COLLABORATE. ENGAGE. TRANSFORM.

Defining Synthetic Identity Fraud

A Fed-led effort involving industry experts to create an industry-recommended definition for synthetic identity fraud

THE FEDERAL RESERVE
FedPayments Improvement

Table of Contents

The Need to Define Synthetic Identity Fraud

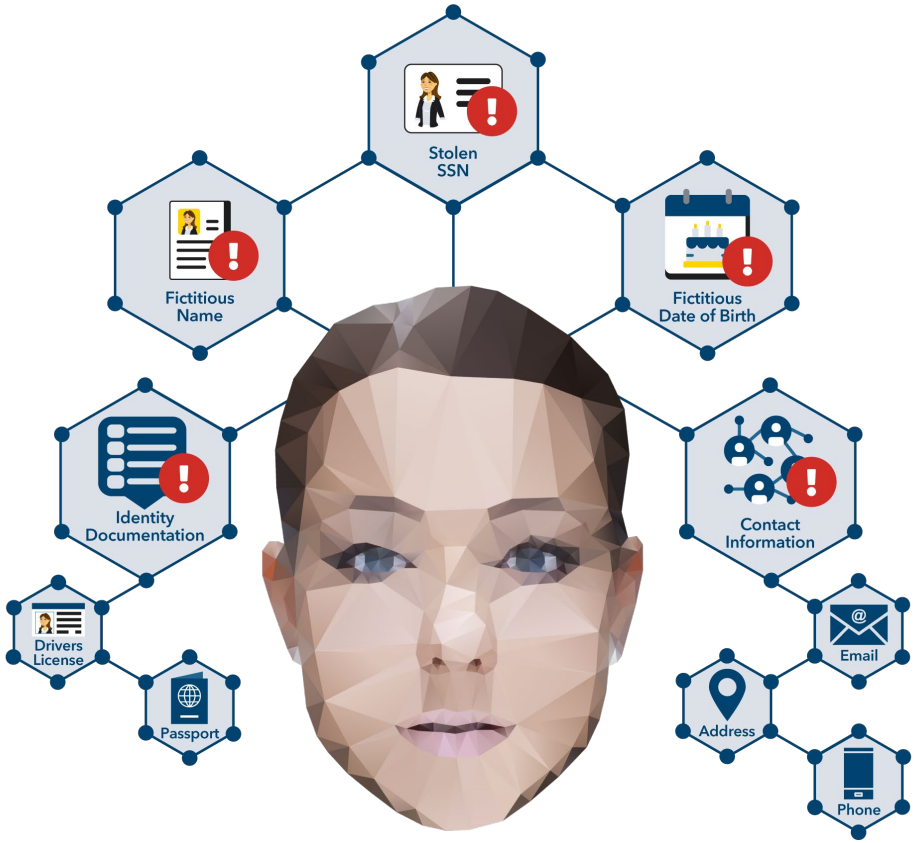
- Reported to be the fastest growing type of financial crime[1]
- Multiple definitions in use which can lead to inconsistent categorization and reporting, making it difficult to identify and mitigate this type of fraud.

To respond to this challenge, the Federal Reserve assembled a focus group of 12 fraud experts to develop an industry-recommended definition of synthetic identity fraud.

1. Reported to be the fastest growing by multiple sources, including: FBI, Experian, and GIACT

Synthetic Identity Fraud (SIF) Definition

The use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain



Note: This definition of synthetic identity fraud 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 definition throughout the industry is encouraged, adoption of the definition is voluntary at the discretion of each individual entity. Absent written consent, this definition may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Synthetic Identity Creation

The following reflects personally identifiable information (PII) elements that may be used to create a synthetic identity.

Note: These are solely examples and do not represent an exhaustive list.

Element Type	Description	Examples
Primary	Identity elements that are, in combination, typically unique to an individual or profile	• Name • Date of birth • Social security number • Other government-issued identifiers (such as a passport or tax identification number)
Secondary	Elements that can help substantiate or enhance the validity of an identity but cannot establish an identity by themselves	• Mailing or billing address • Email address • Phone number(s) • Digital footprint (such as device ID or IP address)

Common Uses of Synthetic Identities in Fraud

The following list describes common uses of synthetic identities.

Note: These are solely examples and do not represent an exhaustive list. The first three uses are listed in alphabetical order and the order does not suggest a hierarchy, with the fourth item grouping additional common uses for synthetic identities.

Type of Use	Description
Credit Repair	Used to hide from previous negative credit history or bad debt in order to appear creditworthy
Fraud for Living	Used to apply for employment or services such as utilities, housing, and bank accounts because an individual is unwilling or unable to do so with existing primary PII elements, with no intent to default on payment
Payment Default Scheme	Used to obtain goods, cash, or services with no intent to repay over a period of time
Other Criminal Activity	Used to facilitate a means to an end as part of illegal acts *Note: These illegal acts can include activities such as avoiding legal responsibilities, money laundering, human and/or narcotics trafficking, up through and including terrorist financing; these types of activities can be conducted by a wide variety of criminals, ranging from individuals to transnational organized crime groups.*

Potential Methods of Industry Application

- The Federal Reserve 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.
- The approaches below are based on a voluntary adoption progression, anticipating that:
  - Some organizations may lead the industry with early adoption, which may then encourage others to follow, ultimately resulting in widespread adoption.
  - The timing and approach for incorporating the definition will vary by organization based on unique business needs and objectives.

1. *Increase Industry Education and Awareness*
2. *Foster the Ability to Speak the Same Fraud Language*
3. *Enable Consistent Identification and Classification*
4. *Help Organizations Improve Fraud Modeling*

Increase Industry Education and Awareness

Helping the industry understand what constitutes synthetic identity fraud and its impacts on consumers, organizations, and the overall U.S. payments system

- The definition includes a focus on the identity itself and elements used to create the identity, as opposed to payment behaviors.
- This helps distinguish synthetic identity fraud from other types of losses (e.g., credit losses, conventional identity theft, etc.)
- The examples of PII elements can help the industry understand what pieces of information may be used to create a synthetic identity.
- These examples highlight customer information to closely examine or monitor in critical processes such as customer onboarding, account opening, and transaction behavior.
- The common uses provide the industry a clearer picture of the multiple ways synthetics are used and the far-reaching impact of synthetic identity fraud.

Foster the Ability to Speak the Same Language

Creating a baseline to promote a consistent conversation and understanding across the industry

- Within an organization, this definition enables employees to identify and discuss synthetic identity fraud in a consistent manner.
- Across the industry, this definition can also facilitate a common language on synthetic identity fraud and, where appropriate, help improve industry collaboration.

Enable Consistent Identification and Classification

Preventing miscategorization of losses and provides insights into where losses are actually occurring

- The definition can help organizations better identify this type of fraud and help differentiate the event from a credit loss or another type of fraud, which can help organizations:
  - Better recognize losses that have been attributed to other causes are, in fact, a result of synthetic identity fraud
  - Help prevent miscategorization of synthetic identity fraud and enable consistent classification of these events
- The definition enables organizations to focus on who initiated the payment and how the fraud was conducted rather than the payment itself.
  This is similar to the approach laid out in the recently published FraudClassifier℠ model.
- Consistent identification and classification of synthetics can help the industry better understand the scope and magnitude of this issue and the fraud tactics behind this fraud type and develop improved mitigation strategies.

Help Organizations Improve Fraud Modeling

Providing potential ways to increase monitoring
and improve overall fraud management of synthetic identity fraud

- The definition and PII examples can begin to help organizations:
  - Know what to monitor, focusing models on the identity itself (rather than conventional fraud models which focus primarily on payment behaviors)
  - Better quantify the extent of synthetic identities within their portfolios
- Including these elements with behavioral and transactional monitoring can provide additional insights, helping aid the organization better understand fraud trends around synthetic identities.
- The combination of insights gained from consistent classification and increased monitoring could help organizations improve fraud management within modeling (including detection, mitigation, and prevention).

FUTURE OUTLOOK

Vision for Industry Application of Definition

- The industry-recommended definition for synthetic identity fraud can help serve as an important step toward improving consistent identification and classification of synthetic identity fraud.
- While the goal of this effort was to define synthetic identity fraud in the context of the payments industry, the Fed and the focus group recognize this issue impacts many industries (e.g., healthcare, insurance, government agencies, etc.).
  - As a result, the group built this definition with potential application by other industries in mind.
  - This could help facilitate broader use of a similar language about synthetic identity fraud, which could also help prevent fraudsters from leveraging synthetic identities across multiple industries.

Industry socialization of the definition can help promote a consistent understanding of synthetic identity fraud; however, it is the application of the definition by industry stakeholders that can begin building the foundation in the fight against synthetic identity fraud.

FUTURE OUTLOOK

Federal Reserve's Plan to Encourage Adoption

- Actively socialize the definition and its potential applications with the industry
- Replace the synthetic identity fraud definition in the FraudClassifier model with the new definition
- Continue research and outreach efforts to increase industry awareness and understanding of synthetic identity fraud
- Explore ways to arm the industry with additional insights and resources for identifying and managing this type of fraud, including the planned development of a fraud mitigation toolkit

FUTURE OUTLOOK

Join the Fight Against Synthetic Identity Fraud

- Consider how your organization may incorporate this definition and join the industry in helping advance our collective fight against fraud.
- Visit our synthetic identity fraud definition page on FedPayments Improvement to learn more!
- Share your ideas for the planned synthetic identity fraud mitigation toolkit at: SecurePayments@bos.frb.org.

FedPaymentsImprovement.org

fedpayments-improvement

@FedPayImprove

FedpaymentsimprovementOrg

THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

Defining Synthetic Identity Fraud: *Appendix*

A Fed-led effort involving industry experts to create an industry-recommended definition for synthetic identity fraud

APPENDIX

Focus Group Members

The following industry experts were part of the Fed-led focus group that developed this industry-recommended definition of synthetic identity fraud.

- Aaron Brehove, Truist
- John Buzzard, Javelin
- Mike Cook, SentiLink
- Lee Cookman, TransUnion
- Jeffrey Feinstein, Lexis Nexis Risk Solutions
- Toni Gillich, U.S. Government Accountability Office
- Claire Le Gal, MasterCard
- Jack Lynch, PSCU
- Stacey Nash, USAA
- Donald Rebovich, CIMIP, Utica College
- Amy Walraven, Turnkey Risk Solutions
- Greg Woolf, FiVerity