

SYNTHETIC IDENTITY FRAUD: WHAT IS IT AND WHY YOU SHOULD CARE?



Many types of fraud infiltrate the payment system, making it hard to stay one step ahead of the fraudsters. Synthetic identity fraud is one type that is gaining attention in the industry. Read on to understand more about this **fast-growing financial crime**.

WHAT IS SYNTHETIC IDENTITY FRAUD?

Synthetic identity fraud is defined as 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.

Synthetic identity fraud consists of two main components:

1. **The creation of a synthetic identity**
2. **Using that identity to commit fraud**


Note: Sometimes, synthetic identity fraud is committed multiple times using the same identity.

Conventional identity theft occurs when one's existing identity is stolen. In contrast, synthetic identity fraud occurs when a new identity – a synthetic identity – is created. There are various approaches to creating a synthetic identity, but all include piecing together PII, such as a name, date of birth and Social Security number (or other government-issued identifier) to establish a new person or entity.

WHY IS IT IMPORTANT TO KNOW ABOUT SYNTHETIC IDENTITY FRAUD?

- **Synthetic identity fraud accounts for substantial financial loss.**

While today's fraud estimates are concerning, perhaps a greater concern is that the loss dollars and number of incidents continue to grow year over year. In 2020, initial estimates indicate losses within the U.S. financial system were \$20 billion¹, up from \$14.7 billion² in 2018. That, combined with the underreporting of synthetic identity fraud due to miscategorization of credit loss, highlights the need for action.



SYNTHETIC IDENTITY FRAUD: WHAT IS IT AND WHY YOU SHOULD CARE?

- **Synthetic identity fraud is growing in frequency and impact.**

The ease of synthetic creation and the increase in digital account applications have simplified the process of creating these fictitious people and allowing them to penetrate the financial system.

- **Synthetic identity fraud is often undetected by traditional fraud models.**

Many fraud models are not built to look for fabricated identities but assume all identities are real. These models focus more on the payment behavior or alteration of elements belonging to the identity and not on characteristics of the identity making the payment. This allows synthetics to go undetected by many models.


- **Synthetic identity fraud is extremely pervasive, with numerous avenues for application.**

While the Federal Reserve's focus is on the impact synthetics have on the payments industry, synthetics are used to defraud multiple industries, including healthcare and government. The ease and low cost of creating synthetic identities contribute to their widespread use, making synthetic identity fraud one of the most far-reaching types of fraud. Once a synthetic is created, it can be used across multiple organizations at the same time, increasing the payout for the fraudster, but also the impact to the overall financial ecosystem.

- **Synthetic identity fraud can have a devastating impact on individuals.**

Although the initial financial impact usually is felt by a financial organization, the use of synthetic identities also negatively affects individuals. When a synthetic identity was created using an existing Social Security number (SSN), the individual who legally owns that SSN is likely to have poor credit ratings and/or outstanding debt as a result of fraudulent activity associated with that SSN (albeit under a separate identity).

Furthermore, some of the more vulnerable populations, such as children and the elderly, are key targets of fraudsters wishing to create synthetic identities. These populations are attractive to fraudsters as they aren't typically active credit users and, therefore, are not as likely to notice fraudulent activity.



SYNTHETIC IDENTITY FRAUD: WHAT IS IT AND WHY YOU SHOULD CARE?

CHILDREN ARE COMMON VICTIMS OF SYNTHETIC IDENTITY FRAUD

Why:

- Parents typically don't actively monitor their children's identities, credit scores, etc.
- Children do not typically use SSNs until they are old enough to drive, be employed or apply for individual credit lines.

Impact:

- Negative or derogatory information associated with the SSN may not be discovered until the child reaches the upper teens, resulting in several years of fraudulent activity tied to the SSN that must be remedied.
- This can affect the individual's employment opportunities and/or creditworthiness.

TAKE ACTION

Understanding synthetic identity fraud and how it impacts your organization provides a strong foundation for the fight against it. Find more information throughout this toolkit.

SOURCES

¹ [2021 Synthetic Identity Fraud Report](#), FiVerity

² [Deep Dive: How FIs Are Looking Beyond Traditional Know Your Customer Data to Spot Synthetic Identity Fraud](#), PYMNTS.com, July 28, 2020

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.