lifetime Value
- Customers that close their accounts due to fraud
- "Good" transactions rejected by fraud systems (AKA false positives)

Pro Tip: If your firm has several fraud signal providers or point solutions in production, then it might be time to consider implementing a fraud platform that can provide a centralized hub and eliminate the need for monitoring a fragmented infrastructure.

Understanding your firm's total cost of fraud can quantify the financial loss and identify the suite of tools that can mitigate the problem.

2nd Evaluate different vendors.

Start by making a shortlist of companies that have deep fraud expertise. Lean towards vendors who take a partnership approach as no two organizations have the same type of fraud problem. Then, engage in a fraud problem discussion, scope, and solution conversation with them.

Your focus should be on the benefits their solutions can bring to your team and fully understanding their pricing policies. Make sure to include these questions/items in your conversations:

- **Describe the setup costs and ongoing fees that make up your pricing.**
- **List all the items that these prices include.**
- **What add-ons, products, or services are not included in those prices?**
- **How long are your integration times?**
- **Do you offer any professional services, and are they included in the quoted price?**

In your evaluation process, you'll quickly find that some vendors stand out. Below are some pricing red flags you should be on the lookout for.

3rd Pass on vendors that:

1. **Are not transparent** about their pricing practices.
   Beware! Some vendors advertise their prices as final, but in reality these don't include certain "add-ons" that are required to use their services.
2. **Charge high setup costs.**
   Remember that these are usually forfeited if you end your contract and act as a deterrent to your future choices.
   Plus, high setup costs could signal that the vendor is in fact building something after your specifications, which can result in substantial delays.
   Beware! Some vendors charge a premium for machine learning implementation, but in reality use rules to train their models. This can take 6 months or more.
3. **Pretend to sell a technology product,** but in fact offer professional or "managed" services to mitigate fraud.
   These tend to result in high total costs of ownership and are unsustainable in the long run

4th Look for vendors that:

1. Are clear up front, and allow you to **pay only for the volume you need.** Waste is the enemy of efficiency!
2. Can be **implemented in weeks** so you can protect your firm vs all forms of fraud without.
3. **Offer a true technology product** that is modular in nature so you can pay only for the features and use cases you need.
4. **Can scale with you.** True SaaS products can grow with your business, and fraud prevention technology is no exception.

BONUS

Four ways in which the right fraud vendor can improve your ROI

1. Data consumption optimization.

Third-party data queries (e.g. email reputation and ID validations) make up a large portion of the fraud-related expenses of many modern businesses.

Dozens of different data sources exist, but no single one is enough to make confident decisions. Adding up the pieces can get quite costly, and third-party data fees are not really an investment: the information expires quickly and firms can become dependent on other companies to manage fraud.

A well-designed decision engine delivers powerful orchestration capabilities that allow fraud teams to strategically manage third-party data consumption to minimize expenses and increase detection accuracy.

Firms can customize detection workflows so that external queries are only run on an as-needed basis. For example, they can apply differentiated treatment to account openings based on adjustable customer trust profiles determined by advanced machine learning models, device intelligence, geolocation, behavioral insights, or other objective parameters

2. Unlocking the benefits of a true SaaS platform.

This allows customers to say goodbye to traditional solutions that require weeks to implement, and as a result leave them exposed to fraud losses for long periods.

No more relying on legacy vendors–and paying their fees–to write rules, deploy new features, or tune models, resulting in firms who are in control of their fraud and risk management strategies and are self-reliant to respond to threats.

3. A single solution for all fraud use cases.

With an extensible platform, firms no longer have to worry about managing different fraud solutions for each product or business line. From payments to loan applications, account protection, and beyond, look for a solution that supports all use cases.

Say good riddance to having to look for a new fraud solution when your firm launches a new product, service, or market. Eliminate the burden of managing several solutions and achieve substantial savings and efficiency gains.

4. Raising the bar for customer success.

The right fraud vendor should offer industry-leading customer success services at no extra charge. They should deliver value to their client relations by pairing each customer with a dedicated technical account manager with domain expertise and industry knowledge to handle issues like:

- **Continuously monitoring each client's use of our platform and providing support when needed.**
- **Ensuring that clients experience no surprises due to exceeded monitoring capacities, tier changes, or any unknown/unplanned costs.**
- **Providing advice about new fraud trends detected at an industry level and how to stop them before they actually occur.**

This support directly increases ROI by ensuring that your firm faces no surprise charges and is always empowered to stop fraud as efficiently as possible.

Curious about DataVisor's actual pricing for your firm?

Let's talk over a quick call, where we will learn about the fraud problems you want to solve, discuss how we can help, and provide you with a tailored pricing estimate.

Schedule A Demo