

Synthetic Identity: A U.S. Payments Forum Resource Brief

This payments brief seeks to highlight fraud trends related to synthetic IDs and suggest ways to identify and mitigate this fraud. Identity is essential to safe and secure operations in the payments industry. Establishing identity is one of the first exchanges of information between consumers and merchants, card issuers and other stakeholders. To establish that the consumer identity is valid, stakeholders need to be able to trust the information being shared by the consumer; issuers' Know Your Customer (KYC) processes check this information to determine validity. Once the information is verified, the consumer's identity is established.

Synthetic identity (also known as synthetic ID) fraud happens when the information shared to establish identity appears valid but is not. When this takes place, trust is incorrectly established and given to a fictitious entity.

Synthetic IDs serve one of the core desires of fraudsters: the desire to remain undetected. Fraudsters devote extraordinary efforts to create synthetic identities that can pass KYC checks due to their value in committing fraud. Once a synthetic ID has been created, trust can be established with numerous financial institutions, merchants, and other organizations.

Synthetic ID fraud is different from traditional identity fraud. In traditional identity fraud, the fraudster takes over a real person's account. In synthetic identity fraud, there is no real person; a new identity is created to commit fraud. Since there is no real person to notice fraudulent activity, any fraud is much harder to detect.

Synthetic IDs can be used in a number of ways for payments. The two most common use cases are the creation of a new merchant account or the creation of a new personal or business credit card account.

1. **New Merchant Account Creation**

   Creating a new merchant account for payment processing starts with the merchant onboarding process, where a financial institution validates the merchant's identity. Fraudster merchants may be using a synthetic identity with the intention of committing fraud, defaulting with maximum credit limits, or accepting fraudulent payments with stolen payment credentials.

   Typical risk assessments done by acquirers are credit risk checks. Fraudster merchants will start with smaller credit limits, make regular payments over a period of time, request a credit line increase, and then perform fraud with the account to cash out. A common practice for these merchants is to pose as nonprofits accepting donations.

U.S. Payments Forum ©2023

A typical new merchant application process requires a business bank account, financial statements, business license, physical address, and the documents establishing a business identity. These records are not very useful to individuals or companies to establish a trusted identity.

2. **New Personal or Business Credit Card Account**

   Fraudsters with poor or no credit start by using synthetic IDs to get credit accounts, such as secured credit cards. Secured cards are a bank product where a deposit is held against the loan until sufficient customer relationship data can be established; this helps to prevent default risk. Typically, the fraudster will use the card and pay charges on time, behaving as a good cardholder would. Over time, this behavior leads to increases in the card's credit line. When the credit line becomes large enough, the fraudster will make charges up to the credit line and then default on that balance, driving an increase in the issuer's credit losses.

No single technique can stop the use of synthetic identity and the brief does not intend to recommend any one method or combination of methods. The list below provides some of the most common methods to recognize and abate synthetic identity events.

- Use the Social Security Administration's electronic Consent Based Social Security Number (SSN) Verification (eCBSV) service, which validates that an individual's SSN, name, and date of birth matches Social Security records, or indicates if the SSN holder is deceased.
- Correlate Social Security numbers, mailing addresses, IP addresses, and other information. Many identities with different names using the same physical mailing address can be a red flag.
- Analyze personally identifiable information (PII) and other data provided at account creation. Recently created email addresses or social media accounts may be higher risk.
- Verify bank statements for longer periods (longer than only a few years back).
  - The longer a merchant is in business with aged PII credentials generally reduces synthetic ID risk at account opening; many/most synthetic IDs do not have a very long transaction history.
- Use identity validation services.
- Verify the Employer Identification Number (EIN).
- Request and verify payment processing statements from different financial institutions.
- Look for large amounts of unsecured debt.
- Look for a high number of recent credit inquiries.
- Look for a Social Security number that matches different profiles and different names.
- Search for identical digital footprints, e.g. computer IP address, used for financial transactions for many different identities.
- Check for too many rejected applications for credit in the identity credit history.
- Carefully monitor users with an excessively high number of authorized credit card users with different last names and/or addresses. Synthetic IDs tend to incubate on established credit lines to establish (credit) bureau history before applying for credit of their own.
- Check for a mismatch in the person's age, duration of credit history, and SSN age.

- Detect anomalies using artificial intelligence, machine learning and/or behavioral biometrics to find potentially fraudulent activity. These tools can provide alerts on abnormal behavior patterns. Examples include the following:
    - Age anomalies: A suspected synthetic identity may purport to be 85 years old but types much faster than expected. However, an alert of this type could be a false alarm since the 85-year-old may have had a younger person entering information.
    - Name matching: Match the name on the loan account with the name of the person paying. Money may be coming from illegal sources where someone is cashing out a synthetic identity.
    - Expert data entry: Look for evidence of an expert user who rapidly switches between and completes fields, perhaps repeatedly pasting data. A synthetic identity criminal would be extremely familiar with the required fields, making this a sign of suspicious behavior.
        - A "real" person would not typically paste their own name but would probably use a browser auto-fill tool or "hunt and peck" to complete a form.
        - Additionally, a real person might have to spend several seconds or minutes looking up an unfamiliar piece of data, such as an airline loyalty number, while a fraudster would rapidly paste it in.
    - Behavioral biometrics: Develop profiles for valid customers; after a handful of sessions, the profile will contain characteristics such as typing speed, mouse usage, cursor/tab usage, pasting, touchscreen usage patterns, and angle of holding a device. If the purported user initiates a new session with different characteristics, account takeover fraud is likely.
        - While scams, strictly speaking, are different from synthetic identity, behavioral biometrics may be used to detect scams. For example, if the valid customer is being guided to enter data by a trickster/fraudster, the customer will likely be hesitant, worried, unsure, or somewhat suspicious of a transaction. This new behavior will result in out-of-pattern behavioral biometrics.

The test-and-learn approach is recommended for applying the different methods described. In each iteration of test and learn, gather data, analyze the results, and use the insights gained from the data to refine and improve the synthetic ID rules before applying a final solution.

Resources

- NACHA: Account Validation: A Tool for Businesses to Improve ACH Transactions (login required)
- Bank Account Owner Verification | Account Validation | Finicity
- Synthetic Identity Fraud Mitigation Toolkit | The Federal Reserve

About this Brief

The U.S Payments Forum Payments Fraud Working Committee is publishing an ongoing series of short summaries and primers on trending topics related to fraud in the industry. Synthetic identity fraud is the third publication in this series. Additional resources can be found on the U.S. Payments Forum website.