THOMSON REUTERS

REGULATORY INTELLIGENCE

U.S. Fed-led group on synthetic identity fraud agrees common definition; big step against complex crime

Published 21-May-2021 by
Henry Engler, Regulatory Intelligence

U.S. banks may now be better equipped to battle synthetic identity fraud, one of the fastest-growing financial crimes in the United States, and an increasing concern for regulators. An agreement by a Federal Reserve-led focus group on a common definition of what constitutes identity fraud has raised expectations that banks will be able to more effectively identify, classify and combat the complex, widespread crime.

The Fed announced last month an agreed definition of synthetic identity fraud (SIF), which was developed by a group of fraud experts. Estimates suggest that synthetic identity fraud has cost U.S. lenders up to $6 billion, and that the financial theft accounts for 10–15% of charge offs in a typical unsecured lending portfolio.

“A shared understanding of what constitutes synthetic identity fraud is expected to improve its detection, measurement and mitigation in the payments industry,” said Jim Cunha, senior vice president, Federal Reserve Bank of Boston. “Consistent use of this definition within and across organizations can enable us to discuss, identify and classify synthetic identity fraud in a similar manner.”

The industry-recommended definition of synthetic identify fraud, or SIF, is the “use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.” The definition also includes primary and supplemental elements:

- **Primary elements**: Identity elements that are, in combination, typically unique to an individual or profile (e.g., name, date of birth, Social Security number and other government-issued identifiers)
- **Supplemental elements**: Elements that can help substantiate or enhance the validity of an identity but cannot establish an identity by themselves (e.g., mailing or billing address, phone number, email address or digital footprint)

Unlike Other Types of Fraud

A synthetic identity is created by using a combination of real information, such as a legitimate Social Security number, and fictitious information, which can include a false name, address, or date of birth.

Synthetic identities can be used to establish accounts that behave like legitimate accounts and may not be flagged as suspicious using conventional fraud detection models. This affords fraudsters the time to cultivate these identities, build positive credit histories, and increase their borrowing or spending power before “busting out” – the process of maxing out a line of credit with no intention to repay.

There are two significant challenges that synthetic fraud creates for the banking industry: detection and classification.

The fraudster can leverage legitimate processes through tactics such as “piggybacking” – adding a synthetic identity as an authorized user on an account belonging to another individual with good credit. In many cases, the synthetic identity acquires the primary user’s established credit history, rapidly building a positive credit score. Fraudsters also can piggyback new identities onto accounts owned by established synthetic identities, or “sleepers,” within a portfolio.

Apart from the detection challenge, one of the biggest hurdles is how banks classify this type of fraud on their books, which varies and makes getting one’s hands around the problem more difficult.

Industry Collaboration Seen Essential

Because of complex nature of the innovative crime, experts applauded the Fed’s role in facilitating an industry discussion on how to define synthetic identity fraud, which should better equip banks to identify and classify such activities.

“I think the Fed’s big concern is that they really want to promote awareness of this,” said Greg Woolf, CEO of FiVerity, a fintech company that took part in the Fed’s focus group.

“By the Fed putting a stake in ground has enabled greater collaboration by the industry,” Woolf told Regulatory Intelligence. “This is a starting point and allows the industry to get together and develop community group solutions.”

Many of the focus group participants were smaller tech firms such as FiVerity, but there were also larger companies such as MasterCard and LexisNexis Risk Solutions.

Speaking the Same Language on SIF

Fed officials said they hope financial institutions and other organizations will start to incorporate the new industry-recommended definition into their existing fraud models and internal fraud reporting.

“The Fed and focus group members envision that a consistent definition for synthetic identity fraud could be applied in multiple ways – each resulting in unique, but complementary benefits,” Mike Timoney, vice president for secure payments at the Federal Reserve Bank of Boston, told Regulatory Intelligence.

Among the benefits expected, Timoney highlighted several, including fostering the ability to “speak the same language by creating a baseline to promote a consistent conversation and understanding across the industry.”

In addition, the definition should help banks to classify SIF and prevent “mis-categorization of losses and provide insights into where losses are occurring.” The effort should also improve bank fraud modeling, monitoring and overall management of SIF, Timoney said.

(Henry Engler, Regulatory Intelligence)

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 21-May-2021