MACHINE LEARNING: INDUSTRY SUCCESS STORIES

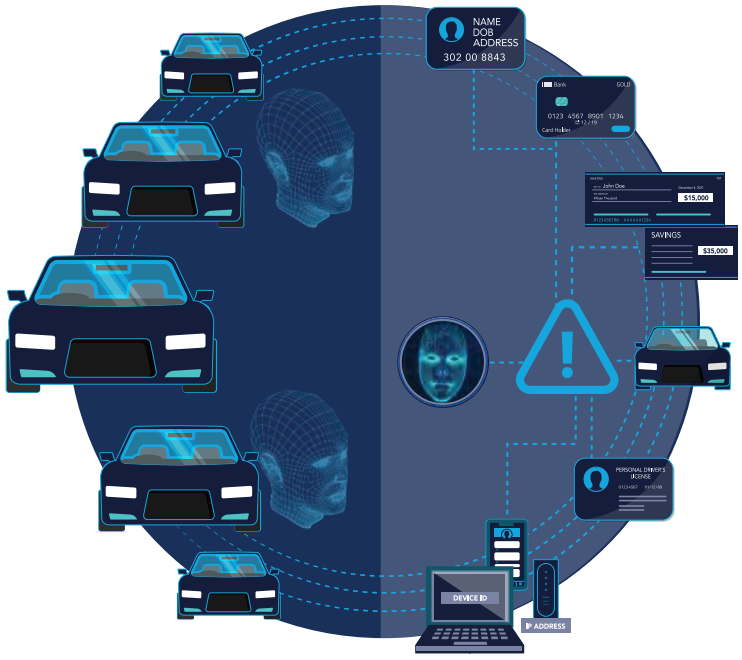
INTRODUCTION

Synthetic identities often are used to apply for financial accounts, such as credit cards, loans and checking accounts. Criminals can build a credit history with the intent to max out credit or overdraw accounts without repaying the balance. Initial payment activity may resemble a normal consumer account, making fraud detection through static rules more challenging as the rules don't automatically adjust with the trends. Machine learning can successfully detect synthetic identity fraud by analyzing large amounts of data across products and platforms – and in addition, use this source data to improve detection models.

SUCCESS STORIES

Synthetic Identities for Car Loan Fraud

A large credit union with fraud prevention tools in place lost $420,000 to a fraud ring that used synthetic identities to obtain car loans. The original application process did not include fraud threat intelligence as part of the loan application review. The multiple car loan applicants were not identified as synthetic identities during the application process. The fraud was detected only when loan payments became past due.



To avoid similar losses in the future, the credit union implemented a solution that proactively detected new fraud threats, including synthetic identity fraud. The new system could process a large volume of data and incorporate human insight and expertise into the analysis. During product testing, it was estimated that the new solution would have detected about 75% of the fraudulent car loan applications. Once implemented, the new anti-fraud platform reportedly detected and prevented more than $1.8 million in fraudulent activity across products and fraud scenarios. The credit union is currently working to expand its machine learning-based detection capabilities to other functions, including customer onboarding.

MACHINE LEARNING: INDUSTRY SUCCESS STORIES

Detecting Fraud Across Financial Institutions

Increased awareness of fraud trends has encouraged financial institutions to identify the impact of synthetic identity fraud in their portfolios. After careful review, losses that were previously treated as credit losses are now being recognized as the result of synthetic identity fraud. An increased number of third-party solutions are available to mitigate synthetic identity fraud.

In 2020, an organization that supports credit unions reported that its members' use of link analysis and machine learning prevented $38 million in fraud activity, including fraud associated with synthetics. The ability to ingest and analyze data from many organizations can help detect multiple synthetic fraud attempts, as it allows for comparison across organizations. If a synthetic identity is detected at one organization, this data is compared across organizations' portfolios to identify synthetic identities prior to default or bust-out actions. Accessing data from many organizations assists in fraud model development, as more examples of fraud and non-fraud activity are available for comparison. Detection models that use machine learning often are designed to produce a fraud score. An organization using the system can determine the score threshold to generate an alert and the corresponding actions that should be taken based on the risk. For example, if a fraud score for a credit card application receives a score indicating a high risk level for a synthetic identity, the institution can automatically decline the application or request more information from the applicant to verify the identity. Systems that use machine learning can process external data inputs, such as public records and digital identity information, to generate the most accurate risk score. Institutions also may apply specific fraud detection rules to support their businesses and work in conjunction with the risk score to produce the best results and address specific scenarios.

A fintech company recently reported its solution successfully helped a client detect synthetic identities during the account application process. For low-dollar loans requiring an immediate approval decision, the solution declines applications for high-risk individuals and increases the approval rate for more reliable consumers. The client reported a positive return on investment from the increased approval rate and a decrease in fraud losses due to synthetic identity fraud.

MACHINE LEARNING: INDUSTRY SUCCESS STORIES

CONCLUSION

For many financial institutions, machine learning has become an element of fraud detection because of its primary benefits:

- Efficient processing of large data volumes to produce a real-time credit decision or risk score.
- Model learning and improvement without constant manual intervention.

The basic features of machine learning can reduce friction for real applicants and customers, while detecting risk when synthetic identity fraud is suspected. Static detection rules alone may not identify changes in fraud tactics, since the established parameters must be updated manually. A system that is solely rule-based may not have the data processing capabilities to quickly compare enterprise account information across multiple products and review data from external inputs to produce an effective risk score. However, machine learning is not an instant solution. Machine learning models require initial testing, validation of the necessary data inputs and a defined specific outcome to be effective and evolve to become more effective. The best fraud detection approach involves layered security using many different tools, such as machine learning, detection rules and industry data sharing.