IDENTIFYING A SYNTHETIC AT ACCOUNT OPENING

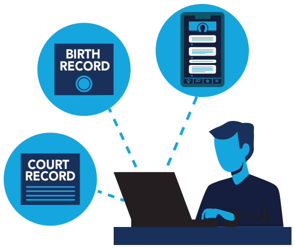
IMPORTANCE OF EARLY DETECTION

Synthetic identity fraud can cause losses, increase operational costs and exacerbate both reputational and money laundering risks. To help mitigate these risks, financial institutions can choose to employ strong customer onboarding requirements and effective data strategies. One of the best mitigation strategies is to identify a synthetic identity before the relationship is opened. If synthetic identities are never on your books, there is minimal chance for a negative impact.

After the customer relationship has been established, it becomes more challenging to detect a synthetic identity based on transaction activity, which often mimics that of a legitimate customer. For example, a credit card relationship most likely will appear to be normal as occasional charges are made and the balance is paid down on time. The more tools you can utilize in conjunction with one another, the more likely you are to identify the synthetic identity before the account is opened.

TOOLS TO AID IN DETECTION

Identity proofing is the process of verifying a person's identity – confirming they are who they say they are. It examines the data elements associated with the identity to help determine if the identity itself is legitimate. Using multiple methods of verification can help further validate the legitimacy of the presented data. It also is important to go beyond verification of basic identity elements, such as name, date of birth, Social Security number and address. The more data points you can string together, the easier it is to verify the identity. Proof of life can be supported further by cross-referencing identity elements with alternative data sources.



Third-Party Data

Leveraging third-party data as part of your identity verification process can be a powerful tool. Real people can be validated using the histories of their everyday lives. The more sources used to validate this information, the more likely it is that you are dealing with a real person. The data attributes that belong to a real identity are generally consistent across different sources, whereas a synthetic identity often has inconsistent data records. For example, an applicant might have a bank account, student loan data from years ago, a current address, previous addresses, a current phone number and email address. These data attributes should be consistent across verified data sources. By assessing the depth and consistency of existing information about applicants using third-party data, institutions can assess the probability of the applicant being real or synthetic.

IDENTIFYING A SYNTHETIC AT ACCOUNT OPENING

Public Records

Data available through public records can help validate an identity. For example, researching an applicant's address in public records may indicate it is also linked to other profiles or show it's an office building rather than a private residence. Being able to triangulate the customer-provided data to publicly available data can help identify potential red flags. Some public records to consider include:

- Property deed and tax records
- Voter registration
- Criminal, arrest and court records
- Birth/death certificates
- Marriage/divorce records
- Commercial licenses

Data Comparison

Comparing data presented on the application to known "bad data" can help identify potential synthetic identities. Fraudsters often reuse data elements when creating a synthetic identity, mixing and matching Social Security numbers, names, dates of birth and addresses. You can potentially identify the synthetic identity by comparing its application information to a database of information associated with known bad actors.

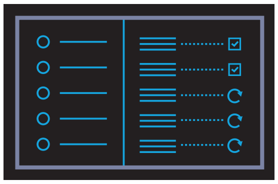
Applicant data also can be compared to other open accounts to see if there is data overlap. For example, if the Social Security number submitted on the application already exists within your portfolio, but is associated with a different name, that should raise a red flag.

If the application data is collected digitally, there is also an opportunity to utilize data attributes (such as device information and IP address) to determine if those same data elements were used to submit applications in other names or access accounts associated with other identities.

IDENTIFYING A SYNTHETIC AT ACCOUNT OPENING

eCBSV

To help control fraud related to Social Security numbers, the Social Security Administration (SSA) introduced the ***electronic Consent Based Social Security Number Verification*** (eCBSV) service. This is an enhanced version of the SSA's traditional CBSV, which enables paid subscribers to verify that a name, date of birth and Social Security number matches the SSA's records. Previously, the SSA required the written consent of the applicant via a physically signed document (also known as a wet signature) to disclose the SSN verification information. This was a manual process that could take days or weeks to complete. Under the new electronic version of this service, applicants can submit their consents electronically in real time. The eCBSV service launched in June 2020. As of February 2022, this service has been expanded to all permitted entities who asked to enroll, with enrollment open indefinitely. This service will help organizations to more quickly verify the information provided on the application is valid. Expeditiously validating key identity elements of a customer when considering the application will enable financial institutions to better identify potential synthetic identities.



Technology

Many vendor solutions offer robust platforms to help identify a potential synthetic identity as part of the account opening process flow. These vendors utilize data from multiple sources, including industry consortium data, to perform data analytics on the applicant and quickly determine the likelihood that an applicant is a synthetic identity.

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.