How Artificial Intelligence and Machine Learning Can Protect Financial Institutions and their Customers From Fraudulent Activities

by ToolCASE

How Artificial Intelligence and Machine Learning can Protect Financial Institutions and their Customers from Fraudulent Activities.

The objective of this report is to describe how **Artificial Intelligence** and its **Machine Learning** capabilities can cut down losses and, in many cases, prevent financial losses due to fraud on the part of hackers, identity thieves and employees of financial services institutions and their customers. This report also introduces a system, developed by ToolCASE, with a track record of preventing losses due to fraudulent transactions.

Banks, big and small, Credit Unions, lending firms and insurance companies have been victimized by fraudsters. There has always been fraud, with criminals trying to cheat or outsmart the system for monetary gain. Nowadays, with far more financial data and transactions occurring on computers and mobile phones, fraudsters have learned to become more sophisticated and knowledgeable on digital fraud techniques, staying well ahead of traditional detection methods.

Identity and PII Theft has Opened Up a Whole New World for Fraudsters

Obtaining the personalized data, or PII, of a credit card or debit card holder has become widespread. Fake cash points and skimmers can extract personalized information from cards as they are used to purchase gasoline, withdraw funds from an ATM machine, purchase groceries and other consumer products and from a number of other consumer touchpoints.

Criminals can use these data to make purchases online from their own sham ecommerce sites, purchase real products from legitimate ecommerce sites or use cash back or fraudulent withdrawal methods to illegally collect ill-gotten hard money.

Even food servers at restaurants have been known to photograph credit cards with a smart phone, and use the data, including the three-digit security code. The perpetrator can then use a bogus e-commerce site to make sham purchases, like a subscription, in effect depositing the money into his own merchant account.

And perhaps most alarming for financial institutions, disgruntled former employees of banks and other financial service providers, who know the inner workings of the systems, can become fraudsters as well.

Fraud Resolution Can be Quite Costly.

It’s hard to peg an exact extent of the loss to the customer and to the service provider as much fraud goes completely undetected.

In addition to the “hard money” losses, there are associated costs with each fraudulent transaction. Financial service firms like banks saw an average of $3.64 cost per dollar of losses due to fraud. This means that a $10,000 fraud costs institutions, on average, $36,400. Of course, some $10,000 frauds may cost less, but many cost far more.

Until recently, fraudulent transactions were often only detected after the fact. Usually it is the bank customer who discovers an unusual transaction in the account’s statement and reports it to the bank. At this point, the fraud has already occurred and funds removed.

This is followed by a lengthy process of dispute resolution, which is costly for both the bank and its customer. Undetected and unresolved fraud not only has a negative impact on the reputation of the institution, but the financial losses eat away at corporate profitability. This is why detecting the fraud on the institutional side is so important.

6 Ways AI Has Revolutionized Banking

The banking industry faces many challenges such as online fraud, changing financial laws, and growing customer demand for faster services. Since traditional methods are no longer enough, banks are increasingly relying on technologies like artificial intelligence (AI) and automation for optimal performance and results.

Analysts predict AI can save more than $1 trillion by 2030 by reducing front and back-office costs. These numbers show AI’s potential to transform the banking industry. Here we share six ways in which AI has revolutionized the banking sector.

1. Fraud detection

With the increasing number of online transactions, the opportunities to commit fraud have also gone up. As per Javelin Strategy & Research, there were 1.7 million fraud cases in 2019 alone. But these numbers have decreased since the record high of 16.7 million cases in 2017. AI is responsible for this nosedive, as it can analyze and interpret an enormous number of transactions in real-time. It takes only seconds for AI to identify fraudulent wire transfers or verify credit cards.

2. Customer service automation

Customers don’t like to wait. The banking industry has sped up onboarding and transacting by implementing AI in processes like KYC and customer support services. This helps in customer retention and increasing customer satisfaction.

According to a McKinsey report, “For every one-point increase in customer onboarding satisfaction on a ten-point Net Promoter Score (NPS) scale, there is a 3% increase in customer revenue.” It translates to an additional $15 million per year in profit for the banking industry.

3. Personalization

Banks have loads of financial data about customers. Earlier, they had no way of analyzing it, but now they can use machine learning to study patterns and create customized services. The day is not far when you would get personalized savings and credit services according to your habits. Moreover, big data analytics has now made precise targeting possible.

4. Cost efficiency

AI reduces bank employees’ workload by streamlining tiresome tasks and helping them reduce or prevent mistakes. Robotic process automation (RPA) is an integral part of a larger AI concept that can automate repetitive, rule-based processes. According to McKinsey, AI will perform 10 to 25 percent of manual labor, freeing employees to do high-value tasks in the coming years. It will help save the money spent on hiring and maintaining an additional labor force.

5. Security

The banking sector uses technological advancements like biometric identification and security codes to tackle safety issues. According to Goode Intelligence, about 1.9 billion bank customers will have to use biometric identification by 2021.

AI does not stop at preventing fraud and hacking; it can also find loopholes or vulnerabilities in the existing system and remove them to minimize such incidents in the future.

6. **Better decision-making**

Banks no longer base their marketing decisions on guesswork. AI-powered analytics provide customer data in a readable and processor bill format that companies can use to forecast upcoming trends and create actionable marketing strategies.

Enter Artificial Intelligence, or AI

Artificial intelligence technology has opened up a whole world of possibilities in analyzing and categorizing typical transactions and initiating actions depending on the nature of the transaction.

Analysts predict AI can save more than $1 trillion by 2030 by reducing front and back-office costs. These numbers show AI's potential to transform the banking industry. Here we share six ways in which AI has revolutionized the banking sector.

Artificial intelligence (**AI**) refers to the simulation of human **intelligence** in machines that are programmed to think like humans, mimic and anticipate their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

AI has taken computing to the next level. This combines the analytical and decision-making capability of human thinking with the light-speed calculations of computers. Speed makes it possible to analyze millions of transactions, across all data channels, in real-time; allowing for appropriate and instantaneous actions as any anomalous transactions arise, are attempted or are anticipated.

How AI Helps Banks Detect Fraud and Measure Risks

Artificial intelligence or AI helps banks detect automating fraud, cybersecurity, and anti-money laundering. According to EMERJ, approximately 26% (the largest share) of the venture funding raised for AI in the banking industry is for fraud and cybersecurity applications.

AI-driven real-time fraud solutions

Here we give you a low-down on the different AI approaches banks can employ to detect frauds related to payments, loans, and customer onboarding.

Banks and financial institutions struggle to find the right technology to analyze transactions and detect suspicious activities in real-time.

Anomaly detection

Online payment fraud losses will exceed $200 billion in the next five years. Banks and financial institutions are vulnerable to illicit activities, making their detection a growing necessity. Here we share five ways AI and machine learning can help banks identify and prevent fraud.

1. Behavioral analytics

It uses machine learning algorithms to anticipate and understand each account holder's transaction behavior (spending and saving) patterns. From this, the program can identify any behavioral anomalies. Algorithms treat uncharacteristic spending as suspicious behavior.

2. Large data sets

Machine learning (ML) improves accuracy with an enormous amount of data from big data analytics. Millions, even billions of data points, enable a smart computer to assess whether a transaction is fraudulent.

Best in class models continually learn from additional data to adjust their decisions based on changing environments in real-time.

3. Supervised and unsupervised machine learning Supervised models have previous input and output variables for the machines to learn from the past and predict future events. It tags the transaction as fraud or non-fraud to let computers determine legitimate or illegitimate patterns.

Meanwhile, unsupervised models use unclassified and unlabeled data as a form of self-learning. The machines must classify the data without prior knowledge.

4. Predictive analytics

AI models can develop predictive analytics software to assess data with a supervised or pre-trained ML-based algorithm. ML models can use data related to an account holder's transaction patterns to determine their legitimacy.

Banks can use predictive analytics to prevent activity from incorrectly flagged transactions. MasterCard uses predictive analytics powered by ML for real-time analytics.

5. Fraud detection

It is AI’s most significant contribution to the financial sector. Big data algorithms can easily detect data inconsistencies and discrepancies and ensure fraud prevention. Likewise, AI algorithms are helping protect consumer data and prevent credit card fraud.

Artificial intelligence, machine learning, and big data are changing the face of fraud detection by bringing real-time solutions. Machine learning uses advanced analytics to collect data about incoming transactions. Meanwhile, AI can adapt to produce touch techniques and deliver actionable insights in real-time.

AI Machine Learning

Machine Learning, or calculated data analysis and prediction, can detect and anticipate transactional patterns in a way not possible by human analytics methods. Certain operational parameters like time between the various stages of an automatic process can be analyzed in real-time and recorded to establish and even predict patterns.

AI Machine learning allows for the instant comparison between all transactions, both legitimate and fraudulent. Once these patterns are established, any transaction can be analyzed to see if it fits the pattern of a legitimate transaction and a possibly fraudulent one. Because of the ability to analyze millions of live data points, machine learning tools can establish and model these patterns in a very short time period. These tools can then predict where fraudulent activities are likeliest to appear in the future, helping fraud teams stay ahead of the criminals.

Certain data points such as the geo location of transactions can give clues to the legitimacy of transactions. Then there is the destination of funds transacted. Artificial intelligence can soon distinguish an online merchant marketing real goods or services from a fake online business set up as a channel for bogus credit card purchases, created for the sole purpose of collecting illicit funds stolen by fraud perpetrators.

Once these sham online businesses are detected, a database can be set up to invalidate any future transactions with such operations. Deep learning can identify the legitimacy of transactional websites.

How Device Identity can Help Prevent Fraud

Computer and mobile devices are being utilized in financial transactions more than ever. Legitimate online purchases and banking transactions are usually made using the same device the legitimate credit/debit card/debit card holder uses regularly.

Sometimes, often when an unrecognized device is used by a legitimate customer to access bank accounts or other financial accounts, customers are met with “we don’t recognize the computer you are using.” An access code will be sent to the account holder’s phone, usually as a text message. This code will allow the legitimate user access to the bank account or perform the transaction.

Every computer or mobile device has an identity known as a device ID. A bank’s advanced AI and machine learning system will associate the user’s identity with the device’s (or multiple device’s) unique ID. Even if a user is changing Wi-Fi networks, or is operating on a cellular network, the device ID attached to a customer never changes. Any identity thief or fraudster, invariably using a device not associated with the customer account, should be barred from access to those accounts. Unfortunately, many banks still rely on outdated anti-fraud techniques that do not know the difference between customer device ID’s and an attacker’s device.

Unique device ID certifications can be extended to almost any online purchases, or new mobile banking, credit account or mortgage openings. Associating a credit card or bank card with a certified device ID, and additional PII, could preclude an identity thief making online purchases, opening new accounts and withdrawing funds from legitimate customer accounts. And AI and advanced Machine Learning systems play a big role in identifying and sequestering these fraudsters.

Introducing RembrandtAI™

RembrandtAI™ is the world’s most sophisticated transactional real-time multi-level AI system. RembrandtAI combines solutions ranging from visualization and statistical trend analytics to pattern, anomaly, profile, and behavior deviation recognition using expert machine learning through artificial intelligence.

The RembrandtAI™ Advantage

The RembrandtAI™ suite offers banks, credit unions and other financial institutions immediate and LIVE data analysis with Artificial Intelligence algorithmic speed and precision. Because we compile and analyze all data across all channels in real-time, fraud risk is diminished substantially. And, our machine learning capabilities can help predict where new threats will arise.

The RembrandtAI™ solution identifies frauds in real-time, allowing banks to potentially save millions of dollars and boost their bottom lines.

RembrandtAi™ is a transactional multi-layer artificial intelligence solution. It is a culmination of decades of technological progress in the field of artificial intelligence, mass data accumulation and interpretation and machine learning. This evolution did not follow a straight line but was a development of a multitude of dimensions in the field of artificial intelligence.

- Multi-dimensional Envelopes – consolidated alerts by entity (customer, account)
- Workflow Management including Personal Docket, Docket Transfers, Envelope Management
- Drill down and research tools
- Pattern recognition with AI event scoring
- Continuous machine learning
- Visualization of data and graphical representation of key decision factors

Any additional information about RembrandtAi™ How it works on the floor of the bank. Which bank employee can, could or should use it.. and how easy it is to operate. How it replaces old school anti-fraud tools that no longer work.

Experience a free demonstration of the ToolCASE suite of anti-fraud tools.

About ToolCASE

ToolCASE is an IT services firm with 20 years of experience providing remote Oracle Database Administration, Linux/Unix System Admin, and System Storage Admin to clients throughout the United States. We offer AI-powered solutions for multiple industries like airlines, health, medical services, oil and gas, manufacturing, transportation, and shipping, plus anti-fraud tools for banking and other financial service providers.

You can fill our online contact form to know more.