Why machine learning is essential in your fight against online fraud

Top use cases for detecting and mitigating fraud with machine learning

Table of contents

Making inroads against online fraud

Online fraud presents a pervasive problem for businesses of nearly every shape and size. According to a PricewaterhouseCoopers (PwC) survey, 47 percent of the 5,000 companies quizzed experienced a fraud in the past 24 months, with a total fraud loss reported of $42 billion.[1]

And, unfortunately, the problem is growing. A 2020 survey conducted by the Association of Certified Fraud Examiners (ACFE) found that, at a worldwide level, 77 percent of respondents reported a significant increase in cyberfraud risk, and 92 percent expected a significant increase in the next 12 months.[2]

Industries like retail, delivery, media, travel and hospitality, gaming, and financial services are the most often targeted by fraudsters. But any organization that conducts business online can fall victim to online fraud—and must seriously consider the risks and impacts.

Companies typically use fraud detection applications that often rely on business rules that don't keep up with the changing behaviors of fraudsters. Rule-based systems also require more human intervention and depend on experts to update the detection logic. If the fraud detection solution is not accurate enough, it will lead to false negatives, which will result in higher fraud losses and false positives, which will lead to lower revenue, negative reviews, and customer churn.

Thankfully, advancements in technologies like machine learning (ML) are enabling organizations to identify potentially fraudulent online activities with greater ease. Machine learning is well suited for the fight against fraud because it:

- Addresses a problem that's rich in data and can benefit from pattern identification within datasets
- Can achieve results that are nearly impossible to accomplish through human input alone
- Produces results that are easily quantifiable in financial terms, helping to foster executive buy-in for larger machine learning investments

By leveraging machine learning to combat online fraud, organizations can avoid revenue loss, mitigate brand damage, and create frictionless online customer experiences. The journey toward these benefits can begin in several ways—so organizations should start by considering the options and determining which path is best for them.

1 "PwC's Global Economic Crime and Fraud Survey 2020." PricewaterhouseCoopers, 2020.

2 "Fraud in the Wake of Covid-19: Benchmarking Report." Association of Certified Fraud Examiners, September 2020.

Evaluating your approach to machine learning fraud detection

AWS offers several services that can help with anti-fraud workflows and fraud detection—and avoid the roadblocks of a do-it-yourself approach:

- Some very specialized fraud detection use cases can be addressed by training your own machine learning models. While this can be daunting, you can use **Amazon SageMaker** to simplify and accelerate the process. Amazon SageMaker is a comprehensive machine learning service that provides built-in algorithms and pretrained models available through the AWS Marketplace.
- If you do not have access to machine learning expertise—or you prefer to dedicate your machine learning experts to other areas of your business—you can use **Amazon Fraud Detector** and **Amazon Rekognition**, two AI services that can be integrated into your business applications using an API.

The pre-built machine learning-model templates in Amazon Fraud Detector were developed from 20 years of experience stopping bad actors from attempting to defraud AWS and Amazon.com. Amazon Fraud Detector provides templates that you can use to easily create machine learning models that can identify up to 80 percent more potential bad actors than traditional methods without writing any code. This fully managed AI and machine learning service provides everything needed to create, deploy, manage, and scale fraud detection and can be utilized by developers, builders, data scientists, and even business users with any level of skill in machine learning.

In the following sections, we'll explore how AWS machine learning helps you detect fraud across several use cases. And we'll look at how specific organizations around the world and across a range of industries are successfully leveraging AWS machine learning for fraud detection today.

Transaction fraud detection

The most common machine learning fraud method, transaction fraud, involves users who attempt to complete inauthentic purchases or make or process fraudulent payments online. This type of fraud can take many forms. For example, in the ecommerce space, fraudsters sometimes take advantage of vulnerabilities associated with “guest checkout” features, wherein users who do not have any account history can purchase items with some degree of anonymity.

AWS machine learning solutions for fraud detection address this type of fraud by scoring the likelihood that a specific transaction is fraudulent. This allows you to more easily identify transactions from compromised payment instruments, such as stolen credit cards. It also helps you detect when fraudsters are using checkout to test multiple stolen card numbers. By identifying fraudulent transactions before they are processed, you can better prevent losses and avoid fines from payment processors.

omnyex

Omnyex levels up its fraud detection capabilities

OMX is a distributor of digital products, headquartered in Dubai, that provides technology to and manages multiple ecommerce websites, including CDKeys.com. CDKeys delivers a trustworthy, reliable, and fast purchasing experience that provides digital game keys to customers almost instantly so that they can make purchases with confidence and spend more time playing the games they love.

> ***"With Amazon Fraud Detector, we reduced fraudulent transactions by 6%. At the same time, we've been able to automate checkout fulfillment on more than 90% of the transactions that would have previously been flagged for manual review. Now, we're manually reviewing less than 1% of our transactions—down from 10%. Since we implemented this service, we've seen a significant improvement in our Trustpilot score, and we know it's a result of this checkout detection automation, as well as additional enhancements we are consistently making on the website. Trust is a big part of our value to customers, so that's a huge win for our business."***
>
> – Kevin Cole, Operations Director, OMX

New account fraud

Another method of online fraud involves the creation of phony accounts. Here, fraudsters create accounts using fake, stolen, synthetic, or bot-generated information. They do this to gain access to the platform, establish a history, and ultimately mask fraudulent or abusive activities.

AWS machine learning solutions for fraud detection can score the likelihood that a specific sign-up may be fraudulent, allowing you to identify new account fraud more accurately at the time of account registration. From there, you can segment new users who join your platform based on risk and implement mitigation measures. By detecting the creation of fake accounts, you can better prevent fraud or abuse before it happens—reducing damage to your brand and your customers.

Duda helps keep web designers moving and secure

Duda, a professional web design platform targeted at small businesses, found initial success in combatting fraud via a rules-based approach. As the company grew, however, it discovered that its fraud detection methods were negatively impacting the customer experience.

By integrating Amazon Fraud Detector into its existing solution, Duda can now identify more fraud, faster and easier, while delivering a frictionless web design experience to its customers. The company has improved its fraud detection accuracy—seeing a double-digit drop in false negatives—and saved countless hours instead of creating a solution from scratch.

> ***"We see lots of potential to expand our use of Amazon Fraud Detector to help us provide the secure, painless web design experience that our customers expect."***
>
> – Amir Glatt, Co-Founder and CTO, Duda

ActiveCampaign catches phishing attacks before they bite

ActiveCampaign is a marketing automation provider that helps growing businesses make meaningful connections and engage with their customers. In the first half of 2020, ActiveCampaign experienced a spike in accounts being used for phishing attacks.

With Amazon Fraud Detector, ActiveCampaign uses its own data to easily build a model that can accurately identify account sign-ups that result in phishing attacks. The solution also helps ActiveCampaign reduce false positives, reducing additional work for its staff. ActiveCampaign further touts Amazon Fraud Detector's competitive pricing model and its easy integration with existing workflows as factors leading to a successful engagement with the solution.

> ***"We needed to supplement our existing homegrown solution with stronger transaction data and signals to identify bad actors sooner. Amazon Fraud Detector made it easy to build a model… that accurately identifies account signups that result in phishing attacks."***
>
> – Alex Burch, Senior Email Operations Engineer, ActiveCampaign

Account takeover

Account takeover is when a legitimate user account has been compromised. This occurs when a bad actor gains possession of authentic user credentials by stealing them, purchasing them over the dark web, or managing to guess them. Account takeovers are often the result of bot activity, wherein bots use “blunt force”—rapidly guessing combinations of user IDs and passwords—until they successfully gain access.

AWS machine learning solutions for fraud detection allow you to more accurately distinguish authentic logins from those likely to be illegitimate, helping prevent account takeover and the resulting damage.

Promotion abuse

Promotion abuse occurs when a fraudster accesses a legitimate user's account and drains it of loyalty credits or points via transfer or purchase. Bad actors will also create multiple fake accounts to exploit promotions meant for new users, such as free trials or virtual gift cards.

AWS machine learning solutions for fraud detection address promotion abuse by scoring the likelihood that specific user activity related to promotions is due to fraud or abuse based on violations of service terms. By accurately identifying and preventing promotion abuse, you can help avoid financial losses and ensure that legitimate users can continue to enjoy the rewards and benefits they've earned.

Qantas Loyalty sends promotion abuse packing

Through its Qantas Frequent Flyer and Qantas Business Rewards programs, Qantas Loyalty rewards its over 12 million members with points they can redeem across a wide range of categories. Leveraging Amazon Fraud Detector has helped Qantas Loyalty significantly improve its ability to detect promotion abuse and fraud. By enabling the company to write custom rules, train machine learning models on demand, and seamlessly integrate other AWS services with its solution, Amazon Fraud Detector helps Qantas Loyalty make decisions quickly and intelligently—while retaining complete control of the platform.

> ***"Amazon Fraud Detector has been a great addition to our fraud detection and mitigation capability…AWS was very helpful during the proof-of-concept stage and has been adding new features to the platform in line with fraud trends."***
>
> – Mary Criniti, CTO, Qantas Loyalty

Fake reviews and content moderation

Fake or abusive reviews and user-generated content pose a growing concern to today's organizations, with customers increasingly relying on online reviews to help them make purchasing decisions. Fake reviews or content posts, like someone posting a fake review to an online marketplace, can unfairly cause products to develop negative reputations, detract from overall ratings and rankings, and boost the visibility of subpar services or content. Abusive reviews, such as those containing profanity or racist, sexist, or threatening language, can anger users and cause them to defect from a platform or turn to a competitor—especially if they determine that this behavior is not well policed.

AWS machine learning solutions for fraud detection can be used to help automate screening for fake and abusive reviews. This can allow your customer service teams to save time, freeing them from wading through mountains of alerts, many of which may be false positives. Amazon Rekognition, Amazon Transcribe, and Amazon Comprehend can be used to streamline and automate your image and video moderation workflows. By catching fake or abusive content earlier and more accurately, you can better protect your reputation and your customers.

Authentication

Machine learning-powered facial biometrics can enable online user identity verification. **Amazon Rekognition** offers pretrained facial recognition and analysis capabilities that you can simply add to your user onboarding and authentication workflows to verify opted-in user identity online. No machine learning expertise is required.

With Amazon Rekognition, you can onboard and authenticate thousands of users in seconds while deterring fraud actors or duplicate accounts. As a result, you can grow users faster, reduce fraud, and lower user verification costs.

aella

Aella Credit leverages computer vision for identity verification

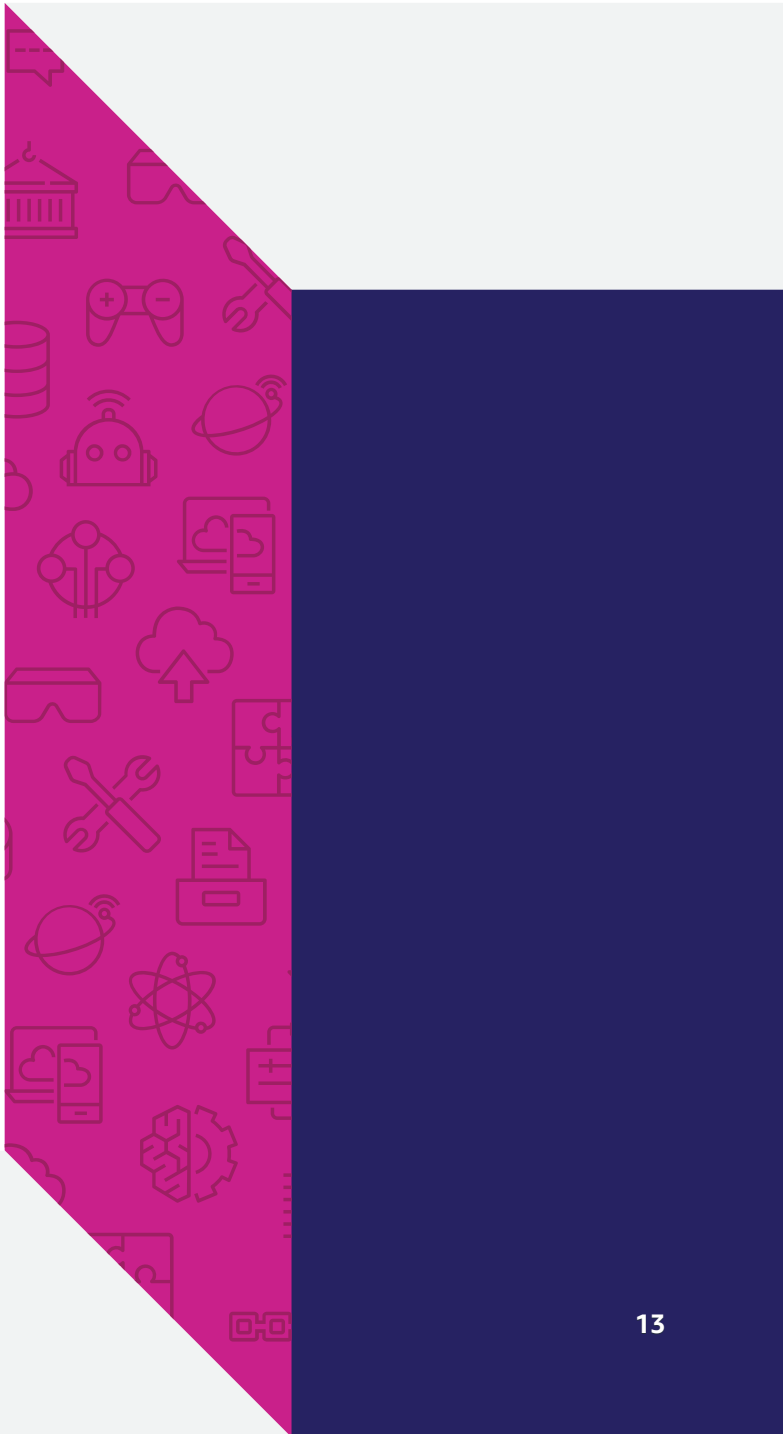
Aella Credit provides instant loans to individuals with a verifiable source of income in emerging markets using biometric, employer, and mobile phone data.

> ***"Identity verification and validation have been a major challenge in emerging markets. The ability to properly identify users is a key hindrance in building credit for billions of people in emerging markets. Using Amazon Rekognition for identity verification on our mobile application has reduced verification errors significantly and given us the ability to scale. We can now detect and verify an individual's identity in real time without any human intervention, thereby allowing faster access to our products. We tried various well-advertised solutions, but none of the popular alternatives could accurately map out various skin tones. Amazon Rekognition helped us effectively recognize faces of our customers in our markets. It also helped us with KYC in discovering overlapping profiles and duplicate datasets."***
>
> – Wale Akanbi, Co-Founder and CTO, Aella Credit

Claims fraud detection

Insurance claims and applications for government benefits or entitlements, such as unemployment or medical assistance, can also be a source of online fraud. Common techniques include “padding” (claiming more than one is legitimately owed), submitting claims for nonexistent injuries or conditions, and identity theft (submitting a claim for another person without their consent).

Amazon SageMaker can be used to help detect fake or fraudulent claims at the time of submission. This allows you to flag these claims for close review or inspection or to prompt for action to validate applicant details. Using machine learning to identify fraudulent claims can help you prevent financial loss and discourage repeat offenders.



Detect more online fraud faster

Wherever commerce exists, fraud is sure to follow. But while the threat of fraud will never be eradicated entirely, that doesn't mean you can't fight back by leveraging technology like AWS machine learning solutions for fraud detection to stay one step ahead of the latest tricks and techniques.

AWS provides you with total flexibility in your efforts to combat online fraud. You can develop your own solution in just days with **Amazon SageMaker** using pre-built algorithms and pretrained models to move with greater speed and accuracy. Or you can integrate **Amazon Fraud Detector** with your business applications using an API—allowing you to identify up to 80 percent more potential bad actors than traditional methods while remaining focused on your business, not fraud.

Amazon Fraud Detector helps you adapt to changing fraud patterns, enabling staff of varying skill levels to develop highly accurate machine learning models. The solution scores the risk of an event in real time so you can instantly apply containment or remediation measures and fast-track low-risk activity. The result: a solution that helps you detect more online fraud faster and without compromising customer experience.

Computer vision can also be used to enable advanced fraud detection use cases in which facial biometrics are used to verify user identity. **Amazon Rekognition** makes it easy to add computer vision authentication to your applications with proven, highly scalable, deep learning technology that requires no machine learning expertise to use.

Learn more about how AWS can help you in your fight against fraud:

Amazon fraud detection ›

Amazon computer vision ›

Contact us to discuss your needs ›