How Do You Identify & Fight Synthetic Identity Fraud?

cyber security risk management pandemic

Summary: Synthetic identity fraud costs financial institutions over $6B per year. This is a continuing problem that has been exacerbated by the coronavirus and affects the most vulnerable populations, such as children and seniors. It is critical to know how to identify and fight synthetic identity fraud with a layered approach and collaboration with other institutions. We provide some insight.

Synthetic fabrics can trace their origin back to 1855 when George Audemars, a Swiss chemist, discovered how to artificially replicate silk using mulberry bark pulp and gummy rubber. Unfortunately for community financial institutions (CFIs), synthetic reproductions have morphed into multiple channels, including fraudulent ones, as in synthetic identity fraud.

Synthetic identity fraud is when false identities are created and used to make fraudulent purchases and open counterfeit accounts and loans. While not new, financial institutions now lose more than $6B annually to synthetic identity fraud. With this as an increasing problem, CFIs need to understand the latest issues around it and how to identify and fight synthetic identity fraud with a layered approach and collaboration with other institutions.

Exacerbated by COVID-19. With social distancing necessitating changes in the way that new accounts are opened, and many people now opening accounts remotely, criminals are seizing the opportunity to utilize synthetic identities. In fact, 60% of businesses experienced losses in 2020 related to account takeovers through synthetic identities. This typically happens by combining information such as a legitimate Social Security number with fictitious information such as a false address or name. Unfortunately, being able to gather this information is easier than ever these days too. There is no shortage of people's personal information that is publicly available online, even before massive data breaches are factored into the mix.

Affecting the most susceptible. With fraudsters typically targeting the most vulnerable communities, children and the elderly are at the top of the list since they are least likely to be actively monitoring their Social Security numbers or to realize their information has been compromised. Given that many children do not realize their Social Security numbers have been compromised until they are old enough to start working, fraudsters are 51x more likely to use the Social Security numbers of children in such efforts than those of adults. CFIs would be well served in educating customers about why these groups are particularly susceptible to such crimes and encouraging active monitoring. More importantly, CFIs need to make sure that the security measures that they put in place account for this as well.

Requires a layered approach. According to the Federal Reserve, the best way for organizations to identify synthetic identity fraud is by utilizing a tiered approach to information analysis that relies on a combination of digital and manual information analysis to ensure that the authenticity of the individual opening an account. While checking names, Social Security numbers, and birth dates against those on file with the government is important, it is not enough. CFIs should consider a combination of security measures from cross-checking the documents that applicants use to open accounts against things such as an individual's transaction history to incorporating features such as on-the-spot selfies to validate an individual vs. a photo of that person.

Collaborate with other institutions. Given the vast amount of data to manage these days, it is important to leverage trends and best practices that are shared by other institutions and payment providers. In one of its white papers on synthetic identity fraud, the Federal Reserve notes that through information sharing, fraud detection and mitigation can be enhanced. The Fed's white paper further notes, "*Collaboration can help stakeholders aggregate and analyze data on synthetic identity fraud – and smaller financial institutions and other stakeholders report these collaborative partnerships to be successful.*"

The fight against synthetic identity fraud is far from over as the fraudsters continue to find new ways to breach the system and configure identities. So, we will continue to bring you the latest updates in order to keep you and your customers safe now and in the future.

OUTSOURCE ALM SERVICES AND REST EASY

Regulators have raised the bar on interest rate risk and liquidity analysis, yet there is more to do than there are hours in a day. To see how easy it can be & get expert help, contact us today.