FedPayments Improvement COMMUNITY FORUM

Collaborate. Engage. Transform.

Synthetic Identity Payments Fraud
Nobody Knows You're a Dog

In late 2018, a diverse group of 300 industry stakeholders came together at the FedPayments Improvement Community Forum to engage in inclusive dialogue focused on improving the U.S. payment system. Through general sessions and topic-specific workshops, Forum attendees provided their candid feedback about the latest payment modernization efforts.

In this workshop expert panelists discussed how synthetic identities are used to commit payments fraud and the challenges of mitigating this type of fraud.

Moderator

Jim Cunha, Senior Vice President
Federal Reserve Bank of Boston

Panelists

Brian Murphy, Vice President and Policy Director
American Bankers Association Office of Strategic Engagement

Joan Pappas, Senior Vice President
Enterprise Fraud Management and Control – Senior Fraud Policy Analyst
Bank of America

Seth Kressin
Senior Fraud Data Scientist
Experian

Highlights From the Panel Discussion

Synthetic identity fraud is considered to be one of the fastest-growing and hardest-to-detect forms of identity fraud today. *Nobody knows you're a dog* refers to online anonymity.

The expert panel, audience Q&A and facilitated small-group discussions were valuable for understanding where the payments system is vulnerable to synthetic identity fraud, as well as helping the Federal Reserve and industry identify ideas and opportunities for actions that could address the challenges and facilitate fraud mitigation.

Synthetic identity fraud is defined as the combination of real information – such as a legitimate Social Security number – with fictitious information (e.g., a false name and date of birth) to create a new identity. Fraudsters can use this fake identity to obtain credit, build a good credit score by keeping up with payments and then commit fraudulent payments activity (bust-out fraud). While not all synthetic identities are created for the purpose of payments fraud, payments fraud was the focus of this panel.

The panelists explained that synthetic identity payments fraud has been exacerbated by several factors, including:

- A change in policy at the Social Security Administration (which now assigns Social Security numbers randomly, making fraud harder to detect).
- People charging a fee to allow a fraudster to become a secondary authorized user on their account (thus inheriting their FICO score).
- The number of years that identity theft involving a child's Social Security number can go undetected.

The panelists agreed on the need for increased collaboration between all stakeholders, the need to educate the public about how to protect their identities and credit histories (including children), and the need for more law enforcement.

CONTINUED ON PAGE 2

Brian Murphy of the American Bankers Association explained that the ABA lobbied Congress for the Economic Growth, Regulatory Relief and Consumer Protection Act (S. 2155), which directs the Social Security Administration to allow online identity-verification requests to its database of people's names, dates of birth and Social Security numbers.

Murphy said this law will be a "game changer" because it allows the industry to interdict fraud before it happens. If a synthetic identity is rejected, the fraudster cannot use it to create a credit file, obtain credit cards and take out loans that won't be repaid.

Joan Pappas of Bank of America said traditional methods of fraud detection are inadequate to detect synthetic identities. She explained that it's difficult to operationalize detection, because it requires a manual review of suspect accounts for red flags, such as a short time on the record and the opening of several accounts over a short period of time.

Also, incident coding can be inconsistent. Banks don't have a flag for both credit loss and synthetic identity payments fraud.

Seth Kressin of Experian agreed that identifying synthetic identities is a manual process. However, he believes that banks are doing a better job of detecting and reporting it to Experian and other credit bureaus. In addition, Experian is working on custom machine-learning models to prevent application fraud.

Kressin noted that synthetic identities can last for years – and through repeated "bust out and rebuild" cycles – unless they are identified and removed from financial institution and merchant databases.

Algorithms can be used to determine whether a given payment or order is similar to the customer's historical patterns, but data modeling is only as good as the data you have.

Tabletop Takeaways

- Attendees discussed actions the industry could collectively take to address synthetic identity payments fraud and to prioritize the challenges from that list.

The audience suggested:

- Improve loss classification to better distinguish fraud loss versus credit loss.
- Improve behavioral analytics to screen transactions and verify identity at three key points: account opening; application for additional credit; and adding an authorized user.
- Facilitate collaboration among the Social Security Administration, law enforcement, financial institutions, credit bureaus and the U.S. Postal Inspector (for international payments fraud).

Industry can collaborate by:

- Sharing examples of payments fraud across institutions.
- Building a database of suspicious and confirmed payments fraud.
- Having the credit bureaus share information and/or serve as fraud data aggregators.
- Creating consumer alerts, including an alert or challenge for new accounts.
- Regularly scrubbing their databases of Social Security numbers against the Social Security Administration database, which will be much easier to do when the agency fully implements electronic access to this database using e-consent.
- Easing regulations to help support more information sharing.
- Building a national register or database on synthetic identity fraud.