HOW IS A SYNTHETIC IDENTITY CREATED?

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. Before this type of fraud can be committed, the identity itself must be created. Read on to understand how a synthetic identity is created and then often groomed for a specific use.

INITIAL CREATION OF THE IDENTITY

Two critical pieces of synthetic identity creation are the elements used and how they are pieced together.

Elements Used

Fraudsters can use a multitude of PII elements to create a synthetic identity. Below are examples of the types of elements (primary versus supplemental) that are often utilized:

- **Primary elements:** Identity elements that are, in combination, typically unique to an individual or profile.

  Examples include name, date of birth, Social Security number (SSN) and other government-issued identifiers (such as a passport or tax identification number).

- **Supplemental elements:** Elements that can help substantiate or enhance the validity of an identity but cannot establish an identity by themselves.

  Examples include mailing or billing address, email address, phone number(s) or digital footprint (such as device ID or IP address).

HOW IS A SYNTHETIC IDENTITY CREATED?

How the elements are pieced together

These PII elements can be taken from a real identity or made up as part of the synthetic creation process. There are three main ways, or methods, for creating synthetic identities:

Method	Description
Fabrication	Involves creating completely fictitious personally identifiable information elements, without using any known real or compromised elements. *Example: An individual creates a synthetic identity by inventing a new name, selecting his favorite holiday for the date of birth, and choosing a random number for the SSN (keeping in mind the conditions that must be met to be considered valid).*
Manipulation	Limited modifications to a real identity's personally identifiable information elements. *Example: An individual creates a new identity with his name and date of birth, but with a modified SSN (altering just a few digits of the SSN).*
Compilation	Involves a combination of real and fake personally identifiable information. *Example: An individual creates a synthetic identity using his SSN but a made-up name and post office box as a mailing address.*

HOW IS A SYNTHETIC IDENTITY CREATED?

VALIDATING THE IDENTITY FOR FUTURE USE

Once an identity is created, the fraudster must introduce it into the financial system. The steps below identify a common approach used by fraudsters to prepare the synthetic for maximum use.

CREDIT LINE EXAMPLE

Step 1: Fraudster applies for credit using the created identity

The fraudster begins validating the identity by first applying for a credit line of some sort. This prompts the financial institution to submit an inquiry to one or more credit bureaus, which will report 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.

Step 2: Fraudster repeatedly applies for credit until approved

The fraudster continues to apply for credit at various financial institutions until one finally grants approval.

Step 3: Fraudster builds, and sometimes accelerates building of, a positive credit history

The fraudster will typically use this line of credit and establish a timely repayment history to cultivate higher credit limits and possibly open additional accounts using this identity. This cultivation can take place over months or even years, especially when the owners of the associated SSNs are not active in the credit system and therefore, are not aware of credit activity (e.g., children and the elderly).

The fraudster can accelerate the process of building good credit by piggybacking – being added as an authorized user to an account with good credit to then acquire the established credit history of the primary user. Piggybacking also can occur on another established synthetic identity with a positive credit history, or on synthetic identities associated with fictitious businesses, which also may extend lines of credit.
Note: In some cases, the fraudster may "skip" this step if satisfied with the initial credit line or loan approval.

Step 4: Fraudster leverages synthetic identity to conduct a purchase(s)

Once the fraudster is satisfied with the amount of credit available, a purchase (or series of purchases) is made with no intent to repay the lender. Fraudsters also use synthetic identities to create fake businesses and sign up with merchant processors to obtain credit card terminals and run up charges on fraudulent cards. Sophisticated crime rings use these tactics at scale, developing intricate networks that support the cultivation of synthetic identities to commit fraud.

HOW IS A SYNTHETIC IDENTITY CREATED?

While it is common to use a synthetic identity in creating and growing a credit line, as depicted in the example above, synthetic identities also can be used to open other accounts, such as a demand deposit account (DDA). By using a synthetic to open a DDA, the fraudster can deposit and withdraw money seamlessly with little or no scrutiny from the institution. This comes in handy when the fraudster wants to move or withdraw funds acquired from other fraudulent acts or endeavors (often using synthetics for those, as well). It also allows them the means to capitalize on timing gaps in deposit and withdrawal activity.

SUBSTANTIATING THE IDENTITY

Fraudsters have become increasingly more sophisticated in how they make the identity appear real. This is typically done for both the credit line and DDA account opening scenarios. Tactics that help validate the "proof of life" of the synthetic include:

- Setting up common household utilities (e.g., electricity, water, gas, etc.)
- Creating and maintaining social media pages
- Signing up for reward and loyalty program accounts
- Obtaining fictitious identity documentation, such as a fake driver's license or passport
- Using drop addresses (e.g., P.O. Box addresses or addresses of vacant properties or vacation homes) that allow fraudsters to receive credit cards or goods without disclosing their actual locations

LEARN MORE

Explore the fraud mitigation toolkit to learn how synthetics are used.