Your Bank Customer's Mis-Taken Identity

cyber security risk management

Summary: Synthetic identity fraud is difficult to track and halt due to its very nature. So, what can community banks do to prevent this dangerous fraud from happening?

The Identity Theft Resource Center reports that while the total number of data breaches reported in 2018 declined 23% from the prior year, the reported number of consumer records containing sensitive personally identifiable information (PII) soared 126% over that same period. Overall some 447mm records were exposed in 2018.

More than ever, one's identity defines who they are, so it is critical to protect. Identities link to one's job, bank, to businesses and to other people with whom they communicate online.

Although not new, crooks continue to advance in their practices to create new synthetic identities for their nefarious activities. This easily allows them to create new fraudulent personas through which they can wreak havoc on the banking system.

Using personal information from a variety of people, especially children or even the deceased - cybercriminals may spend months developing a credit rating and a background of sorts for this synthetic identity, in order to rack up debt. One person's name and social security number may be put with someone else's address and another person's phone number. Synthetic fraud is estimated to account for 1 in 5 bank identity fraud cases.

Synthetic identity fraud is one main reason that global card losses is rising at an estimated average rate of 18% per year, according to Accenture. Synthetic identity theft alone is estimated to account for at least 5% of uncollected debt and up to 20% of credit losses, according to industry analysts.

The worst and most pernicious aspect of synthetic identity fraud is its very construct. The information being misused does not belong to any *one* person, but typically is an amalgam of stolen data. That makes it often much harder to track than conventional identity fraud. What is a community bank to do about all this?

Use multiple means to determine your customer's identity. While you know most of your customers well, as your bank grows, this may change. Check not only the customer ID documents, but also validate particular transactions based on the customer and their registered device, as an extra precaution. You may even want to check identities based on personal questions only the customer would know. Don't rule out calling them directly either, if needed, if any red flags appear.

Boost your anti-fraud measures. While your frontline employees are a good first line of defense, they can't do it all. Make sure that you also have an automated system in place that is thorough and allows manual review too when questions may arise. Lexis Nexis' study found that 72% of transactions flagged for manual review by a group of financial firms were done so by an automated system. This can save community bankers time and money, as long as there are not too many false positives.

Consider vulnerable populations. Cyber-criminals, like real-world criminals, often prey on the least suspecting and most vulnerable. This includes children and the elderly, since they are least likely to check

accounts regularly or sound alarm bells. Banks should be wary of customers who have never carried a loan balance or who have sudden increases in account activity.

While there is lots to do on the fraud front, we hope these tips have helped, as you work to stay ahead of the bad guys!

LOAN SERVICES FOR COMMUNITY BANKS

PCBB is almost entirely owned by community banks and it does not compete for your business. Contact us to do loan participations as you protect your customer relationships.