Machine Learning and Artificial Intelligence in Fraud Detection and Anti-Money Laundering Compliance

Learn how machine learning and artificial intelligence can help detect and prevent financial crime while keeping you AML-compliant.

Alyssa Abrams

Senior Content Manager at Sumsub

Pavel Goldman Kalaydin
Head of AI/ML at Sumsub

According to Sumsub's 2023 Identity Fraud Report, there's been a10x increase in the number of deepfakes detected globally across all industries from 2022 to 2023, with notable regional differences. Deepfakes are up 1740% in North America, 1530% in APAC, 780% in Europe (inc. the UK), 450% in MEA, and 410% in Latin America. This surge has been caused by the greater accessibility of AI among bad actors. However, where AI is a threat, it also happens to be the solution.

With the growth of generative AI tools, businesses are using new technologies to detect fraud and money laundering. One of them is machine learning and artificial intelligence algorithms.

ML/AI tools can learn complex transaction patterns, enabling businesses to proactively monitor customer behavior, therefore more accurately identifying and preventing risks.

In this article, we'll observe what ML/AI technology is, how it's used in different industries, and how it can be best used to prevent fraud and money laundering.

What is ML/AI?

Machine learning (generally referred to as ML/AI) is a field of artificial intelligence (AI) that enables computers to learn, predict, and make decisions without being explicitly programmed.

ML/AI algorithms are designed to analyze and process vast amounts of data, identify patterns, and make informed predictions or decisions based on this information.

What is AI/ML fraud detection?

AI-powered fraud detection utilizes ML/AI algorithms to analyze data and detect patterns indicative of fraudulent behavior. It gathers data from transactions, user interactions, and historical patterns, preprocesses it, and applies algorithms for anomaly detection and risk scoring. These systems assign risk scores to activities, enabling real-time decision-making like flagging suspicious activities. They are used across various industries to combat fraud, minimizing financial losses and safeguarding customer trust. Continuous learning ensures these systems stay updated with emerging fraud patterns.

The role of ML/AI in the detection of fraud and other criminal activity is growing. Here is how it can be used in the field.

Detection of deepfakes and other spoofed images, videos, and audios

Today, ML/AI plays one of the most important roles in detecting deepfake fraud, which is growing day after day. As deepfake techniques become more sophisticated, so do the detection methods:

1. Detection of artifacts not present in authentic media. Deepfakes often contain certain visual or audio artifacts that are not present in authentic media. Machine learning algorithms can be trained to detect these artifacts by analyzing specific features of digital content, such as inconsistencies in facial expressions, unnatural eye movements, or distortions in sound waves.

2. Detection of deepfake generation techniques. Machine learning algorithms can identify traces left by specific deepfake generation techniques. These models can learn to recognize the unique characteristics introduced during the deepfake generation process.

Behavioral fraud detection

ML/AI can be used to analyze customer behavior patterns in order to detect fraud. This analysis processes a huge set of data, such as usual login times, device types, typical transaction types and amounts, and even styles of keyboard/mouse use. Here machine learning algorithms can be applied in the following ways:

1. Profile-based analysis and anomaly detection. ML/AI algorithms can create profiles based on historical data and customer behavior, and remember patterns of normal behavior for individuals and groups. Trained on historical data, these models can flag suspicious transactions, user activities, and other behavioral deviations. This way, multiple fraud types can be detected, including account takeovers, payment fraud or identity theft.

2. Ongoing learning. ML/AI models can continuously learn and adapt from new data, allowing them to stay up-to-date with evolving fraud techniques.

Document forgery detection

Machine learning can help with document forgery detection in the following ways:

1. Understanding document features. Machine learning models can extract relevant features from documents that are indicative of forgery, including texture, font, signatures, stamps, watermarks, etc.

2. Verification of signatures. ML/AI techniques can be applied to verify signatures, comparing a signature on a document with a reference signature. These algorithms can analyze stroke patterns, pressure, and thus recognize unique features of genuine signatures—differentiating them from forged signatures.

3. Detection of forgery in digital documents. ML/AI models can analyze metadata, digital signatures, or compression artifacts and detect traces of manipulation. These algorithms can also check the textual content of digital documents to identify inconsistencies, plagiarism, or content alterations which indicate forgery.

Identity theft detection

ML/AI is used to detect identity theft by analyzing various data sources, such as account activity, user behavior, biometric data, and historical patterns to identify anomalies, inconsistencies, and other suspicious signals of fraud and identity theft.

Anti-Money Laundering (AML)

In anti-money laundering analytics and compliance, ML/AI can be used for the following:

- Identity verification at onboarding. ML/AI algorithms can assist in verifying client identities by analyzing various data points, including personal information, biometrics, and behavioral patterns.

- Document verification. These models can be trained to analyze documents, such as passports, driver's licenses, and IDs. These systems can extract necessary information from documents, compare it to reference data, and detect potential inconsistencies. They can also flag forged or altered documents.

- Transaction monitoring. ML/AI systems can process large amounts of transaction data.

- Fraud and money laundering detection. By analyzing historical fraud patterns and continuously monitoring transactions in real-time, ML/AI models can identify and flag potentially fraudulent activities.

- Ongoing monitoring. ML/AI algorithms can also be used to continuously monitor customer behavior patterns based on historical data. These algorithms can learn what constitutes normal behavior for each customer, such as typical transaction amounts, frequency, IP addresses, and other factors.

What is rule-based fraud detection?

Rule-based fraud detection is based on predefined rules and criteria. In this approach, specific rules are set up by analysts to flag transactions or behaviors that are considered suspicious or potentially fraudulent. These rules are typically based on known patterns of fraud or unusual activity.

For example, a rule might be set to flag any transaction above a certain monetary threshold, or if a user attempts multiple failed login attempts within a short period. Other rules might involve detecting inconsistencies in user behavior, such as unusual spending patterns or accessing accounts from multiple geographic locations in a short time frame.

Rule-based fraud detection systems are relatively straightforward to implement and understand, as they operate on a set of predetermined guidelines. However, they may lack adaptability to new or emerging fraud patterns and can produce false positives if the rules are too rigid or outdated. Therefore, it’s important to retrain these models frequently to enhance adaptability. Additionally, implementing an additional check for users, such as Liveness, can be beneficial. Moreover, ML/AI algorithms may assist in creating these specific rules, especially if a business utilizes rule-based fraud detection.

ML/AI-based vs rule-based fraud detection

AI-powered fraud detection uses ML/AI algorithms to analyze large volumes of data and identify patterns indicative of fraudulent behavior, adapting to evolving fraud tactics. It involves training models on historical data to detect anomalies and assign risk scores to activities, enabling real-time decision-making.

In contrast, rule-based fraud detection relies on predefined rules and thresholds to flag suspicious activities, lacking adaptability to new fraud patterns.

Combining both approaches can leverage the strengths of each, providing a robust fraud detection system capable of capturing a wide range of fraudulent activities while minimizing false positives.

What are the benefits and challenges of AI-based fraud detection?

The benefits of artificial intelligence for fraud detection include enhanced accuracy in identifying fraudulent activities, real-time detection and prevention capabilities, scalability to handle large volumes of data, and adaptability to evolving fraud tactics.

However, the challenges include:

- AI hallucinations
- The need for extensive data preprocessing and labeling
- The risk of false positives and false negatives
- Potential biases in data or algorithms

ML/AI in transaction monitoring

A reliable Transaction Monitoring tool is essential for any business today, especially in the financial industry—and ML/AI may be of great help for transaction fraud detection.

ML/AI systems can process large amounts of transaction data, detect behavioral anomalies, and flag suspicious signals in financial and non-financial transactions (e.g. fiat vs crypto, or vice versa), customer profiles, and historical patterns.

These models can learn from labeled data to identify patterns that indicate money laundering or other fraudulent activities, like account takeovers, buy-now-pay-later schemes, and card-not-present attacks. They can also learn from unlabelled data (e.g. by clustering) and use it to detect unusual patterns.

Businesses following AML regulations often want to use rules that flag certain transactions as suspicious. If AI is used to enforce these rules, the models arrive at conclusions without explaining how they were reached. Therefore, the challenge for machine learning in AML compliance is to create reliable AI-based AML software that provides understandable rules explaining the model’s conclusions.

The future of ML/AI

According to Statista, the market for artificial intelligence (AI) is expected to grow substantially in the coming years. Currently valued at $100 billion, the market is expected to grow twentyfold by 2030, up to nearly two trillion USD.

Today the AI market covers a vast amount of industries and professional fields, including financial services, supply chains, marketing, product making, research, health tech sector, as well as EduTech. More fields are expected to adopt artificial intelligence within their business structures.

As democratization of modern technologies continues, digital fraud and deepfakes become more sophisticated and easier to create. This can’t stay unnoticed. Regulators worldwide are expected to start paying closer attention to AI-related technologies and their application in business.

In light of the above, today companies are recommended to:

- Closely monitor new fraud trends
- Monitor AI-related AML regulations
- Invest in technological development.

AI software for AML and fraud detection

When evaluating an artificial intelligence software for fraud detection and AML, it’s important to consider the needs of your organization. In general, the following features make for a reliable AML AI solution:

1. Security standards. A reliable software should adhere to robust security standards to protect sensitive information and ensure data privacy. It should have measures in place for data encryption, access controls, authentication, and secure data storage.
2. Rule-based alerts. A good software should enable creating and managing rule-based alerts and scenarios that flag suspicious activities based on predefined rules and thresholds. These rules can be customized to align with specific regulatory requirements and risk profiles.
3. Risk scoring. A reliable software should assign risk scores to customers’ profiles, historic activity and transactions based on their likelihood of involvement in money laundering or fraudulent activities. It should

prioritize alerts and investigations based on the assigned risk scores, allowing analysts to focus on high-risk cases.

4. Real-time monitoring and alerts. A good tool should provide real-time monitoring capabilities through a customer's lifecycle to detect suspicious activities as they happen at any stage.
5. Hidden networks analysis. The software should offer entity link analysis to uncover connections between customers, accounts, transactions, and other entities. It should help identify complex network patterns and hidden relationships.
6. Visualization and reporting. The software should offer a convenient UI and UX with dashboards and reporting tools to present analysis results in a clear manner.
7. Flexibility. The software should be flexible and scalable, capable of handling large volumes of data and adapting to changing regulatory requirements.
8. Regulatory compliance support. The software should assist with compliance requirements by incorporating regulatory rules and guidelines.

All of the above are offered by Sumsub. Sumsub's Liveness Detection can outperform humans in spotting enhanced photos. Moreover, in October 2023, Sumsub released the industry-first "For Fake's Sake", a set of machine learning-driven models that enable the detection of deepfakes and synthetic fraud. This tool is available for free to download and use by all.

Moreover, you can uncover interconnected patterns of suspicious activity on your platform using Sumsub's AI-powered Fraud Network Detection solution, which is a great tool to spot deepfake networks. This tool provides you with the ability to identify fraud networks before the onboarding stage through AI, allowing you to apprehend an entire fraudulent network rather than just a single fraudster.

FAQ

How is AI used for fraud detection?

AI is used for fraud detection by employing advanced algorithms to analyze large volumes of data, detect patterns, anomalies, and suspicious behaviors indicative of fraudulent activity across various industries and domains.

What is the best machine-learning algorithm for fraud detection?

There isn’t a single ‘best’ machine learning algorithm for fraud detection; rather, a multi-layered approach—including a combination of algorithms such as anomaly detection methods, decision trees, random forests, and neural networks—is often used to achieve optimal performance depending on the specific characteristics of the data and the nature of the fraud being targeted.

Do banks use ML/AI to prevent fraud?

Yes. ML/AI can be used in banking and financial services as follows:

- AI fraud detection as part of AML compliance
- Risk assessment and credit scoring
- Trading and investment strategies
- Chatbots and virtual assistants for customer support.

How does ML/AI detect fraud on bank payments?

ML/AI detects fraud in bank payments by analyzing transaction data, identifying patterns, anomalies, and suspicious behaviors indicative of fraudulent activity.

What is AI in AML?

Artificial Intelligence in anti-money laundering stands for the use of AI to analyze and detect fraud, money laundering, and other financial crimes.

How can AI detect money laundering?

AI systems analyze vast amounts of data in real-time and identify unusual behavioral or transactional patterns that humans may miss.

sumsub

Start exploring Sumsub today.

Get started