AMERICAN BANKER®

Updated customer identification rules are long overdue

By Maxwell Blumenfeld | April 22, 2022

Modern customer identification regulations are not only outdated, but actually contribute to a rise in identity crimes. New threats posed by identity fraud today have made the federal Customer Identification Program regulatory framework obsolete, and also exacerbate the issues that CIP was designed to address. Federal regulators, the Financial Crimes Enforcement Network in particular, are exploring whether modernization of these rules is necessary. In fact, it is critically overdue.

Take synthetic identity fraud, for example. This type of identity crime — which causes billions in losses to financial institutions — was seemingly designed by fraudsters to circumvent CIP regulatory requirements. A "mature" synthetic identity has some amount of positive credit history and a name, date of birth, Social Security number and address that match with what appears to be a credit report of a legitimate person, and which is often used for nondocumentary ID verification.

In the event this application is approved for even a relatively "low-risk" credit product, the financial institution will face losses from "bust-out" fraud and the regulatory and reputational harm that comes from money laundering or other financial crimes for which synthetic identities are often used. For example, based on our analysis, credit card accounts associated with synthetic identities charge off at a rate 50 times more frequently than a typical consumer, and for an average of $13,000. Some financial products are specifically targeted by synthetic identities as a means to build their credit score and receive larger lines of credit elsewhere.

In existing CIP requirements, verifying an applicant's physical address is important to forming a true belief of their identity. However, the mailing address is no longer a reliable indicator of risk with the move to fully digital experiences. It's no longer a prerequisite to activate something received in the mail (such as a debit card) to start using a new loan or line of credit. And, because of countless data breaches, it is now all too easy to obtain a valid name, date of birth, SSN and address combination which can be simply paired on a new account application with an email and phone number controlled by the fraudster.

A basic CIP check wouldn't require verification of email or phone which, on a digital application, is often all that is required to open an account using a stolen identity.

To illustrate this, we examined just over 92,000 checking account applications over the last year that our models indicated as likely based on stolen identities. Nearly 55% had a consistent address history of at least two years. Of those: 68% provided known risky VoIP phone numbers, and 82% of the phone numbers provided had an area code with no connection to the applicant. Further, 77% included a brand-new e-mail address, or one that had been created less than two months before the application date.

It's clear that the tactics used by fraudsters are able to circumvent existing CIP requirements and compliance minimums by simply controlling the means of electronic communication.

The CIP rules outline a less rigorous identity verification process for someone applying for a basic checking account than for, as an example, a high-net-worth individual applying for an offshore private banking account. On the surface, there's some logic to this. In reality it's an antiquated approach that's overly focused on factors like product type instead of the actual threats financial institutions face from identity fraud.

This reality was brought into focus during the pandemic. The U.S. Department of Labor Inspector General estimates that as much as $80 billion was stolen in unemployment insurance fraud during the pandemic. While it would be easy to criticize the states that administered these payments for lackluster identity verification controls, the enormous influx of unemployment claims to state agencies created a nearly impossible task of verifying identities and providing funds quickly to consumers in need. The CIP rules provided little backstop against identity thieves in need of accounts to receive ill-gotten funds, since the perceived regulatory risk associated with opening a checking account is so low. The incidence of incoming checking account applications with stolen credentials reached all-time highs in 2021 as fraudsters found an easy way to launder illegitimate benefits through U.S. financial institutions.

Technology has allowed established financial institutions and newcomers to make it easier for customers to access financial products and services. Fraud typologies such as synthetic fraud continue to emerge that have found ways to elude traditional CIP checks. The billions lost in pandemic-related government fraud highlights the need to rethink controls related to financial products previously believed to be low risk.

Technology and the market have changed. Customer identification rules should, too.