SEON

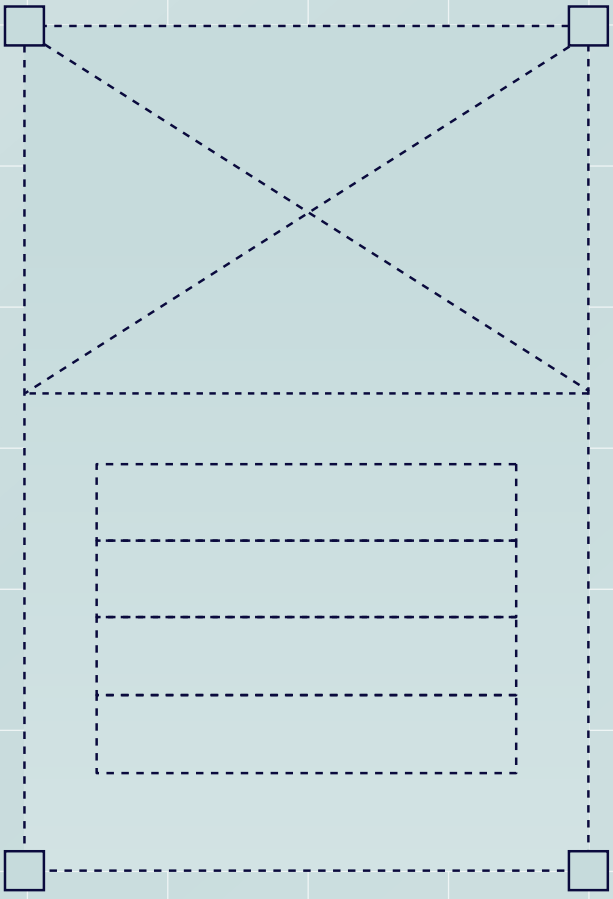
GUIDE

Buy Versus Build: What to Consider When Assessing Fraud Solutions

YOUR FIRST LINE OF DEFENSE AGAINST ONLINE FRAUD

INFO@SEON.IO

WWW.SEON.IO



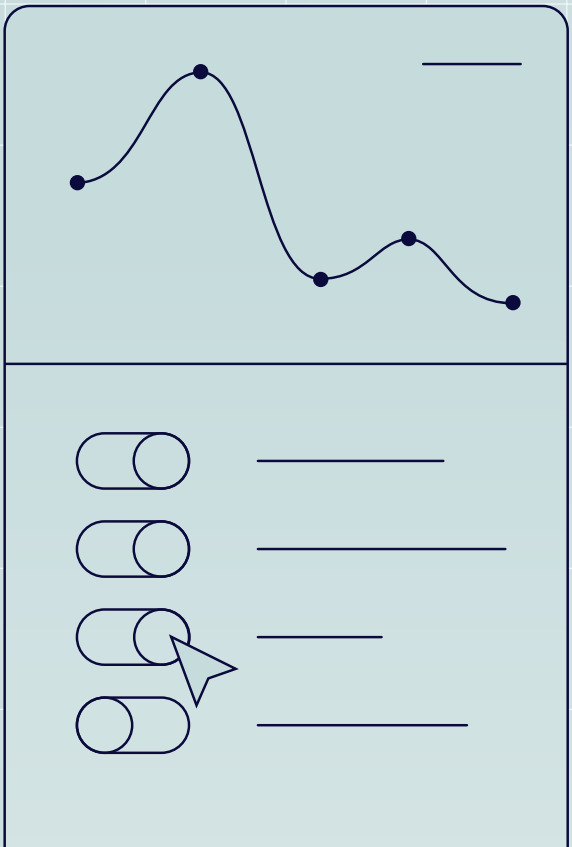


Table of Contents

46%

of businesses worldwide have reported facing fraud[1], corruption and other economic crimes that impacted their bottom lines, within the last two years.

49%

of CEOs place cyber risk at the top of their concerns for the year ahead.

1 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Introduction

The impetus to invest in an anti-fraud solution is greater than ever as companies want to protect themselves and their customers. However, the complexity of deciding whether to buy or build can slow momentum.

Those choosing to develop a fraud solution often do so because they want customizable control over the build, their data and the costs involved. Yet modern off-the-shelf platforms can also cater to these needs without requiring significant investment in research and development.

Ultimately, buying or building a fraud detection solution should be based on a combination of your business's specific needs, the available resources of your internal teams weighted against project priorities and long-term strategy.

This guide will help you make that choice by walking you through key considerations to find the right solution for your business, including questions such as:

- What does successful fraud mitigation look like?
- Is the solution scalable to effectively meet our needs as we grow?
- Do we have the expertise to build and sustain a platform as fraud trends increase in sophistication over time?
- Do we have the necessary resources to commit to updates?
- How reliable will our own solution be versus an off-the-shelf solution?
- How long will it take to build our own solution versus implementing a purchased one?
- Can we wait to develop our own solution, or is this an issue requiring an immediate solution?

Conduct Your Internal Assessment to Build or Buy an Anti-Fraud Solution

Performing an internal assessment is crucial when deciding whether to develop or procure an anti-fraud solution. This comprehensive evaluation process can help organizations seeking to bolster their fraud prevention measures. The process involves the following steps:

1. Identify Urgency and Timeline
2. Assess Internal Capabilities
3. Evaluate the Build Option
4. Consider External Solutions

1. Common Build Regrets

Building a bespoke anti-fraud solution may seem tempting with the promise of data control, customization and cost management, but we've rounded up several of the most common regrets expressed by those who have opted to build rather than buy.

Underestimating Project Complexity

It's a common misconception that building an anti-fraud solution is more affordable than buying one, as this idea often ignores the impact on a business if the project hits unexpected delays or complexities. Building an internal solution will always take longer than implementing one off-the-shelf and requires a substantial investment – and continued commitment – of resources. Most problems arise when the complexity is underestimated, creating a drag on costs, time and any expertise allocated to executing the build. Common hurdles include the development of the technology itself, integration stages, and a lack of the fraud expertise required to deliver meaningful results.

Recommendations

Consider the estimated initial investments in terms of costs, time and other essential resources required to establish a solution. Then, factor in the ongoing resources needed for maintenance, innovation and adaptation to the evolving nature of fraud. This process should be weighed against the immediacy of your needs and existing commitments. Delivery delays, inefficiencies and deflection from other growth projects represent hidden, incalculable costs.

45%

of large IT projects run over budget, on average.

56%

less value than expected is delivered in large IT projects.[2]

2 www.mckinsey.com/capabilities/mckinsey-digital/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value

Not Futureproofing Your Business

Those who build a fraud solution without consulting with fraud experts often do so because they consider their fraud needs specific and confined to one part of a product feature or portion of their customer journey. This results in the building of a point solution that meets immediate needs but does little to futureproof to protect against other fraud attack methods.

When needs inevitably change, you're likely to either scramble to extend your built solution or, more commonly, buy additional point solutions to plug the gaps. This results in a messy tech stack full of integration complications. You might start out wanting to build your own anti-fraud solution but end up with a complex system that relies too heavily on different standalone solutions. The same situation can arise if you buy separate solutions to tackle specific problems instead of opting for a comprehensive fraud detection platform that can grow with your business as needs change.

Recommendations

Look beyond point solutions and immediate needs to consider your long-term growth plans and fraud risk. When evaluating options, ensure that the solutions you consider can protect your customer journey and adapt to changing fraud threats and regulations.

Failing to Critically Assess Resource Constraints

Developing a comprehensive risk detection system demands more resources and skills than many initially expect, including expertise that covers risk management, regulatory compliance, fraud detection, anti-money laundering, cybersecurity best practices, machine learning and data analysis.

Constructing risk models is a complex task, particularly with niche industry insights. Interpreting data requires data scientists and analysts, which means building an entirely new team for many. The most considerable regret we hear in this arena is that companies fail to assess their team's bandwidth and resource constraints critically.

Recommendations

When deciding to build or buy, honestly assess your team's knowledge in these areas and the bandwidth necessary to dedicate time and resources to such an undertaking. The most commonly overlooked skill needed is fraud expertise. For those who desire to build, focus on whether you have the insightful capabilities to stay ahead of fraudsters and other competitive solutions. For those leaning toward purchasing a platform, search for a partner who brings a vast amount of fraud expertise, who is willing to share critical insights and who will be able to help your company navigate emerging fraud trends across your customer base.

Not Fully Considering the Maintenance Needs

The effort of building a fraud solution doesn't stop once it's built, as it will require continuous updates to maintain its effectiveness. Ongoing tasks include fine-tuning risk scores, ensuring the ability to detect new fraud threats and emerging fraud patterns, staying up to date with regulations, and changing fraud behavior and competitive threats for fraud teams.

Continuous maintenance of an internally built solution puts pressure on developer teams. It is a common source of regret, mainly when it competes with the resources needed for primary business objectives. Many who choose to build find that the development velocity of their solution simply can't match the growth of their business.

Recommendations

Since fraud evolves quickly with emerging threats always on the horizon, consider how you will maintain this side project. Can you dedicate the resources and skills needed to keep pace with fraudsters while delivering against primary business objectives? If purchasing, consider whether paid-for solutions, especially point solutions, will be able to adapt and grow in line with your business growth and evolving exposure to fraud.

Conduct Your External Assessment to Buy or Build an Anti-Fraud Solution

Performing an external assessment to determine whether to procure or develop an anti-fraud solution is a critical process that involves a structured approach encompassing five essential steps:

1. Identify functional requirements and long-term fraud needs
2. Define a minimum viable solution and a best long-term solution
3. Diverge by conducting research on all considered solutions
4. Converge research to determine best option
5. Refine needs and create a solutions shortlist

Payment Service Provider Felix Frees Focus for Business Growth

"The effects [of deploying SEON] have been pretty immediate; it's been really eye-opening. ***Ultimately, it has allowed us to have peace of mind to drive our growth initiatives forward at full steam,*** *knowing that we can identify and mitigate the risk from potential fraud."*

Jonathan Kleinmann, Head of Partnerships, Felix

2. How to Weigh the Benefits of Buy Versus Build

Now, let's look at how to pit the benefits of building or buying a fraud solution against one another.

The Rationale for Building	Considerations	What to Look For When Buying
Customizable systems for specific needs You might be focused on targeting one type of fraud, like bot attacks or account takeovers, for example, and are contemplating whether developing a point solution unique to your needs is more or less advantageous than purchasing one.	Custom in-house-built solutions present fixes for particular fraud scenarios but often **fail to adapt to new fraud risks or scale as your needs change.** Further, they do little to prepare your business for growth and can exacerbate fraud elsewhere in your customer journey.	An **anti-fraud solution** that will protect you against all fraud risks, supporting your business across its customer journey as it scales and as fraudsters adapt.
Stronger control You want more granular control over how your system serves your unique fraud needs, with decisioning subjective to your business.	Some fraud solutions offer **custom rules and scoring,** giving your team the transparency and control to finetune based on your business risk appetite.	Look for a solution with out-of-the-box rules to get you started and customizable rules you can easily update. Ideally, this is supported by a whitebox machine learning model for transparency and granular control and a blackbox machine learning model for fully-automated decisioning. Both models should leverage machine learning to provide continuous improvement and accuracy**.**
Data privacy You're concerned about data security and want to keep data within your business to lower risk.	Containing data within your business does not protect against breaches, especially if your business is exposed to fraud attacks. The **risk of data breaches exists in all scenarios** and should be weighed among other factors.	Choose a solution offering data protection and **support across international regions and varying data privacy regulations.** Ensure the solution has a proven track record of reliability, as evidenced by achievements such as SOC2 certifications.
Integration You want your anti-fraud technology to integrate seamlessly with your existing tech stack and to be able to take into account proprietary data sources. Many believe that integration is more successful if built internally.	Many companies need to pay more attention to integration issues when building internal solutions and **face complex issues without the expertise** to resolve them.	Choose an **API-first solution** that can accommodate your data library and integrate at speed easily instead of bending your data to fit the solution. An API solution also means that product updates are available as soon as they are released, with minimal need to reconfigure or update your code.

3. What to Look for When Buying a Fraud Solution

When buying a fraud prevention solution, there are many factors to consider.

Proven Success

The primary outcome to evaluate for an effective fraud prevention platform is a solution's track record. The best way to validate a provider's value is to look at their previous and current customers – ensuring that they serve an industry similar to yours, face the same threats you do – and produce favorable results. Case studies that include vital success metrics and personal validation from customers can show applications of claims.

Data Platform Oxylabs Achieves Greater Efficiency and Significant Time Savings with SEON

"We can accurately detect multiple fraudulent accounts without manual effort and with better accuracy. ***Seeing an 80% time saving on manual reviews and an 80% drop in manual queries*** *culminates in a lot of time saved for other business functions."*

Vaidotas Sedys, Head of Risk Management, Oxylabs

oxylabs®

Expertise to Stay Ahead of Evolving Threats

Purchasing an anti-fraud solution isn't just about buying technology; it's about finding a partner committed to your success. Look for a well-informed, trusted advisor who stays abreast of changing fraud patterns, regulations and evolving exposure for companies like yours and knows how to protect against threats.

A Solution That Will Grow With You

Point solutions may seem the most straightforward route, but they cannot expand with your business and scale up to meet changing exposure to fraudsters. When evaluating solutions, consider those solutions that grow with you and can update regularly with minimal impact on your business.

The Ability to Customize to Your Needs

While specific commercial solutions offer customization, they may align differently with your business processes and requirements. Look for pre-set, out-of-the-box rules to get you started, plus the ability to fully customize rules and update them as your fraud protection needs change. Ensuring that your provider offers expertise to set you up with the rules and decisioning you need is the quickest way to optimize for success.

Transparent Machine Learning

Some fraud protection solutions are augmented with machine learning to quickly identify fraud patterns and help your business automate decisions while removing manual workloads. However, certain machine learning algorithms lack transparency to help your team understand the rationale behind risk choices, meaning you aren't informed or in control of the rules that govern your fraud exposure. Be sure to check solutions for transparent decisioning and whitebox and blackbox machine learning to keep you in control.

Regular, Low-Impact Updates

Your solution should be regularly updated to comply with the latest regulations and stay ahead of competitor advancements and fraudsters' sophisticated methods. You'll need to examine these updates' impact on usability, function and continuity.

API Integration

Opt for an API-first solution to avoid integration challenges. A 'plug-and-play' platform enables integration at speed backed by a provider that grants you access to a team of experts who can support and optimize integration, deployment and beyond.

A Simple Interface

One reason for poor adoption and deployment of a new platform is that it's too hard for a new team to operate. This learning curve can be solved with a user-friendly interface that your fraud team can intuitively understand, leveraging data insights and quickly reviewing or managing user actions in one platform – in addition to interfacing for multiple teams. If purchasing, look for a solution that supports beyond just subject matter experts, as fraud is a cross-departmental problem.

4. Questions to Ask Your Sales Advisor

Expertise

- How long has your organization been operating?
- What fraud expertise and skill set does your team have?
- How will you support my team?
- How aware are you of changing fraud threats, and how can you protect me?
- What customer case studies and proof of success can you show me?

Fraud Protection Coverage

- How will it support our business as it scales and adapts to changing fraud exposure?

Customization

- How customizable is your platform?
- Do you have customizable fraud rules and risk-scoring systems?

Machine Learning

- Is your risk decisioning supported by machine learning?
- Is that machine learning transparent?
- How does your solution tackle false positives and avoid declining safe transactions?

Maintenance and Updates

- How often do you maintain and update the solution to adapt to evolving fraud threats and changing regulations?
- How are those updates made, and how will you support us with their adoption?

Integration

- How long does integration take, and what support do you offer?
- Are your integration times expedited through the use of APIs?

Cost

- How is pricing structured, and are their tiers involved?
- How does the fee break down between implementation and ongoing maintenance?

The Choice is Yours

Many businesses underestimate the effort and long-term technical maintenance required to build a fraud solution from scratch. Fraud is an ever-evolving problem with increasingly sophisticated actors and tactics. As a result, the need to stay one step ahead inevitably draws companies away from where they should spend their time – building and selling products for their customers – and instead, concentrate their resources on the bad actors putting their business at risk.

Online Lender Solventa Decreases Fraudulent Transactions, Cuts Costs and Increases Effectiveness

*"SEON's implementation resulted in a **25% drop in fraudulent transactions while also showing a 15% increase in the effectiveness of the machine learning model,** enabling better overall fraud detection. This immediately equated to savings on costly biometric and ID validations, fewer portfolio losses and increased productivity in terms of approvals."*

Lucrecia Vera, Partner, Solventa

Solventa

At SEON, our entire business model centers around staying ahead of fraudsters for our customers, letting them focus on growing their business while allowing we take care of fraud prevention in real time.

Find Out How SEON Can Stop Fraud Now →

SEON

GUIDE

Buy Versus Build: What to Consider When Assessing Fraud Solutions