AMERICAN BANKER®

Florida credit union overhauls its fraud prevention with big assist from AI

By Carter Pape | May 06, 2022

As algorithmic techniques for fraud prevention improve, financial institutions have more and better options to stop losses in real time rather than try to recover funds hours or days after the fact.

Rather than rely on tellers to identify whether a check is fraudulent or a wire transfer is authorized, credit unions and community banks increasingly identify and prevent fraud with machine learning, but some still lag. For institutions that make the leap into real-time fraud prevention, the gains can be major.

That was the case for Launch Credit Union, which serves a six-county area on the Atlantic coast of central Florida, and switched to a real-time solution at the end of 2020. The credit union's chief financial officer claims it reduced fraudulent transactions across its 16 locations by 97% after purchasing the product, saving $1.8 million in 2021.

The product Launch adopted is RembrandtAI, a solution from Toolcase, an IT services firm that specializes in artificial intelligence and machine learning. Toolcase is not the only vendor of fraud prevention services powered by artificial intelligence; other companies specializing in such services include Feedzai, Nice Actimize, FiVerity, Inscribe, Resistant AI and larger firms such as IBM.

For the credit union, what made the biggest difference after adopting an AI fraud prevention service was its real-time nature. Its previous system relied on batch processing.

"We would upload two or three times a day," said Kevin LeBeau, chief financial officer at Launch Credit Union. "Well, if you're uploading three hours later, that money is already gone."

The technology Launch was using before was already years past its date of obsolescence, according to Alex Grinberg, the chief operating officer of Toolcase.

"We think that anything that's not real time is way, way past its use by date," Grinberg said. "Similarly, without the application of AI, you're simply not bringing the best tools and the best technology to the table to fight."

The RembrandtAI software Launch Credit Union now uses provides insights on individual transactions much quicker, LeBeau said.

Fraud prevention that uses artificial intelligence can be thought of as a means of superpowering fraud teams — acting as a force multiplier, according to Greg Woolf, FiVerity's CEO.

Those techniques can also work in layers, according to Martin Rehak, Resistant AI founder and CEO. He said Resistant AI's products use artificial intelligence to make real-time decisions about transactions by processing information from a variety of sources — the customer's credit history, information about the device they are using, and more.

Rehak said these techniques are particularly useful against automated or scripted fraud, which can be particularly painful for fintechs, banks and credit unions that pay rewards for referrals for new users.

"Automation is rapidly increasing and has been increasing since, I would say, the middle of 2021," Rehak said. "We see much more automated fraud than we have ever seen of manual, one-off fraud."

As for where batch processing plays a role, Rehak said the technique is useful for tuning the real-time decision-making systems to catch novel fraud schemes that are not mere spinoffs of previous schemes.

"This can provide additional insights derived from data outliers that may not have been possible in real-time," Rehak said. "However, batch processing means the institution has either already taken on the fraud risk (i.e. the transaction has occurred) or is holding off on completing the transaction until its analysis has been run — a very undesirable user experience these days."

According to LeBeau, that is exactly what Launch dealt with before it adopted real-time fraud detection. If a human didn't smell something fishy with a fraudulent transaction, that typically meant it was too late.

"We have great tellers, but tellers do a lot of work," LeBeau said. "It always falls back to the teller to do the first evaluation, and I'm afraid to say if they're really busy, they may not look at a check as closely as they should, or if they are looking at it, and they don't see anything quickly wrong with it."

As for the barriers that get in the way of financial institutions adopting real-time fraud prevention solutions, a few exist. According to Ronan Burke, CEO and co-founder of the fraud detection software company Inscribe, access to data can be a huge barrier.

The computer models that undergird fraud prevention systems require data on previous fraud attempts to stop new ones that are the same or highly similar. However, the siloing of user data at financial institutions often means fraudsters' attempts on one institution can easily be repurposed for another.

"Machine learning models benefit from as much data as possible, but each individual company is limited to only their own data," Burke said. To get around this problem, Inscribe and others use data from their client institutions to inform shared models to catch copycat fraud attempts.

While learning from past fraud can prevent future fraud, Rehak said, there is a constant "escalation game" that occurs in fraud prevention, with fraudsters adapting to the new preventative models of financial institutions and vice versa.

Grinberg of Toolcase said inertia also poses a barrier to wider adoption of real-time fraud solutions, and it sometimes takes a change in mentality or personnel to get over that, which is what happened at Launch Credit Union. LeBeau said all it took was one good hire — the manager of their small fraud department — to make the shift.

"We just had an opening, and I'm telling you, we were very lucky that she came over and interviewed," LeBeau said. "She had a lot of experience, and when she joined us, very quickly, you could see that she had the knowledge that was needed. She said, 'I can do this, but I need the right tools.' "