More resources /

Risk management

Contact sales >

Radar

How machine learning works for payment fraud detection and prevention Get started with Stripe >

Last updated 27 June 2023

How is machine learning used in fraud prevention and detection? Machine learning fraud certification **Examples of machine learning for** fraud detection In-person payments

What is machine learning?

Introduction

Mobile payments E-commerce Other relevant use cases

Get started with Stripe >

Beyond payment fraud's immediate financial losses, businesses also face potential erosion of customer trust and loyalty, as well as increased scrutiny from regulators and law enforcement agencies. To combat this growing threat, organisations are turning to machine learning. Machine learning, a subfield of artificial intelligence (AI), offers a powerful and adaptive solution to tackle the complex and evolving nature of payment fraud. By mobilising large datasets and advanced algorithms, machine learning can identify patterns and anomalies that indicate fraudulent behaviour, making it possible for businesses to detect and prevent

Global online payment fraud losses in 2022 reached US\$41billion, a figure expected to

balloon to US\$48 billion by the end of 2023. Combating payment fraud – and mitigating its

devastating financial and reputational damage - has become a top priority for businesses.

fraud in real time. Ultimately, machine learning can help businesses uphold a secure environment around payments to protect their customers, revenue, and reputation. We'll cover the benefits of machine learning for fraud prevention and how businesses can use this tool in different payment scenarios.

• What is machine learning? • How is machine learning used in fraud prevention and detection?

give computers the ability to learn from data, identify patterns from within the data, and make

What's in this article?

- Examples of machine learning for fraud detection
- What is machine learning? Machine learning is a subfield of AI that focuses on developing algorithms and models that

decisions based on their learnings.

Machine learning fraud certification

There are three main types of machine learning:

Supervised learning Supervised learning is a type of machine learning in which a computer is taught to make

or decisions for new data that it has not seen before.

analyse this data and discover underlying patterns.

the teacher provides the student with a set of problems and correct answers to those problems, and the student studies these examples, learning to recognise patterns. When the student faces a new problem, they can use their previous knowledge to find the correct answer. In supervised learning, the computer algorithm is given a dataset with both the input data

(problems) and the correct output (answers). The algorithm studies this dataset and learns

the relationship between the input and output. Eventually, the algorithm can make predictions

predictions or decisions based on examples. Think of it like a student learning from a teacher:

Unsupervised learning

Unsupervised learning is a type of machine learning in which a computer learns to identify

patterns or structures in data without being given any specific examples or correct answers.

relationships. In unsupervised learning, the computer algorithm is given a dataset with only

input data, without any corresponding correct outputs (answers). The algorithm's job is to

Reinforcement learning is a type of machine learning in which a computer learns to make

decisions by interacting with an environment and receiving feedback in the form of rewards

trick correctly, you offer it a treat (a reward), and when the dog doesn't do the trick, you may

or penalties. Think of how you might train a dog to perform tricks. When the dog performs the

This is similar to how a detective would try to solve a case without any initial leads – by looking for clues and connections in the available information to uncover hidden patterns or

Reinforcement learning

and autonomous vehicles.

Anomaly detection

investigation.

Text analysis

or scams.

Identity verification

emerging fraud patterns.

security and customer experience.

Network analysis

give it a gentle correction (a penalty). Over time, the dog learns to perform the trick correctly to maximise the number of treats it receives. In reinforcement learning, the computer algorithm, often called an agent, explores an environment and makes decisions. For each decision that it makes, it receives feedback as either a reward or a penalty. The algorithm's goal is to learn the best strategy, or policy, to make decisions that maximise its cumulative rewards over time. It does this through trial and error, adapting and improving its strategy based on the feedback.

Machine-learning techniques are used in many different scenarios, including natural

language processing, image and speech recognition, medical diagnosis, financial analysis,

How is machine learning used in fraud prevention and detection? Increasingly, machine learning is being used in fraud prevention and detection due to its

ability to analyse large quantities of data, identify patterns, and adapt to new information.

Some common applications of machine learning in fraud prevention include:

recognise legitimate transactions and flag suspicious activities that may indicate fraud. Risk scoring Machine-learning models can assign risk scores to transactions or user accounts based on

various factors, such as transaction amount, location, frequency, and past behaviour.

their resources and focus on specific transactions or accounts that warrant further

Higher risk scores indicate a higher likelihood of fraud, enabling organisations to prioritise

Machine-learning algorithms can identify unusual patterns or deviations from normal

behaviour in transactional data. By "training" on historical data, the algorithms learn to

Fraudulent actors often collaborate and form networks to carry out their activities. Machine-learning techniques, like graph analysis, can help uncover these networks by analysing relationships between entities (such as users, accounts, or devices) and identifying unusual connections or clusters.

Machine-learning algorithms can analyse unstructured text data, such as emails, social

media posts, or customer reviews, to identify patterns or keywords that may indicate fraud

Machine-learning models can analyse and verify user-provided information, such as images of identification documents or facial recognition data, to ensure that an individual is who they claim to be and prevent identity theft. Adaptive learning One of the key strengths of machine learning is its ability to learn and adapt to new

information. As fraudulent actors change their tactics, machine-learning models can be

retrained on new data, allowing them to stay up to date and better equipped to detect

Using machine learning in fraud prevention can be a powerful way for organisations to

enhance their detection capabilities, reduce the risk of false positives, and improve overall

Commits Human intervention Leads to Scammer Rules **Detection**

Machine learning approach to fraud detection

Leads to (Constantly improving)

Fraud

Executes

normalisation.

input to output).

cybersecurity specialists.

Credit card fraud detection

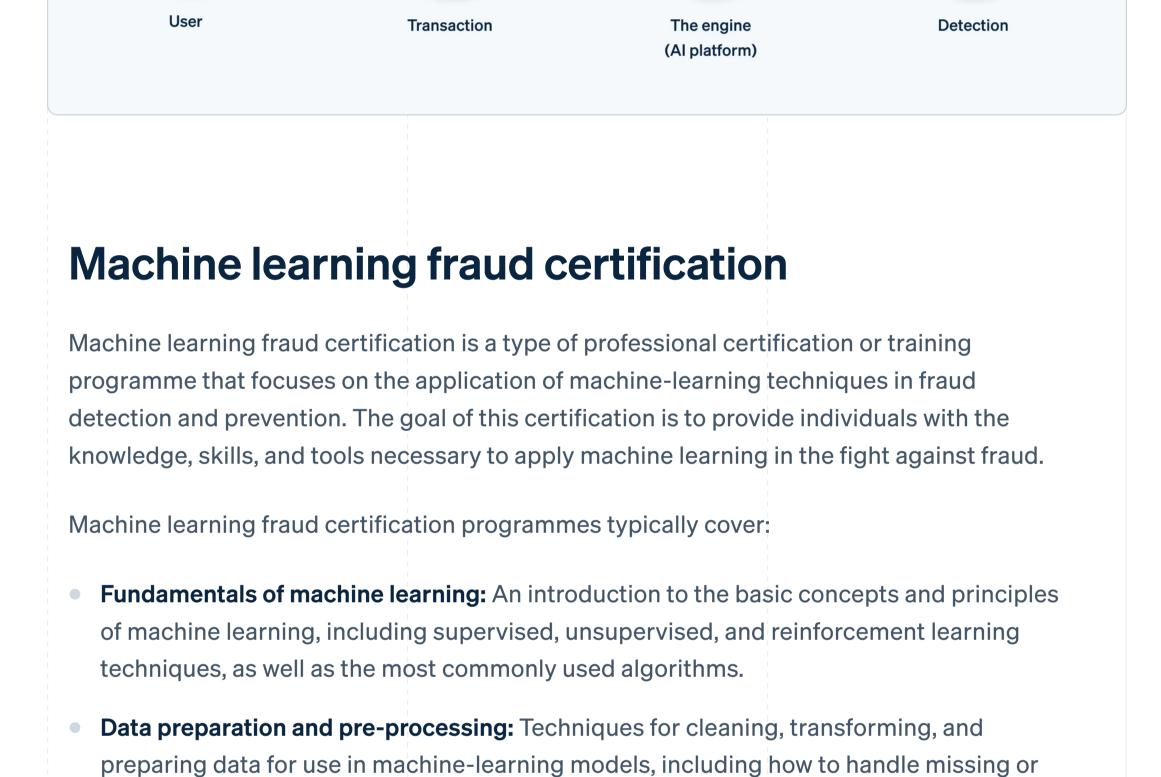
Point-of-sale (POS) anomaly detection

may indicate internal fraud or theft.

analysis, and identity verification.

recall).

Traditional rule-based approach to fraud detection



noisy data (corrupted or otherwise unusable data), feature engineering, and data

Model training and evaluation: Methods for training machine-learning models, selecting

appropriate algorithms, optimising model parameters, and evaluating model performance

using metrics such as accuracy, precision, recall, and F1 score (a measure of precision and

• Fraud detection techniques: An overview of various machine learning-based approaches

used in fraud detection, such as anomaly detection, risk scoring, network analysis, text

Implementation and deployment: Best practices for implementing and engaging machine-

learning models in a production environment, including model versioning, monitoring, and

maintaining model performance over time. Ethics and regulations: A discussion of ethical considerations and regulatory compliance related to machine learning and fraud prevention, such as data privacy, fairness, and explainability (the ability to explain to a human what a machine-learning model does from

Earning a machine learning fraud certification can help professionals demonstrate their

expertise in this specialised field, making them valuable assets for organisations that want to

improve their fraud detection capabilities. There are many types of professionals who may

benefit from such a certification, including data scientists, analysts, fraud investigators, and

detection and prevention for different payment scenarios: **In-person payments**

Machine-learning algorithms can analyse transaction data (e.g. time, location, amount, and

business) to identify patterns and flag potentially fraudulent transactions in real time. For

instance, if a customer's card is used in two locations that are far apart and within a short

instance, if an employee processed an unusually high number of refunds or discounts, that

Machine learning can monitor POS transactions and identify unusual patterns. For

time frame, the system can flag the transactions as suspicious.

Examples of machine learning for fraud detection

Businesses that deal with customer payments can apply machine learning-based fraud

Machine-learning models can analyse device-specific information (e.g. device model, operating system, IP address) to create a unique "fingerprint" for each user. This helps detect fraudulent activities, such as account takeovers or multiple accounts that are linked to a single device.

suggest fraud.

E-commerce

Behavioural biometrics

Device fingerprinting

Mobile payments

 Account takeover prevention Machine learning can monitor user login patterns and detect unusual activities, such as multiple failed login attempts or login attempts from new devices or locations, which may indicate an account takeover attempt. Friendly fraud detection

Machine learning can identify patterns related to friendly fraud, in which customers make a

purchase and later claim that the transaction was unauthorised or that they never received

the product. Models can analyse factors such as customer purchase history, return rates,

Machine learning can analyse invoices and related documentation to identify

By implementing machine learning-based fraud detection and prevention systems,

businesses can better protect themselves and their customers from fraud, reduce financial

discrepancies, such as duplicate invoices, mismatched amounts, or suspicious vendor

and chargeback patterns to flag potential friendly fraud cases.

Machine learning can analyse user behaviour patterns, such as typing speed, swipe

gestures, or app usage, to verify the user's identity and detect any anomalies that may

Loyalty programme fraud detection Machine learning can monitor customer behaviour within loyalty programmes, such as points accumulation, redemptions, and account activity, to identify and flag potential fraud or abuse.

Other relevant use cases

details, which may indicate fraud.

losses, and improve customer trust and satisfaction.

✓ Six types of payment fraud – and how businesses can prevent them

Invoice fraud detection

completeness, adequacy, or currency of the information in the article. You should seek the advice of a competent lawyer or accountant licensed to practise in your jurisdiction for advice on your particular situation.

The content in this article is for general information and education purposes only and should

not be construed as legal or tax advice. Stripe does not warrant or guarantee the accuracy,

The 6th EU Anti-Money Laundering Directive in Germany: What companies need to know ✓ Fraud detection services 101: How they work and how to choose a provider

Fight fraud with the strength of

no contracts or banking details required. Or,

Contact sales >

Explore Radar > Explore the docs >

the Stripe network.

Radar

stripe ✓ United Kingdom (English)

More articles

See all risk management articles

Ready to get started?

business.

Start now >

Climate Connect Data Pipeline Elements **Financial Connections** Identity Invoicing Issuing Link **Payments** Payment Links **Payouts** Radar Revenue Recognition Sigma Tax

Products & pricing

Pricing

Atlas

Billing

Capital

Checkout

SaaS Retail **Platforms** E-Commerce Marketplaces Crypto Creator economy Al companies Embedded finance Global businesses Finance automation Integrations & custom solutions

Documentation

API reference

API changelog

Stripe Apps

API status

Prohibited & restricted businesses

Terminal Treasury © 2025 Stripe, Inc.

We use cookies to improve your experience and for marketing. Read our

Newsroom Stripe Press Contact sales Support Get support Managed support plans

Create an account and start accepting payments contact us to design a custom package for your

> **Solutions** Startups **Enterprises**

Jobs

Guides **Customer stories** Blog Annual conference Privacy & terms

Resources

Radar docs

Use Stripe Radar to protect your

business against fraud.

Licences Sitemap

Cookie settings Company

cookie policy or manage cookies.

Accept all

Reject all

Stripe App Marketplace Partner ecosystem Professional services Developers

Sign in >