



# Why AI is the future of online fraud detection

---



# Table of Contents

Introduction .....	2
AI For Online Fraud Detection: The Missing Part Of The Puzzle .....	3
Industry Insights On Why AI Is The Future Of Online Fraud Detection .....	5
How Is AI Used For Online Fraud Detection? .....	8
AI Is The Future Of Online Fraud Detection .....	11





As digital businesses continue to grow, so does online fraud.

The total fraud losses in 2020 amounted to 56 billion USD and U.S. businesses will lose an average of 5% of gross revenue to fraud, making fraud mitigation a core area of focus in businesses of all manner.

At the same time, detecting fraud in real-time is a difficult proposition causing substantially high monetary losses due to late detection of fraudulent behavior. More than 50% of organizations said in a survey that they recover less than only 25% of fraud losses. In addition to monetary losses, late fraud detection causes irreparable damage to brand equity and user trust alike.

Fraudsters are getting more sophisticated in their methods, and it is becoming more difficult for businesses to detect and prevent fraudulent activity. This is where Artificial Intelligence (AI) comes in. AI is the foundation of effective online fraud detection, and businesses must implement AI-based fraud detection strategies to stay ahead of ever-evolving fraud patterns. In this blog post, we will discuss why Artificial Intelligence is the future of online fraud detection, what it entails, and how it can help your business protect itself from sophisticated fraudulent activity.

# AI for Online Fraud Detection:

## The missing part of the puzzle

Up until recently, the primary approach to fraud prevention was centered around human-defined rules coupled with a manual review of potentially fraudulent transactions. While human review of fraudulent transactions might lead to fewer false positives, it, unfortunately, leaves a window of opportunity for advanced and fast-evolving adversarial techniques leading to substantial financial and reputation damage. Therefore, **effective fraud mitigation requires accurate and instant decisioning ability with low false positives.**

**Instant fraud decisioning involves ingesting hundreds of signals**, some from the incoming transaction and some from historical analytics, to decide the appropriate course of action for the transaction as it is happening.

This is where artificial intelligence comes in. Artificial intelligence is ideal for detecting online fraud because it can rapidly and accurately identify automated, increasingly complex fraud attempts.

See Oscilar in action!

[Get a Demo](#)

The best AI-based fraud detection strategies use a combination of supervised and unsupervised machine learning, as well as, an integrated machine learning and rules approach, which enables businesses to quickly identify patterns in fraudulent behavior.

This is important because as fraudsters become more sophisticated, they develop new methods that are difficult to detect using traditional fraud detection methods.

There are several reasons why Artificial Intelligence is the future of online fraud detection:

- 1 AI can help businesses keep up with the increasing sophistication of fraudsters.
- 2 AI-based fraud detection strategies are more effective than traditional rules-only and manual methods in detecting and preventing complex multi-dimensional fraudulent activity.
- 3 Artificial intelligence enables businesses to rapidly and accurately identify fraudulent behavior, which is essential for protecting businesses from loss.



# Industry insights on why AI is the future of online fraud detection

Recent research is shedding light on why AI is the future of online fraud detection. According to the [Association of Certified Fraud Examiners \(ACFE\)](#)'s [Anti-Fraud Technology Benchmarking Report](#), over 60% of organizations will significantly increase the budgets allocated to the adoption of anti-fraud technology over the next two years.

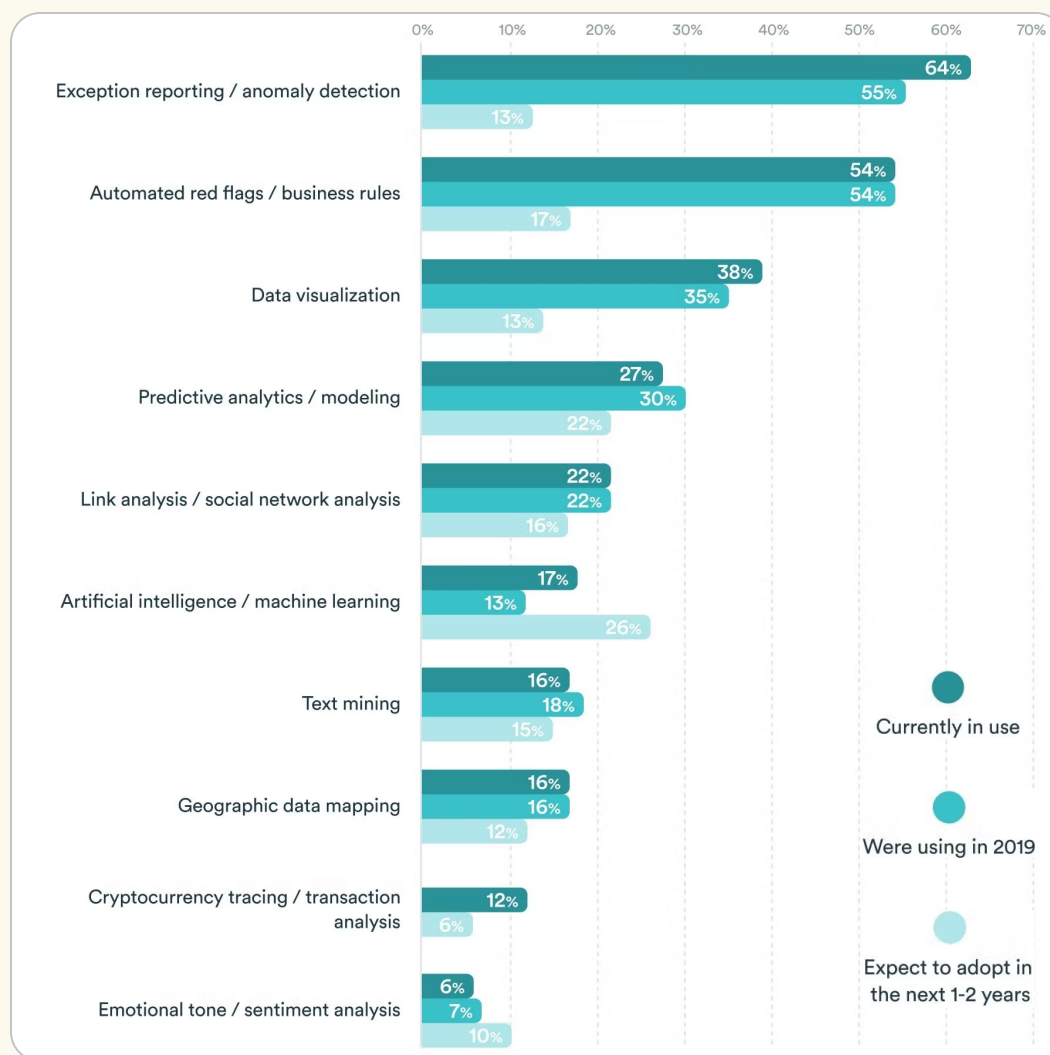
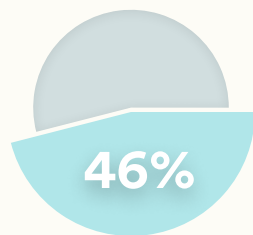



Figure 1. Data analysis techniques organizations use to fight fraud

While currently, only **17% of businesses** employed artificial intelligence to detect and prevent fraud, that number is **expected to jump to 26% by 2023 - 2024**, a growth of almost 53%. The ACFE study found that the use of AI techniques to fight fraud will double over the next two years.

The 2022 [Global Economic Crime and Fraud Survey](#), conducted by PwC, is based on interviews with 1,296 executives across 53 countries and regions around the world to assess how well digital fraud prevention is progressing globally. The report discovered that **46% of surveyed organizations reported experiencing fraud**, corruption or other economic crimes in the last 24 months.



Out of 1,296 executives across 53 countries and regions around the world

 experienced fraud, corruption or other economic crimes in the last 24 months

The report states three critical recommendations made by the survey respondents:

1

Understand the end-to-end lifecycle of customer-facing products.

2

Strike the proper balance between user friction and fraud controls. The dual objectives of keeping false positives as low as possible and catching true fraud can be achieved by applying AI in fraud detection efforts.

3

**Orchestrate data:** It is crucial to consolidate fraud indicators in a central platform, like Oscilar, that can track the end-to-end lifecycle of users (fraudsters or not) and generate meaningful alerts.

To overcome these challenges, businesses should use more machine learning and AI in tandem with prescriptive analytics, as the graph below from the 2018 report shows.

**The financial services and technology industries are finding the most value in Artificial Intelligence (AI) and Advanced Analytics**

To what degree is your organization using and finding value from Artificial Intelligence of Advanced Analytics to combat/monitor for fraud and other economic crimes? (% of respondents who said their organization uses and derives value)

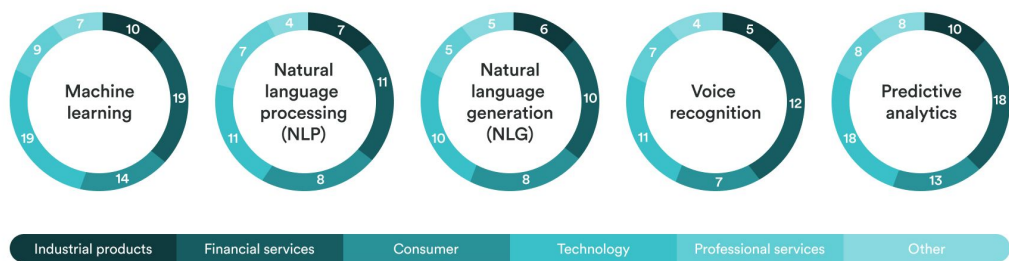


Figure 2. Value of Artificial Intelligence and Advanced Analytics for Online Fraud Detection  
(Source: PwC's 2018 Global Economic Crime and Fraud Survey)

Oscilar's unique approach to combining machine learning with rules, **integrating supervised and unsupervised machine learning techniques**, and allowing the **use of both custom in-house machine learning models with 3rd party fraud scores** in one platform is the future of online fraud detection.



# ARTIFICIAL INTELLIGENCE

## How is AI used for online fraud detection?

Digital businesses with the best track record of defeating internet fraud do the following to apply AI for fraud detection:

1

Use performance insights from high-quality rules to train models using supervised machine learning for detecting fraud attempts quicker than manual approaches.

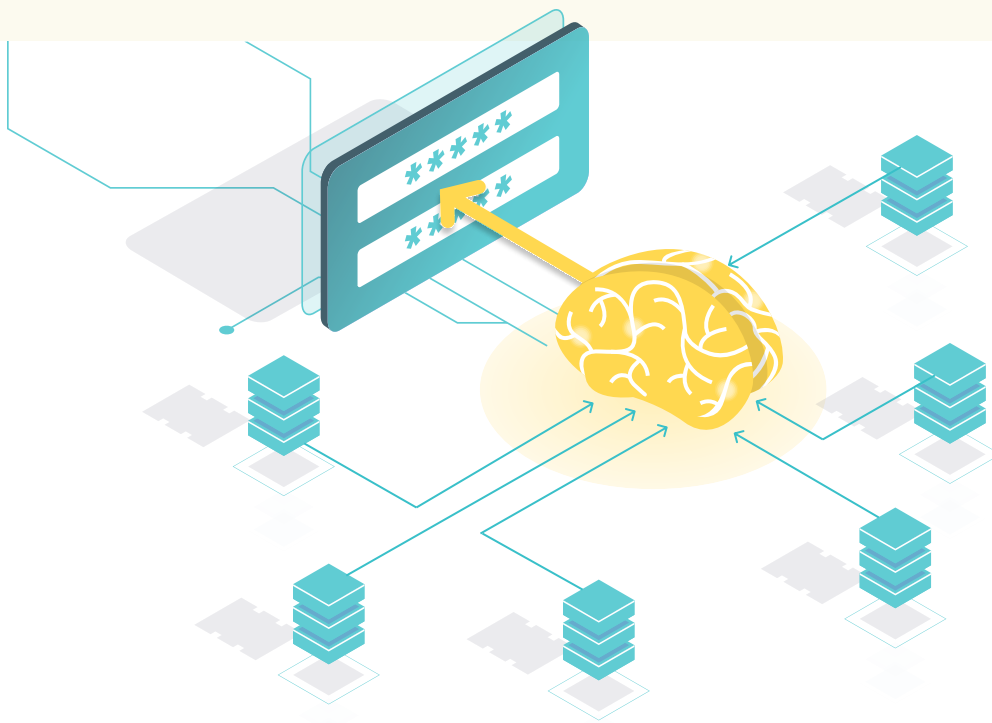
Digital businesses we work with say that they start their fraud detection journeys with rules-based approaches that are easy to put in place. As fraud patterns become increasingly complex, **scaling online fraud detection efforts becomes challenging with a rules-only approach**. This scaling is best achieved by replacing a subset of rules with supervised machine learning models.

Adopting supervised machine learning is easier for some businesses that have data scientists on staff who are trained on the foundational concepts and algorithms. Others might depend on consulting a variety of third-party fraud scores that assess the risk of a user's transaction based on a multitude of signals such as phone, email, online identity, ip address, and more.

2

Integrate supervised and unsupervised machine learning to effectively find anomalies in emerging user transactions.

Integrating supervised and certain unsupervised machine learning techniques is one way AI can be effectively applied for online fraud prevention. While a subset of fraud signals are best modeled by supervised machine learning techniques, certain types of anomaly detection is best achieved with an unsupervised machine learning approach. In our experience, **a more integrated approach to online fraud prevention that combines supervised and unsupervised machine learning can deliver fraud scores that are twice as predictive as previous approaches.**



3

Capitalize on large-scale, universal data networks to complement custom machine learning algorithms to dramatically improve the predictive power of fraud prevention scores.

Often **consulting custom in-house machine learning models is insufficient** to capture a large enough surface area of fraudulent patterns. The most advanced digital businesses are looking for ways to supplement their machine learning models using large-scale universal data sets. Many businesses have years of transaction data they rely on initially for building in-house machine learning models.

However, no business or tool has the best data. Therefore, **supplementing in-house machine learning models with 3rd party fraud scores** that have large-scale universal data networks--often including billions of transactions captured over decades from thousands of customers globally--improves fraud prevention dramatically.

The combination of these three factors forms the foundation of online fraud detection. Digital companies faced with a high risk of fraud leverage online fraud detection platforms, like Oscilar, that have the above functionality, to **enable their fraud experts to have the insights they need to identify and combat fraud early**.

# ARTIFICIAL INTELLIGENCE

## AI is the future of online fraud detection

Fraud detection is hard enough, but it's made much more difficult when the only data available to an organization is limited, fragmented and not appropriately analyzed. **AI is a must-have foundation for online fraud detection**, and platforms built on these technologies need to achieve three things exceptionally well to succeed.

1

First, supervised machine learning algorithms need to be fine-tuned with the invaluable historical performance of high-quality rules data to minimize false positives and scale fraud detection efforts.

2

Second, unsupervised machine learning is required to find emerging anomalies signaling more sophisticated forms of online fraud.

3

Finally, for an online fraud platform to be more effective, it needs to supplement in-house custom machine learning models with 3rd party fraud scores computed using a large-scale, universal data network of transactions in one platform to improve the accuracy of fraud prevention scores.



If you'd like to learn more  
about Oscilar's approach to  
using AI for online fraud  
detection, drop us a note!

**Get a Demo**