bank automation news

AI, cybersecurity education key to avoiding fraud

Consumers reported losing more than $5.8B to financial fraud in 2021

By **Henrik Nilsson** September 8, 2022 in **Center of Excellence** Reading Time: 3 mins read

Leveraging adaptive behavioral technology can help banks combat financial crime and fraud — but educating consumers on how to avoid suspicious links is key.

Consumers reported losing more than $5.8 billion to financial fraud in 2021, an increase of more than 70% compared with 2020, according to the **Federal Trade Commission**. Today's successful anti-fraud technology relies on connecting banks' independent silos, Carolyn Homberger, president of Americas at U.K.-based cybersecurity company **Featurespace**, told *Bank Automation News*.
"In silos, you can't see a trend, but across them, you can start to identify behavioral patterns that ultimately position you to prevent the fraud to begin with," Homberger said, adding that the tools are called holistic risk hubs.

Tricking people into submitting fake deposits or paying for goods they'll never receive are among some of the more common scams. Peer-to-peer payment apps are especially favored by scammers due to their increasing popularity and seamless transaction capabilities, Homberger said.

However, artificial intelligence (AI) models can be trained to stop suspicious transactions by analyzing internet activities, identifying irregular payments or pulling data from ISO 20022, the messaging format behind many financial institutions' (FIs) payment systems.

"We look at a number of these attributes," Homberger said. "We bring them together within the models and then the model basically scores the transaction to say: does this one require a manual review?"

Anti-fraud solutions that run on APIs simplify the integration process. The key is fine-tuning the program to predict malicious behavior.

However, change within large FIs also can be slow.

"[Banks are] highly regulated organizations that have to follow a very strict governance process," Homberger said.

Rethinking cybersecurity education

Stopping suspicious payment activity is critical, but so is simply teaching people how to identify a phishing message — especially at smaller banks with fewer cybersecurity capabilities, Chip Gibbons, chief information security officer at IT solutions company **Thrive**, told *BAN*.

An efficient spam filter can weed out 80% of suspicious emails. However, just one click on a fraudulent link can cause myriad challenges for both FIs and customers. Important data is at risk, and banks must dedicate valuable time to recover money if a scammer contacts a client in the bank’s name with a fraudulent routing number.

So-called “business email compromises” (BEC) cost U.S. businesses $2 billion in 2020, according to the **Federal Bureau of Investigation**. To avoid BEC, FIs must rethink how they approach educating their staff, Gibbons said.
Rather than staff watching a 45-minute cybersecurity training video once a year, regional banks should adopt shorter and more frequent training sessions. At Thrive, anti-fraud education includes fake phishing attacks for clients.

“It used to be a pretty bad stigma when you got compromised,” Gibbons said. “Now that stigma is going away. [Fraud is] still there. But most people in the security industry already know you’re going to get compromised, and are you doing enough to protect yourself against it?”