# JPMorgan Chase using advanced AI to detect fraud

**0-eds-p-ebscohost-com.librus.hccs.edu**/eds/detail/detail

## Citation

**Title:**

## JPMorgan Chase using advanced AI to detect fraud.

**Authors:**
Crosman, Penny

**Source:**
American Banker. 12/22/2023, pN.PAG-N.PAG. 1p.

**Document Type:**
Article

**Subject Terms:**
**Company/Entity:**
J.P. Morgan **Chase** & Co.

**NAICS/Industry Codes:**
522329 Other financial transactions processing and clearing house activities
522320 Financial Transactions Processing, Reserve, and Clearinghouse Activities
713290 Other Gambling Industries
713299 All other gambling industries

**Abstract:**

One area of focus for the bank is **using advanced** artificial intelligence to **detect** business-email compromise. The payment messaging network Swift and online gambling host Caesars are also **using AI** to stop people from gaming their systems. [ABSTRACT FROM AUTHOR]

**Full Text Word Count:**
1247

**ISSN:**
0002-7561

**Accession Number:**
174425324

**Database:**
Business Source Complete

This content may contain URLs/links that would redirect you to a non-EBSCO site. EBSCO does not endorse the accuracy or accessibility of these sites, nor of the content therein.

## Full Text

Listen

One area of focus for the bank is **using advanced** artificial intelligence to **detect** business-email compromise. The payment messaging network Swift and online gambling host Caesars are also **using AI** to stop people from gaming their systems.

In Ryan Schmiedl's work protecting **JPMorgan Chase** from **fraud** of all kinds, business-email compromise has been the most devastating type of attack lately.

Fraudsters look for the weakest link, the place that is least protected, Schmiedl said. And they often find it somewhere inside a corporate client.

"In a lot of cases, they're attacking corporates, because there are so many people in a corporate entity and they don't communicate a lot," Schmiedl — who is global head of payments, trust and safety at the bank — said on a panel at Fintech Connect last week.

He oversees **JPMorgan's** efforts to **detect fraud** and financial crimes through **fraud** controls, sanctions screening, know-your-customer checks and other means. Before joining the bank, he had a similar role at Amazon.

"I can't tell you how many times we have clients that have been socially engineered," he said.

Often fraudsters send an authentic-looking email that appears to be from a genuine vendor or partner. It might say the company is changing accounts, and that the recipient should send the money to a convincing but fake website the fraudsters have created.

Whenever bank employees become suspicious of a corporate transaction and call clients to ask if they are sure they want to send the money, clients often initially say yes because they believe the transaction is legitimate. It's only when vendors call a few days later to say they never received payment that clients realize they were duped.

To catch incidents like these and the many other types of **fraud** banks are hit with constantly, **JPMorgan** is **using** large language models, a type of technology that can process large amounts of text and that is behind the wildly popular artificial intelligence chatbot ChatGPT.

This is part of a trend in which many organizations, including banks, payments networks like Swift and online gambling companies like Caesars Entertainment, are shifting from more basic machine learning to **advanced AI** in their pursuit of bad actors and suspicious transactions.

**JPMorgan Chase's** use of large language models

**Fraud** detection technology at **JPMorgan** evolved from the use of basic business rules and decision trees to the use of machine learning. More recently, the bank has been **using AI** to extract entities, such as names of companies and people, from unstructured data and analyze them for signs of **fraud**. One example is **using** large language models to **detect** signs of compromise in emails.

"There's an inherent signal in every email that's created," Schmiedl said. "Actors that are trying to create fraudulent emails tend to basically use different patterns and you can learn those patterns through machine learning."

The bank is **using** large language models to examine patterns that are close together and ones that are far apart to understand the context and association.

"We do that in a number of different things, whether it's looking at instructions for a wire or doing sanctions screening and I'm matching a list against instructions," Schmiedl said. He did not say which large language models the bank uses.

For instance, a large language model could be used to match a list of seafaring vessels against multiple data sources, and flag that one of the items on the list is at a location next to a street address, making it a false positive.

"Now we've got hundreds of models that look at a lot of different things, whether they're behavioral, whether they're around payment, whether they're on new accounts, just assessing the risk and trying to figure things like that out," Schmiedl said.

The bank uses only data within its ecosystem to train the large language models, he said, noting the danger of **using** a large language model that gathers data from across the internet, the way ChatGPT does.

"If you start **using** these models and outside data, you start to see things that are presented as facts that aren't facts," Schmiedl said. "You have to make sure the data you have has been audited, validated and is true."

Finding **fraud** in payments

Swift, the international payments messaging organization, is in the middle of building a new **AI** model with several technology partners, including Google and Microsoft, according to Kalyani Bhatia, global head of payments.

"We really believe that this is going to help us add on to the rule-based engines that we already have today and bring higher success rates with **fraud**," she said.

Swift is merging **AI** into some of its existing products to improve them, she said.

**For instance, it has a pre-validation service in which the sender of a payment can ask a beneficiary bank if a given account is open and valid. Today, this is done through an application programming interface.**

**Swift could apply AI to its historical data store of 10 billion transactions a year and find anomaly indicators, which it could then share with bank members.**

**Swift also has a midtransaction service called payment controls, a rules-based engine that every bank can use to set its own thresholds for transactions that should get a second look. AI could help make this system better, too, Bhatia said.**

**Post-processing, Swift plans to apply a score to every transaction and provide trend analysis and report on fraud patterns and fraud lessons to its bank members.**

**At Caesars Digital, the division of the entertainment company that provides gambling sites and apps, Maria Christina Kelly, head of payments and fraud, said her team focuses on two major categories of fraud.**

**The first is first-party fraud, which is also called friendly fraud or account-owner fraud. It's when "you had a good time and you have remorse and now you charge back," Kelly said. "That needs to be distinguished from third-party fraud, which we're calling hostile fraud. Those are the people that are attacking our site." These groups tend to buy consumer data, create fake accounts and extract money from Caesars through these made-up accounts.**

**Kelly has turned to third parties to build AI-based fraud-detection models. She's now in the process of training those models.**

**"Missing stuff is a real problem," Kelly said. "It takes a real combination of the humans who know what's going on and then making sure that the model is getting the right material. It takes a lot of lift, it takes a lot of attention and you don't go out on day one with a beautiful model. You have to keep improving it, working on it and feeding it the correct data."**

**The dark side of AI**

**Like all corporate defenders of data, Schmiedl, Kelly and Bhatia all worry that fraudsters and criminals will use AI to commit scams.**

**"It is something that keeps me up at night," Schmiedl said. "It's something that has been becoming a more and more prevalent problem, these adversarial attacks or these adversarial machine-learning models that are growing."**

**JPMorgan is investing in technology and research that will try to stay one step ahead, he said.**

**"It's a challenge," he said. "It takes consistent investment, consistent research, consistent time and effort to work on some of these things. And there are a number of players right now that have made good progress in some of the space," for instance in detection of deepfake voices and photos.**

**~~~~~~~~**

**By Penny Crosman**