Executive Summary – Synthetic Identity

When Payments Fraud Wears a 'New Face'

Synthetic identities are essentially fictional "people" linked to valid Social Security numbers. The creation of synthetic identities is increasingly popular among fraudsters, who can use the identity to commit payments fraud and other types of fraud, such as filing false insurance claims or applying for government benefits that the fraudster isn't eligible to receive. Unfortunately, the very nature of synthetic identity payments fraud makes it more difficult to determine the scope of the problem, much less how to prevent it. While the immediate victims are financial institutions and individuals, synthetic identity payments fraud ultimately drives up costs for everyone in the U.S. payment system.

When are "you" not "you?" When someone decides to commit payments fraud by creating a "synthetic you" – for example, by combining your Social Security number with a fictional name, date of birth and address to create a synthetic identity with its own credit file. Fraudsters can use this newly created identity to apply for loans or credit cards and walk away with a lot of money that they never intend to repay. Financial institutions and law enforcement officials face the challenge of finding the person behind the synthetic identity.

> *"Synthetic identity payments fraud is rising due to large-scale data breaches, use of static information for identification, the shift to remote payments channels and remote applications for payment accounts, a lack of identifiable victims reporting fraud – and high payoffs for fraudsters. A better understanding of synthetic identity payments fraud can improve our ability to address it."*
>
> **Ken Montgomery**
> Payments Security Strategy Leader
> First VP & COO, Federal Reserve Bank of Boston

The theft and use of a Social Security number for payments fraud can go undetected for many years – and synthetic identity payments fraud is rarely reported because financial institutions may not realize fraud has been committed. Typically, a synthetic identity can cause the real person to receive an unexpectedly negative response after checking his or her credit report or applying for a new loan or line of credit. The most likely victims of this type of fraud are children, the elderly, the homeless and those who are incarcerated. For example, fraudsters can take advantage of children's personal information for several years, since kids generally don't apply for credit until age 18 or later. Likewise, senior citizens are less likely to apply for standard mortgages, student loans or new credit cards, processes that might uncover credit problems. To clean up their credit histories, individuals must prove that they did not incur the synthetic identity's debt. Fraudsters also use the Social Security numbers of deceased people, which may be readily available due to data breaches.

Five Steps of Synthetic Identity Payments Fraud

1. A fraudster creates a synthetic identity using a combination of real and fictional personal information – generally including a valid Social Security number which is not actively being used – to apply for a low-limit loan or credit card.

2. The financial institution submits an inquiry to one or more credit bureaus, which report back that the identity does not have a credit history. As a result, the financial institution typically rejects this initial application for credit. However, this initial inquiry creates a credit file for the synthetic identity – even though the application was rejected.

   As another precaution, the financial institution can use the Social Security Administration's Consent Based Social Security Number Verification (CBSV) Service to verify that the applicant's name, date of birth and Social Security number match the administration's records. However, this verification currently requires written consent of the Social Security number holder and cannot yet be requested electronically.

3. The fraudster keeps applying for credit until the financial institution approves that first low-limit loan or credit card. After the fraudster makes timely payments over a few months or even years, the synthetic identity has a firmly established and positive credit report. This enables the fraudster to successfully request higher credit limits and/or additional accounts. The fraudster can accelerate the process of building good credit by "piggybacking" – offering a fee to an existing cardholder with good credit in exchange for adding the fraudster as an authorized user on the cardholder's account for a short time.

4. To obtain as much money as possible, the fraudster then "busts out" by maxing out the established credit and vanishing. The financial institution cannot find a real person to pursue for payment. In fact, it may be unclear that this is not a real person simply walking away from a debt.

5. Whenever possible, the fraudster will "rinse and repeat" the payments fraud using this same synthetic identity.

The Federal Reserve Continues to Advance Payments Security

The Federal Reserve has a history of working transparently and collaboratively with the payments industry to reduce fraud risk and advance the safety, security and resiliency of the payment system. As outlined in the 2017 paper, *Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey*, the Federal Reserve works to identify payments security vulnerabilities, potential mitigation approaches and challenges that may hinder progress.

In 2019, the Federal Reserve launched a synthetic identity payments fraud initiative to educate the industry, create a sense of urgency and influence action. The Federal Reserve's focus is on both research and industry dialogue about synthetic identity fraud in the U.S. payment system, including the scope of the issue and mitigation strategies. Working collaboratively, the Federal Reserve and industry seek to reduce synthetic identity payments fraud in the United States over time.

For more information, visit FedPaymentsImprovement.org and submit or update your FedPayments Improvement Community profile and select "Payment Identity Management" as a topic of interest.

THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.