MARLUC

CASE STUDY · MARLUC SYNOPSIS

JPMorgan Chase machine learning fraud detection

IMPLEMENTED 2010S ONWARDS · FINANCIAL SERVICES AND INSURANCE · UNITED STATES · BAND C · CLAIMED ONLY

VERSION 1.0 · PUBLISHED 17 NOVEMBER 2026 · UPDATED 17 NOVEMBER 2026 · FACTS CHECKED 17 NOVEMBER 2026

JPMorgan Chase has used machine learning to score card and payment transactions for fraud since the 2010s. By its own account the models approve more good customers, decline more fraudsters and have held the cost of fraud flat while attacks grow.

ABOUT THIS SYNOPSIS

This is MarLuc's summary and grading of publicly available sources, for information only. It is not investment, legal, financial or professional advice, and should not be relied on for any decision. Readers must validate it against the original sources and, where appropriate, challenge its conclusions.

Facts and figures are as reported by the sources listed below, which may be incomplete, self-reported or out of date. Check the original source before relying on any figure.

The impact band, proof marker and SEAM view are MarLuc's opinion. The organisation is not a MarLuc client and has not reviewed or endorsed this synopsis. Names and trademarks belong to their owners.

NOTICE WORDING LAST UPDATED 16 NOVEMBER 2026

AT A GLANCE

AI used: Predictive machine learning models scoring card, payment and check transactions for fraud.

Implemented: 2010s onwards. Grade: band C, Process change, Claimed only.

Headline result, as reported: Machine learning fraud tools expected to bring about $150 million a year in benefits, by the bank's 2018 annual letter; fraud cost held flat as attacks grew 12% a year, by its 2025 Investor Day account

1 · The case

The facts, as reported by the 6 sources listed at the end. Where a source is silent, the field says "Not reported".

Organisation

JPMorgan Chase & Co.. US bank, the largest in the United States by assets, per Entrepreneur. More than 320,000 employees in 66 countries and a 2026 technology budget of about $19.8 billion, by its 2025 annual report. Canvas block: 4. Operations and process. Also 8. Governance and risk, 6. Data and technology.

Business challenge

The challenge. Card and payment fraud. In its 2025 Investor Day account the bank said attacks were growing at a 12% compound annual rate. Fraud screening also declines some genuine customers: the 2018 letter describes good customers who would have been declined for potential fraud.

How it was addressed. The bank uses machine learning models to make automated decisions on transactions at the point of sale in milliseconds, by the 2018 letter, and said it would also use them to analyse signatures, payee names and check features to curb check fraud. Its consumer bank says its AI work initially focused on risk management such as fraud detection. By 2023 it reported over 400 AI and machine learning use cases in production across marketing, fraud and risk, and the corporate and investment bank said AI had improved the cost and effectiveness of sanctions screening and fraud protection. In 2025 the consumer bank added improved models to detect suspicious logins alongside passkeys and checks on higher-risk transactions. [1] [2] [3] [4] [5] [6]

Who implemented it

In-house (In-house): Built and runs the fraud models with its own AI and machine learning teams.
The 2023 letter reports more than 2,000 AI and machine learning experts and data scientists; no outside vendor for the fraud models is named in the sources.

Technology (SEAM pillar E)

SEAM types: T8 Predictive / ML models. Deployment: Not reported. Vendors and products: Not reported.

Where it was built in: Built into transaction authorisation at the point of sale, with automated decisions in milliseconds, and into check processing and login checks, by the bank's annual letters.

What changed

Before: fraud decisions that declined some genuine customers and approved some fraudsters, by the bank's 2018 account. After: automated machine learning decisions at the point of sale, with about 1 million more good customers approved and about 1 million more fraudsters declined, by the same account. In 2025 the bank said AI tools had held the cost of fraud flat while attacks grew. [1] [2] [3] [4] [5] [6]

What it cost

Not reported for fraud models. The chief executive told Bloomberg TV in October 2025 that the bank spends about $2 billion a year on AI across the firm, per Entrepreneur.

What it saved

About $150 million of annual benefits expected from machine learning fraud applications, by the 2018 letter. Cost of fraud held flat against 12% compound annual growth in attacks, by the 2025 Investor Day account relayed by Constellation Research. A 21% year-over-year reduction in fraud and scam claim rates across payment methods in 2025, from a mix of measures that

Governance and control

The 2023 letter describes a risk and control framework for AI-related risks and a Chief Data & Analytics Officer on the Operating Committee, reporting to the chief executive and Daniel Pinto. The 2025 annual report says models are connected to well-governed data with safeguards. Model validation, error rates and complaints about wrongly declined transactions: Not reported.

S2 · Accountable owner · Claimed
The 2023 letter says the bank created a Chief Data & Analytics Officer role on its Operating Committee, reporting to the chief executive and Daniel Pinto; a named owner for fraud models is not reported. [2]

A1 · Safe use · Claimed
The 2023 letter describes a risk and control framework to stay ahead of AI-related risks and a commitment to transparency on how AI helps make decisions, for example to counter bias. [2]

A2 · Human in the loop · Not reported
Not reported. The 2018 letter describes automated decisions on transactions made in milliseconds. [1]

A3 · Monitoring and assurance · Claimed
The bank reports outcome measures such as customers approved, fraudsters declined, claim rates and the cost of fraud, by its own account. [1] [4] [5]

A4 · Vendor AI · Not reported
Not reported.

A5 · Agent controls · Not reported
No agents described for fraud detection.

A6 · Standards and regulation · Not reported
Not reported for fraud models; the 2023 letter says the bank works with regulators as the regulatory landscape evolves. [2]

What worked, what did not, what is unproven

WORKED

– More good customers approved and more fraudsters declined at the point of sale, by the bank's 2018 account.

– Cost of fraud held flat while attacks grew, by the bank's 2025 Investor Day account.

– Use spread from fraud to credit, marketing and personalisation, by the bank's 2023 and 2025 letters.

DID NOT

– Not reported. No failure or withdrawal of the fraud models is reported in the sources found.

UNPROVEN

– Whether the $150 million of annual benefits expected in 2018 was achieved: no later figure was found.

– How much of the 26% (2024) and 21% (2025) reductions in fraud and scam claim rates came from machine learning, as the letters credit a mix of measures such as Zelle warnings and blocking social media-originated transactions.

– False decline rates and the effect on customers wrongly declined: Not reported.

Timeline

Apr 2019 Annual letter for 2018 says machine learning fraud applications are expected to bring

Apr 2024 Annual letter for 2023 reports over 400 AI and machine learning use cases in production, including fraud, and a Chief Data & Analytics Officer on the Operating Committee [2]

Apr 2025 Consumer bank letter says its AI work initially focused on risk management such as fraud detection [3]

2025 At its Investor Day the bank says AI tools have held the cost of fraud flat while attacks grow 12% a year [5]

Oct 2025 Chief executive tells Bloomberg TV that about $2 billion of AI spending brings about $2 billion of benefit, with fraud detection among the use cases [6]

Apr 2026 Annual report for 2025 says machine learning and AI deliver measurable value across credit, fraud and personalisation [4]

2 · Grade and SEAM assessment

MarLuc's opinion, made on the evidence above. How cases are graded: marluc.co.uk/case-studies/how-we-rate

Level of change and impact

Claimed: Not applicable. Grade: C, Process change. Proof: Claimed only. Level of change: Process change.

Process change (Level 2, band C). Fraud screening runs on machine learning decisions made in milliseconds, by the bank's account; no change to roles or structure is reported for this use.

Fraud screening of card and payment transactions was rebuilt around machine learning models that decide in milliseconds, a process change. The figures are the bank's own and are not broken out from other fraud measures in recent years.

The SEAM view and lessons learnt

Fraud screening is one of the longest-running uses of machine learning in a large bank, and the bank reports value on both sides: fewer genuine customers declined and more fraud stopped. The figures are the bank's own and recent ones mix AI with other controls, so the share due to the models is unclear. For a mid-sized or larger organisation, the transferable point is to measure false declines as well as fraud caught.

1. Measure wrongly declined customers alongside fraud stopped.
2. Report the effect of models separately from other fraud controls.
3. Revisit early benefit estimates and publish what was achieved.

Evidence

Score 1 of 4. Self-reported: annual shareholder letters and executive statements at the 2025 Investor Day and on Bloomberg TV, relayed by Constellation Research and Entrepreneur.

Evaluation method. Self-reported company figures: an expected benefit estimate (2018), claim rate changes and executive statements; no independent evaluation.

3 · Original sources

Read these in full. To challenge a fact or a grade, use the contact form at marluc.co.uk or the link on https://marluc.co.uk/case-studies/jpmorgan-chase-machine-learning-fraud-detection

[1] JPMorgan Chase: Annual Report 2018, Chairman and CEO letter to shareholders (April 2019)
https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/ceo-letter-to-shareholders-2018.pdf

[2] JPMorgan Chase: Annual Report 2023, Chairman and CEO letter to shareholders (April 2024)
https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/ceo-letter-to-shareholders-2023.pdf

[3] JPMorgan Chase: Annual Report 2024, line of business CEO letters to shareholders
https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/line-of-business-ceo-letters-to-shareholders-2024.pdf

[4] JPMorgan Chase: Annual Report 2025, Chief Operating Officer and line of business CEO letters to shareholders
https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/line-of-business-ceo-letters-to-shareholders-2025.pdf

[5] Constellation Research: JPMorgan Chase's IT, AI bets: where the returns are (Investor Day 2025)
https://www.constellationr.com/insights/news/jpmorgan-chases-it-ai-bets-where-returns-are

[6] Entrepreneur: JPMorgan Chase is saving $2 billion a year using AI, according to CEO Jamie Dimon (October 2025)
https://www.entrepreneur.com/business-news/jpmorgan-ceo-jamie-dimon-ai-saves-the-bank-billions-a-year/498115

JPMorgan Chase & Co. website: https://www.jpmorganchase.com

Version 1.0 · Published 17 November 2026 · Updated 17 November 2026 · Facts checked against sources 17 November 2026 · Downloaded 26 November 2026. This PDF may be out of date: the latest version, and a way to report an error or a better source, is at https://marluc.co.uk/case-studies/jpmorgan-chase-machine-learning-fraud-detection

VERSION HISTORY

v1.0 17 November 2026 First published