Neuroscience giving banks a chance to detect both fraud and friction

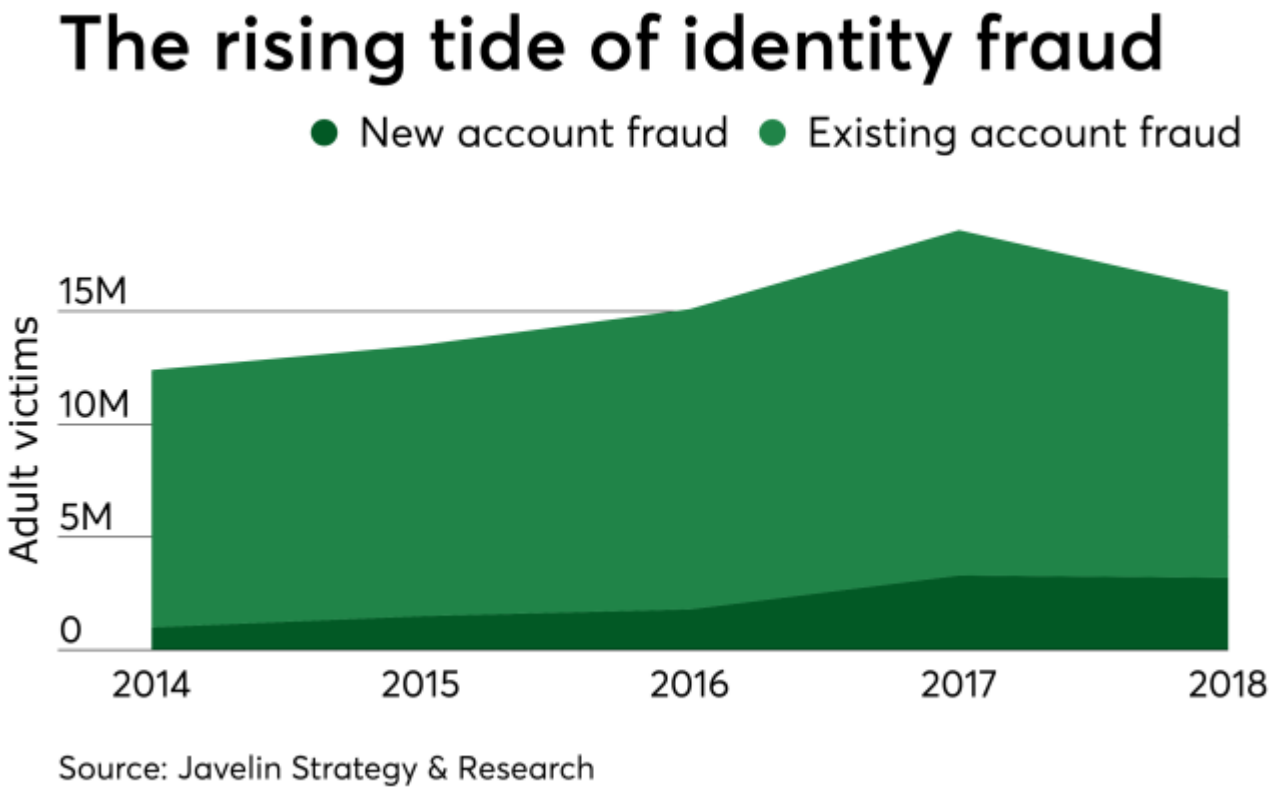
By **David Heun**
Published August 29 2019, 12:01am EDT

More in **Fraud detection, Fraud prevention, Payment fraud**

With the Federal Reserve last month citing synthetic identity fraud as a growing concern for financial institutions, there's more pressure to detect fraud at the start of the relationship.

Neuro-ID is making the case that the best way to thwart the growing number of fakers applying for payment cards, loans or merchant accounts online is to fully understand their bad behavior.

That bad behavior manifests itself in many ways. Most often, it is detecting an applicant's hesitation to click when inputting answers to simple questions; erratic or different activity with a computer mouse; and unusual copy-and-paste movements.



Neuroscience digs however deep it can go in giving banks a real-time security layer that complements historical data a bank may already have about an applicant. This can greatly decrease the number of successful synthetic fraud attacks, said Jack Alton, CEO of Whitefish, Mont.-based Neuro-ID.

"Initially, our focus was to leverage our real-time behavioral analytic technology in the unsecured lending space in the fintech market, but we have since moved into traditional banking and merchant acquiring in screening those applying for merchant contracts," Alton said.

Fintechs, banks and other organizations spend a lot of money to lure potential customers to their sites to apply for various services, whether it is credit cards, merchant accounts, insurance products or loans. In addition to making sure those applicants are who they say they are, the neuroscience screening can help detect any friction good customers may encounter.

"What is really frustrating to those banks is when people leave a site before taking up an offer or finishing an application," Alton said. "It is because of a digital gap that causes a drop in conversion rate; the verification and fraud teams can't see that customer very well beyond basic fraud checks."

Various companies are attacking the synthetic fraud problem with variations on analytics tools, such as ID Analytics or Global Risk Technologies; and some behavioral science, such as BioCatch.

The advancement of neuroscience as a security layer is showing early positive results, said Julie Conroy, research director and fraud expert with Boston-based Aite Group.

"In looking at the cadence at which data is being entered and how fast the applicant is doing things ... that is not just helping catch fraud, but also addressing channel abandonment," Conroy said.

"This is very useful in application flow today, but these technologies are growing and there is room for improvement and other use cases," she added. "I think it is great we are seeing positive results already."

The Javascript that Neuro-ID deploys within a bank's fraud detection system helps develop a score in real-time of the authenticity of an applicant. Any type of hesitancy, frustration, answer switching or other actions not common in a good applicant, gives the banks reason to pause before approving an application.

When combined with other data such as device ID, bank verification processes, credit bureaus and other analytics, the extra behavioral information helps reduce fraud and friction. The evaluation and a score on the applicant occurs in less than 50 milliseconds.

"We are not approving or declining, or making any decisions for the client," Neuro-ID's Alton said. "Based on the score, the business makes the decision to either increase or reduce verification to enhance conversions."

Neuro-ID says its computer interface also allows a business to differentiate between a machine or bot and that of human behavior when filling out an application.

"With merchant onboarding, we are typically gathering more than 400 behavioral data points per question," Alton said. "On a typical customer journey, we may be picking up from 20,000 to 40,000 customer data points."

Because of that, the technology quickly knows when a bot is infiltrating a system.

"When we see the applicant struggle with things that should come very easy, like writing a name or Social Security number, or they are making changes about income, where they live, or what their car looks like, those become new vectors for us to detect fraud or risk," Alton said.

Behavioral scientists Jeff Jenkins and Joe Valacich founded Neuro-ID in 2014 and incorporated the company in 2015. Alton became CEO in 2017 as the platform became available for clients.

Updated August 29, 2019 at 10:58AM: Story has been updated to clarify the evaluation time frame to produce an applicant score.

David Heun