SEON

GUIDE

SEON Fraud Trends 2024

YOUR FIRST LINE OF DEFENSE
AGAINST ONLINE FRAUD

INFO@SEON.IO

WWW.SEON.IO

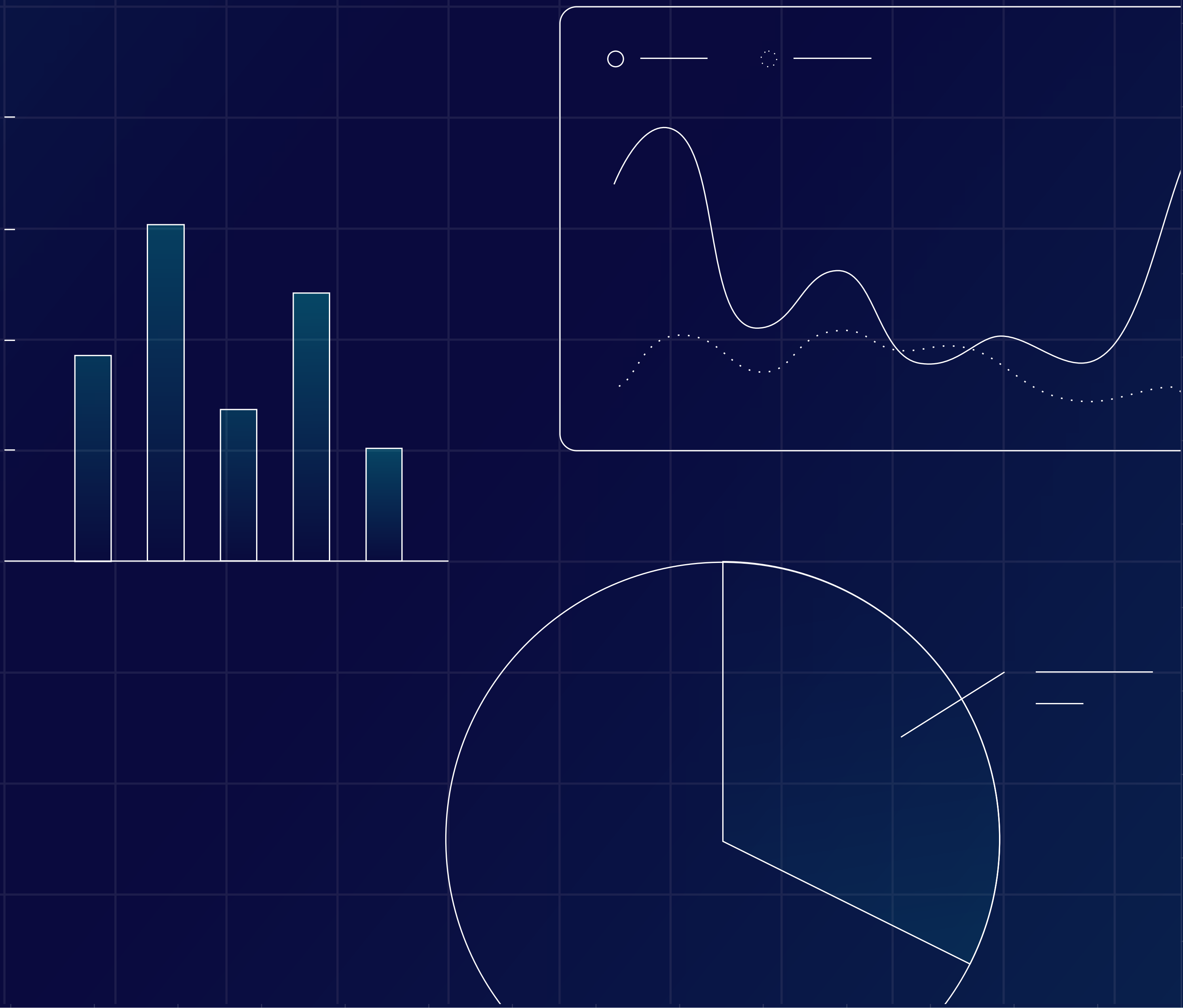


Table of contents

Executive Summary

87% expect the volume of fraud to increase in 2024

71% believe AI will be the biggest challenge for fraud prevention in the year ahead

73% expect an uptick in volumes of synthetic fraud, the creation of new identities by combining real and fake information, versus other fraud types

57% of fraud experts plan to increase their spending on anti-fraud solutions in 2024

86% expect the biggest blocker to fraud investment to be cost

Introduction

The volume, cost, and complexities of fraud are on the rise, and the increase in sophistication and frequency of fraud is accompanied by significant revenue threats that companies can no longer afford to ignore. The ramifications of negative business and customer impacts make fighting fraud a top priority heading into 2024.

With the onus on leaders to step up fraud prevention, protection and mitigation efforts, we surveyed our customers and partners to understand the central challenges better. Here is a compilation of the best practices and trends to fuel your fraud prevention strategy - to stop fraud before it happens - for the year ahead.

In this guide we'll explore:

- Predictions for the volume and costs of fraud
- The types of fraud increasing in volume and velocity
- The biggest threats to fraud prevention efforts
- Best practices for investing in comprehensive fraud protection

With these insights, we aim to help your business prepare best. Our fraud specialists are ready to share their knowledge for a more detailed and customized exploration of your fraud issues.

Speak to a Fraud Expert →

Research Methodology

Insights included here have been derived from a series of industry polls surveying 316 cross-industry customers, with an additional seven participants contributing responses to a more extensive edition. This is supplemented by SEON's independent research, the collection of knowledge from fraud experts, and the shared experiences of our global customer base.

Job Function	Industry
CSuite/Founder	Banks
Director of Fraud/Risk	Insurance
Fraud/Risk Manager	Digital banks
Finance/Analyst	Lending, BNPL
Operations/Product management	Gambling
Compliance/Legal	eCommerce

As your business's first line of defense against online fraud, SEON's end-to-end platform proactively stops fraud earlier by combining advanced digital footprinting with a fully customizable machine learning engine to ensure real-time fraud prevention without impacting your customers' user experience.

With a trusted track record among over 5,000 global companies, SEON reviews billions of transactions daily, resulting in nearly $200 billion in cost savings.

$200+

billion saved in cost

1.7+

billion transactions reviewed daily

5,000+

global companies served

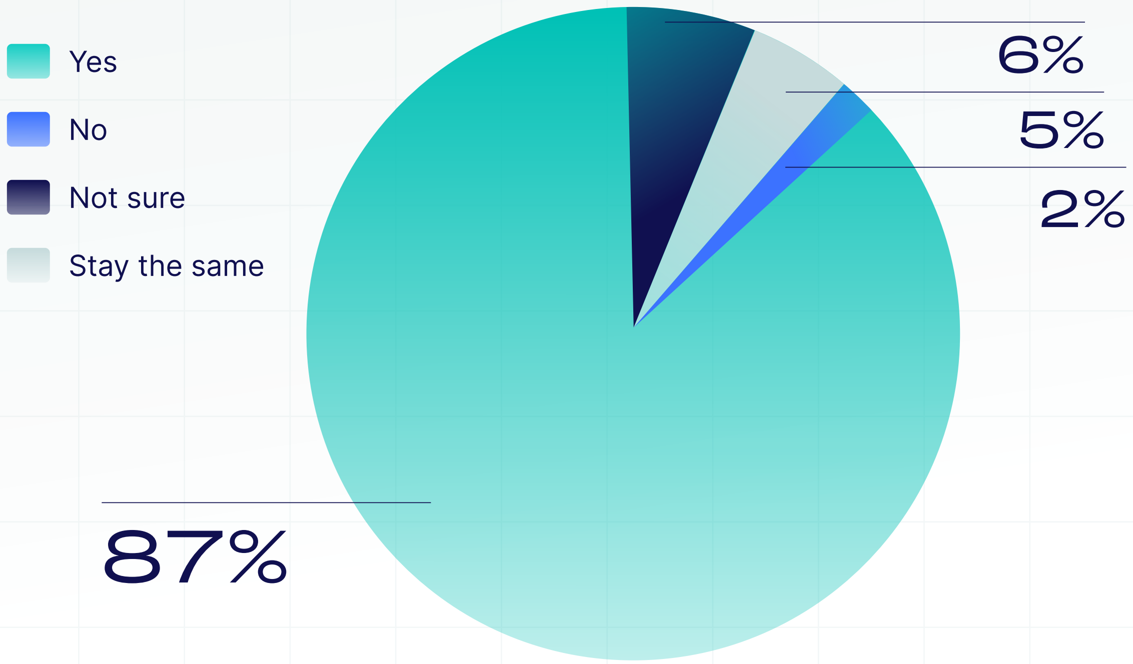
1. Increasing Fraud Volume Trends

Responses from the industry were almost unanimous – 87% of the industry experts surveyed expect an uptick in fraud in the year ahead.

This prediction follows a year in which the volume and types of fraud increased. In 2023, 50% of our surveyed industry players reported that the volume of fraud they encountered rose, while 60% saw the number of fraud types expand.

Interestingly, this was not mirrored by a rise in the cost of fraud, which only 30% of our customers experienced. It should be noted that our survey respondents are predominately SEON customers and are, therefore, proactively protecting against fraud.

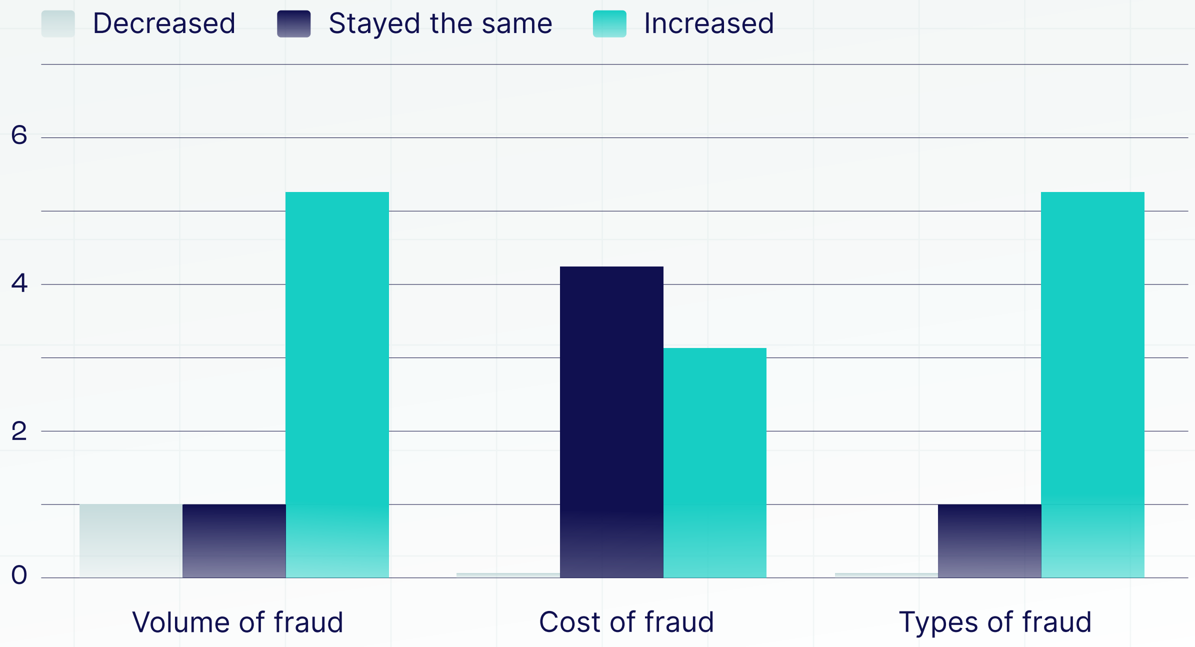
Will the Volume of Fraud Increase in 2024?



1.1. Preparing for the Predicted Rise in Fraud Volumes

Automating fraud detection will reduce the manual work burdens, enabling fraud and risk management teams to benefit from new levels of efficiency, precision and safety. Anti-fraud solutions that leverage artificial intelligence (AI) and machine learning (ML) support automated and lightning-fast risk decisioning.

In the last year, how has the volume, cost and type of fraud changed?



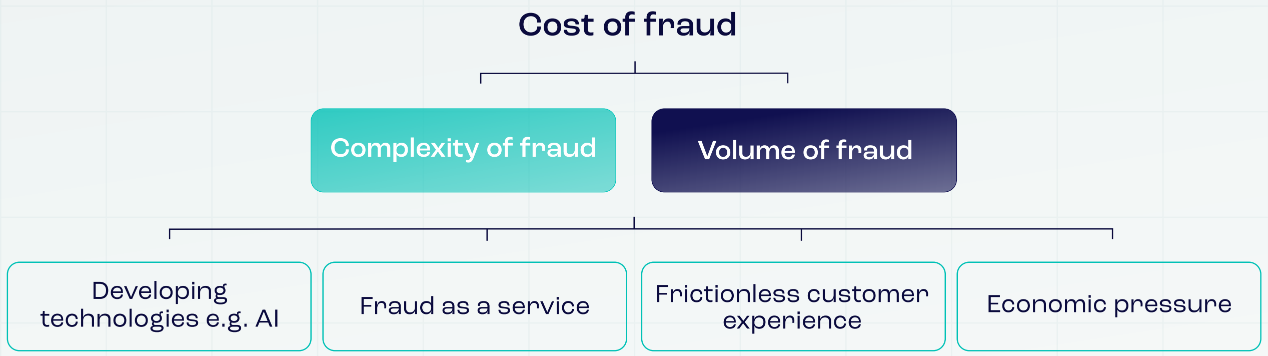
Combat Rising Fraud Volumes with AI →

1.2. What's Driving the Increase in Fraud?

The increased complexity and volume of fraud is being driven by several factors that overlap, including:

Innovative Technologies, Including AI

The advancement of innovative technologies, especially AI, along with widespread browser anti-fingerprinting extensions, bots, automation tools and proxies, are making it easier to carry out mass fraud attacks.



Fraud as a Service

Fraud as a Service (FaaS) is a popular business model where professional fraud-related services are offered online to paying clients.

Fast, Frictionless Transactions

The need for real-time transactions and a frictionless customer experience means that fraud teams must make lightning-fast decisions. If your team lacks the right data and technology, your company faces higher fraud rates, missing out on genuine transactions and more dissatisfied customers.

Economic Pressure

As an opportunistic pursuit, fraud rates are expected to rise in correlation with the downturn in global economics. Last year witnessed $485.6 billion in losses attributed to fraud scams worldwide[1] – and with mounting economic pressure forecast, fraud rates are expected to increase at around 3% in the year ahead.[2]

> *"The digital age is a double-edged sword. We've seen technological advances, online communications, and the growth of remote working provide unparalleled efficiency and convenience to all those using online shopping, banking, gaming and other services. These same factors create new opportunities for fraudsters, meaning businesses' anti-fraud solutions are more important than ever.*
>
> **Tamas Kadar, CEO and Co-founder, SEON**

1.3. Cost of Fraud

With worldwide fraud costs at $5.13 trillion each year[3], climbing a steady 56% over the last decade[4], much of this growth is attributable to long-term social and technological factors and the effects of economic cycles.

On average, businesses lose five percent of their annual revenues to fraud[5], but this is just the tip of the iceberg. While the cost of fraud varies across companies, it's typically more than leaders think. The traditional approach of focusing solely on financial losses fails to accurately depict the consequences of fraudulent activities. The true – and total – cost of fraud can extend beyond these losses, profoundly impacting core pillars of business functionality, such as operational efficiencies, compliance, customer experience and scalability.

Cost and Frequency of Global Fraud in Business

52%

of companies with a global annual revenue of over $10 billion experienced fraud – with one of five companies reporting losses of $50 million or more, over the last two years.[6]

38%

of companies with revenues of $100 million or less experienced fraud – resulting in costs for one in four companies above $1 million, within the same timeframe.

[1] https://finance.yahoo.com/news/nasdaq-ceo-financial-crime-is-now-a-multitrillion-dollar-epidemic-100545542.html

[2] www.imf.org/en/Publications/WEO#:~:text=Description%3A%20The%20baseline%20forecast%20is,to%201.3%20percent%20in%202023.

[3] www.crowe.com/global/news/fraud-costs-the-global-economy-over-us$5-trillion

[4] www.accountancydaily.co/global-fraud-costs-balloon-ps389-trillion

[5] www.accountingtoday.com/news/organizations-lose-5-of-revenue-to-fraud-every-year

[6] www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

Fraud Predictions: The Biggest Threats for 2024

1. Top threats

71%

Rise of AI

57%

Increase in fraud sophistication

2. Second biggest threats

71%

Increase in fraud volumes

71%

Manual demands of fraud

3. Lowest threats

29%

Changing business models

14%

Changing regulation

2. AI Will Be The Biggest Threat To Fraud Protection

According to 71% of the industry experts we surveyed, AI is predicted to be fraud's biggest threat, followed by fraud sophistication, volume and manual demands.

With AI enabling fraudsters to carry out more sophisticated attacks, it not only contributes to an increase in the volume of fraud but also amplifies the demands for manual transaction reviews by fraud teams. Lacking the proper anti-fraud protection and prevention strategy renders businesses more vulnerable and exposed than ever before. While fraudsters have quickly deployed AI as an efficiency tool, particularly in phishing, fraud fighters are innovating to use AI to enhance fraud prevention resiliency.

2.1. How Are Fraudsters Using AI?

SEON customers have seen fraudsters using AI to create fake identities, generate false information, create phishing emails, conduct fraudulent transactions and other fraudulent actions. AI-based threats come in a variety of forms, including:

- **Automated attacks:** When testing large datasets of stolen credit cards or log-in credentials, fraudsters are using AI to automate account takeover attacks with efficiency at scale.
- **Behavioral biometrics spoofing:** Fraudsters are leveraging AI tools to bypass security mechanisms and defenses designed to spot behavioral anomalies.
- **Deepfake technology:** This form of AI-based technology is being used to impersonate individuals.
- **Sophisticated phishing attacks:** Using generative AI, fraudsters create compelling and convincing content for illicit individuals to click on bad links.
- **Adversarial attacks:** Fraudsters exploit machine learning model vulnerabilities to change input data and produce misclassifications.
- **Sophisticated social engineering attacks:** Fraudsters use AI tools to gather large amounts of data to inform powerful social engineering attacks.

2.2. How Fraud Fighters Can Use AI

Comprehensive anti-fraud solutions leverage the power of AI to analyze large-scale data points, gain clear insights into decision-making and deliver control over customizable risk thresholds according to your business needs. This reduces the need for manual review processes and speeds the detection of real-time fraud patterns and operations.

Good anti-fraud solutions protect your customer's journey and aren't just point solutions targeting one part of your business flow. While many fraud prevention solutions include AI, you want to opt for one that uses whitebox machine learning for transparent AI rationale. Whitebox machine learning offers transparent decision-making models, providing clarity and explainability. This transparency ensures enhanced scrutiny, accountability and confidence in outcomes, empowering your risk teams with a deeper understanding of how conclusions are reached.

With AI fraud prevention solutions rapidly growing in popularity, SEON's whitebox machine learning rules have increased over 30% in the past year alone, supported by a 46% increase in blackbox rulings.

30% whitebox machine learning rules increase

46% blackbox machine learning rules increase

Improve your fraud detection with SEON's whitebox ML →

3. Fraud Types on the Rise

We asked our customers to assess the number of fraud attempts they experienced across different sectors during 2023 to inform predictions for the year ahead. Here's what they had to say.

3.1. Phishing and Synthetic Fraud Dominated

The most prolific fraud attack reported by our customer base was phishing, followed closely by synthetic fraud at 43% and ID theft at 23%, respectively. The two lower categories of fraud were account takeover, with a 15% increase and money laundering, with a 14% increase. Note that these numbers reflect fraud attempts and unsuccessful attacks, denoting the power SEON has to stop fraud in its tracks.

Increased Fraud Vectors: 2023

- **Phishing** - 57% increase
- **Synthetic Fraud** - 43% increase
- **ID Theft** - 23% saw an increase
- **Account Takeover** - 15% saw an increase
- **Money Laundering** - 14% saw an increase

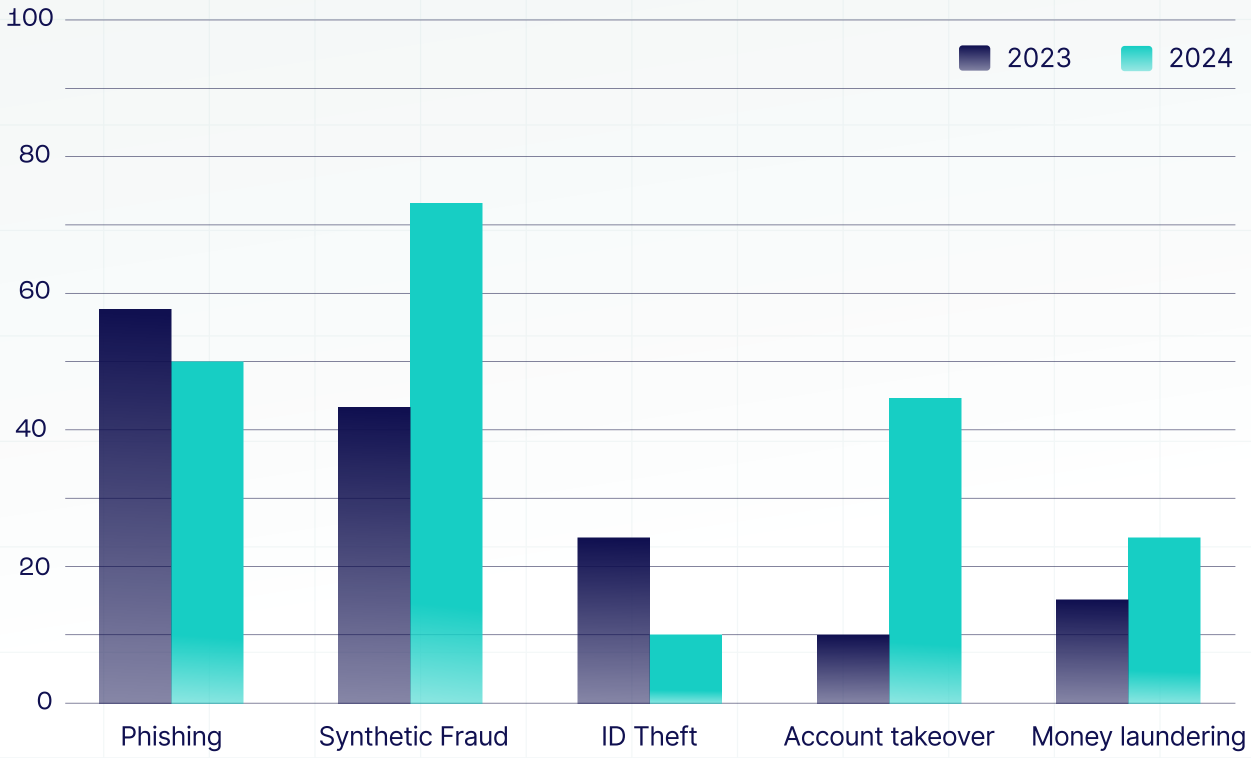
3.2. Fraud Types Expected to Increase in 2024

When asked what types of fraud our customers expect to see in the year ahead, synthetic fraud came out on top with 73%, followed by phishing at 50% and account takeover at 44%.

Predicted Fraud Vectors: 2024

- **Synthetic Fraud** - 73% predicted an increase
- **Phishing** - 50% predicted an increase
- **Account Takeover** - 44% predicted an increase
- **Money Laundering** - 24% predicted an increase
- **ID Theft** - 15% predicted an increase

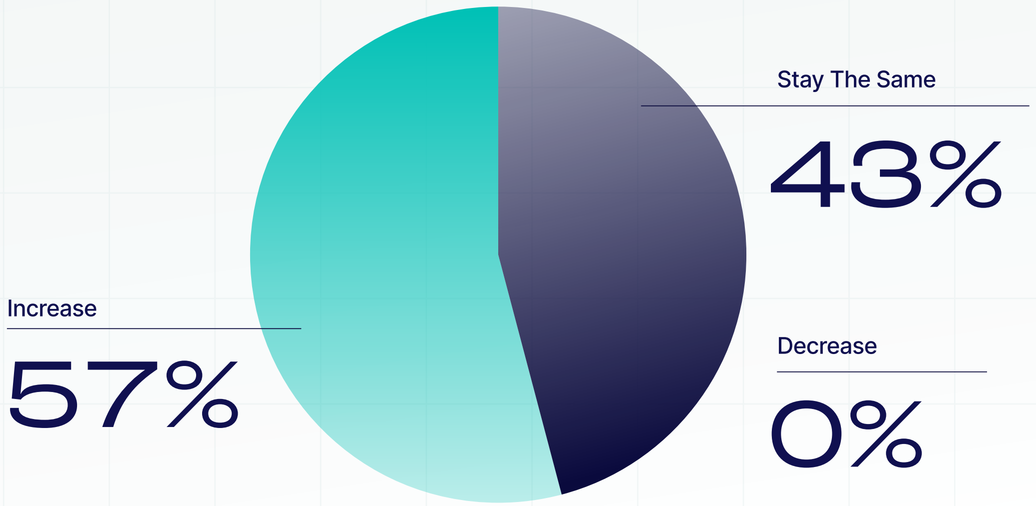
How will the types of fraud increase in 2023 compared to the fraud predictions of 2024?



4. Investment in Fraud Prevention an Imperative

As SEON customers are keenly aware of the increasing sophistication and frequency of fraud, 57% of those surveyed said they plan to increase anti-fraud solutions for the year ahead. Many anticipate expanding their usage of our solution to cover even more use cases and touchpoints to resource their fraud teams for success appropriately.

How will your spending on anti-fraud solutions change in the year ahead?



AI and Red Flag Reporting

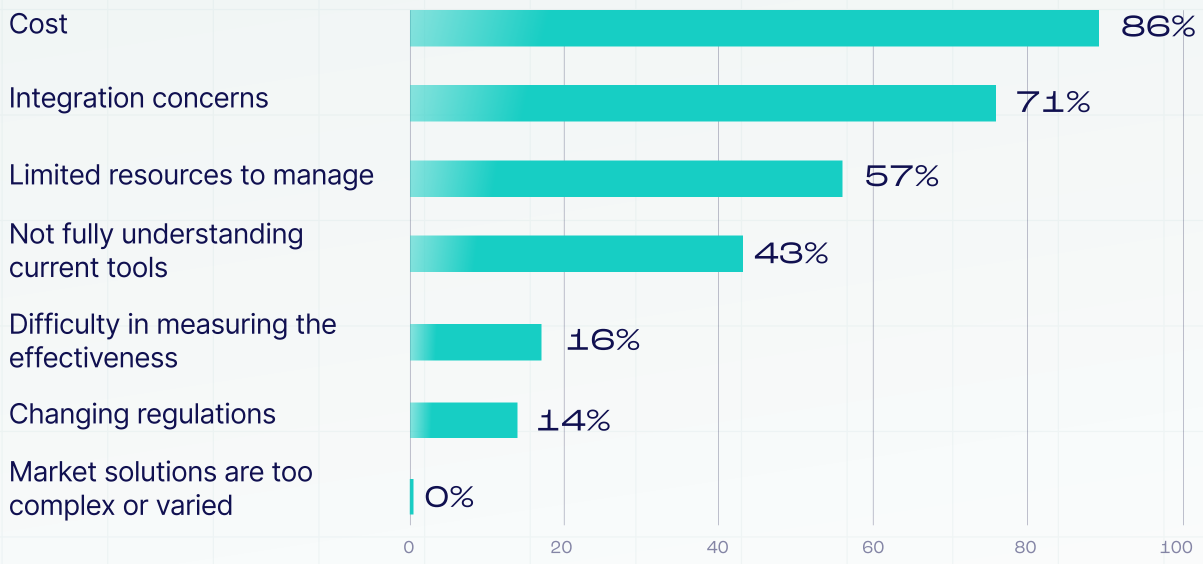
The use of AI and machine learning in anti-fraud programs is expected to double throughout 2023 and 2024, with half of the businesses[7] integrating reporting by exception, anomaly detection and automated red flag monitoring as part of their programs.

[7] www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report

4.1. Common Blockers to Investing in Anti-Fraud Solutions

Given the growing volume of fraud and the need for better protection, we wanted to better understand the blockers for investing in anti-fraud solutions. Chief among reported challenges was cost, with 86% of survey participants citing expenditure as their main reason. This primary challenge was followed by integration concerns (71%), limited bandwidth and resources to manage solutions (57%) and a need for more buy-in from leadership (43%).

What are your company's primary challenges when allocating budget to anti-fraud solutions?



Cost

To protect your business and customers, the impetus to invest in an anti-fraud solution is greater than ever. The choice to deploy a platform should be based on a combination of your business's specific needs, available resources and long-term strategy.

Fraud is a cross-departmental problem that can damage your bottom line if ignored. Factoring revenue threats and other soft costs, including reputational impacts, loss of productivity and potential legal and compliance costs associated with remediation, can further exacerbate and expand fraud's cost footprint.

Mapping the existing cost of fraud against projected fraud volumes can give you a projection that informs you on whether the investment is worthwhile. Opting for a solution with a free trial period and tiered pricing can help define value before you make a more sizable investment.

Integration Concerns

Poor integration experiences can drain time and resources from other projects – and rarely do solutions reach full deployment to maximize return on investment. API-first anti-fraud solutions enable a seamless 'plug-and-play' experience that integrates and interfaces with different tech stacks and variegated systems and adapts as your business scales. Plus, opt for a provider that grants you access to a team of experts who can support and optimize integration, deployment and beyond.

Limited Resources to Manage Anti-Fraud Solutions

Both long-term growth plans and fraud risk appetite are two factors that need to be considered when weighing resource allotment. A lower price tag accompanies many point solutions and solves an immediate issue but does little to futureproof your company against expanding fraud attack vectors. Partnering with an end-to-end fraud prevention solution willing to share critical insights to help your company navigate the current fraud landscape and stay atop of emerging trends is strategic. It can reduce the total cost of fraud, protect your bottom line and result in cost savings - even with limited resources.

Lack of Leadership Buy-In

The true - and total - cost of fraud extends beyond revenue losses. It profoundly impacts core pillars of business functionality, such as operational efficiencies, compliance, customer experience and scalability. As such, fraud is an urgent business problem that demands leadership buy-in. However, efforts to combat fraud can be significantly hindered without leadership buy-in. Look for a finance or compliance department leader to advocate for your cause.

5. SEON's Perspective: Our View on the Big Trends

Tamas Kadar, CEO and co-founder of SEON, shares his thoughts on the broader trends to expect in 2024 based on our experience of global fraud prevention.

Moving Beyond Rigid Rule Systems

Traditional rule-based systems in fraud detection are becoming a thing of the past. Their rigidity and the sheer size of data make them challenging to maintain. Testing accuracy through a confusion matrix is ideal but only feasible with a significant investment, especially in human resources.

Investment in Automation by Implementing Feedback Loops

Machine learning models offer a promising solution but require feedback loops to get smarter. Many teams still struggle with implementing these feedback loops, but this will be one of SEON's focus areas to help fraud and risk teams tackle. Chief risk officers and decision-makers won't be increasing their headcount with traffic spikes. Instead, there will be more investment in automating processes so their people can focus on higher-value tasks.

Human Intelligence and Intuition Are Here to Stay

Fraud specialists often hesitate to depend solely on machine learning due to inherent biases and the continuous need for human oversight. AI won't be eliminating human intelligence just yet. A realistic 2024 focus will be a symbiotic integration of rule-based engines and machine-learning models. This dual approach enhances accuracy and provides the necessary oversight, allowing for intervention when needed. It's about striking the right balance for more thoughtful, efficient fraud prevention.

SEON can help your business tackle rising fraud volumes →

SEON's fraud expertise, real-time data, and AI-enhanced technology can help your business tackle rising fraud volumes

SEON

GUIDE

SEON Fraud Trends 2024

YOUR FIRST LINE OF DEFENSE
AGAINST ONLINE FRAUD

INFO@SEON.IO

WWW.SEON.IO