AMERICAN BANKER®

Identity fraud is soaring. Here's how one lender is attacking it.

By Penny Crosman | July 02, 2020

The use of stolen and synthetic identities to perpetrate fraud skyrocketed last year, and the pandemic may be helping make the problem worse.

Losses stemming from identity fraud rose 15% in 2019 to $16.9 billion after hitting a five-year low in 2018, according to the latest Identity Fraud Report from Javelin Strategy & Research.

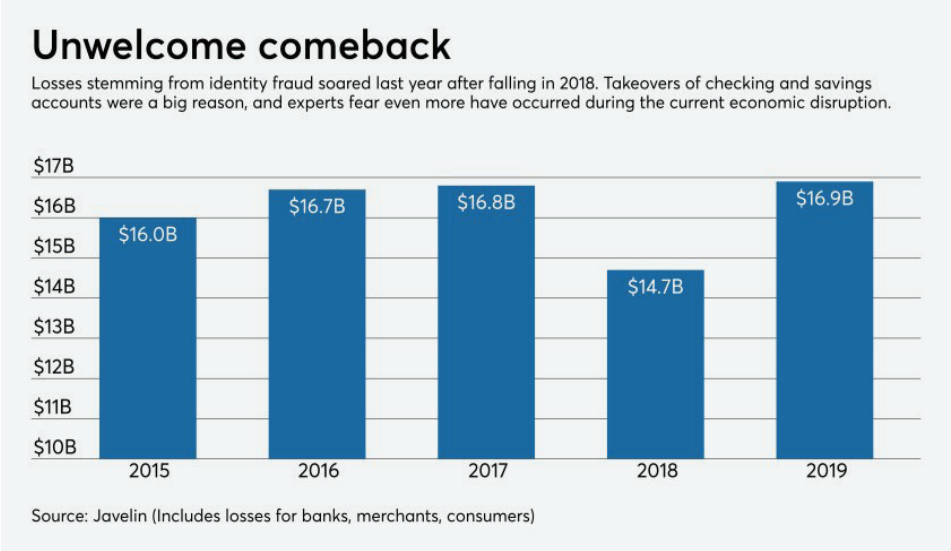
The firm doesn't yet have numbers for 2020, but the coronavirus-related shutdown of the economy is said to have become a breeding ground for a wide range of financial fraud. For instance, credit and debit card fraud rose 35% in April from a year earlier, according to FIS, which assists about 3,200 banks with fraud monitoring.

One of the main culprits for the soaring ID fraud numbers last year was a spike in account takeovers, a high-impact kind of crime that takes fewer victims to add up to big money, said Krista Tedder, head of fraud at Javelin.

"Account takeover is really difficult," Tedder said. "In 2015, 12% of fraud was due to account takeover, and this past year it was 53%."

While banks have invested time and money in monitoring transaction activity to identify transaction fraud, identifying new accounts created with stolen or synthetic identities (fake identities made up of bits and pieces of real identities that could pass validation checks) has been far more challenging. Account takeover can also be as simple as a password reset.

One company, Axcess Financial, is using technology to confront the problem.



The Cincinnati company, which offers financial products through several brands including Check 'n Go and Allied Cash Advance, has to fight off charlatans and criminal networks masquerading as online loan applicants.

Two years ago, the company hired Richard Cooney from Synchrony Financial to lead fraud strategy. He had been Synchrony's senior vice president of fraud risk and previously was senior VP of fraud policy at Citigroup.

"Much of the business was going digital, so I was brought in to figure out, how can we survive digitally in this world today without destroying our business?" said Cooney. "Having been in this industry for 35 years and in fraud for 30 of those, I knew that you have to protect yourself, your customers, and the general public if you're going to survive in the digital world."

Cooney said his biggest concern about fraud is how naive the general public is about the schemes out there.

"Most people don't understand that their information has probably already been compromised in one data breach or another over the past 15 years, whether in full or partially — it's sitting in some dark web database somewhere," he said. "Their identity is compromised, and most folks don't know the signs of it." They don't know how to take advantage of services that monitor their bank accounts, credit card accounts and credit scores, he said.

"We have to train the general public to take more of an active interest in their identity and start to own it," Cooney said. "I don't see us there yet. I see us a long way away from that. Until people take ownership of and know what to do to protect their own identity and

start taking those steps, this is going to continue to get worse."

When he joined Axcess, Cooney began analyzing how identity theft was affecting the company and what it would take to protect all three parties. Early on, he decided a large part of the answer was stronger authentication.

He and his team began beefing up authentication for every new account opening and every online transaction, starting with customer identification and Office of Foreign Assets Control checks.

"Until people take ownership of and know what to do to protect their own identity and start taking those steps, (fraud) is going to continue to get worse," said Richard Cooney, director of fraud strategy at Axcess Financial.

"We started with that idea, to make authentication as tight, strong and optimized as we can make it so that the person who is trying to manipulate an identity, create a synthetic identity or steal an identity is going to have a hard time getting through that process," Cooney said. "And the good customer is going to come through very easily."

He brought in software from SAS that vets each digital encounter against authentication data from multiple providers. The software helped reduce identity fraud by 80% in 90 days, he said.

"We connect to SAS through an [application programming interface], we move the data that we want validated there, and we collect more information," Cooney explained. "We hook to different companies that can provide us with, for example, customer identification and OFAC checks."

The SAS software helps Axcess look at behavioral aspects of how the application is filled out and sent in, in real time.

"We can look at that in the context of either rule sets that we create of known bad footprints, or we can create scoring algorithms, or we can even go to the extent of using unsupervised machine learning to recognize new patterns that are emerging that we can't even see ourselves," Cooney said. "In the old days, we had a magnifying glass when we looked at an application. Now I have a high-powered microscope, and I can really get way down into the data, which allows me to understand patterns that even fraudsters don't realize they do."

A human investigator reviews every application to determine whether or not it's truly fraudulent.

The new software has helped Axcess's fraud operations team shorten the time needed to investigate consumer identity fraud disputes from hours to minutes per case.

Cooney declined to say how much Axcess has spent on this technology, but said he's not spending more than he used to and the cost benefit has been significant.

"It's not just about stopping the bad guys from coming into your institution," he said. "It's about getting the good people, the people that need your help, through the process in such a way that it doesn't become so onerous that they just throw up their hands and walk away."

Cooney pointed out that knowledge-based authentication, which asks questions like where did you live in 1991, what color was your car and what was the registration number on it, doesn't really work.

"We don't remember those things," he said.

Under the new system, "if you try to commit third-party fraud against me, you're going to be very lucky to succeed," Cooney said.

In addition to bringing in the new authentication platform, Cooney had the team compile a file on everything the company knew about bad actors. That way, instead of blocking victims of stolen or manipulated identities, the company could focus on the wrong information bad actors provide in their applications, to catch synthetic identities that way.

Axcess also plans to start using automated Social Security number validation from the Social Security Administration as soon as that is available. That will help weed out synthetic identities in which valid numbers are combined with valid identity data from other people. It will also help catch the fraudsters who use children's Social Security numbers to create synthetic identities.

"We're going to have a bit of a crisis around 2027, 2028, 2029 and 2030, when all the kids that have been born since 2011 begin to mature and we find out just how many of those identities were used as synthetic items, Cooney said. "I don't think anybody knows right now, but I would say it's in the millions, maybe tens of millions."

Banks often don't recognize synthetic identities. They see a customer who stopped paying, perhaps went on a spending spree, and then disappeared off the face of the earth. These accounts are often labeled credit defaults.

"Many of these losses show up in credit and reserve losses," said John Watkins, global lead for identity and digital fraud solutions at SAS. "Sometimes banks don't know that they have fraud sitting in those reserve losses. And sometimes they choose not to identify it. It's an area that once you see it, you can't un-see it. So they take it as just part of their normal credit losses."

"My hope is that the financial services industry, the insurance industry, the securities industries get to the point where we quit this idea that some losses are acceptable," Cooney said. "We should be starting from the standpoint of no losses are acceptable and working back from there, not starting from the standpoint of, we can lose up to this and we're OK."