IDENTIFYING EXISTING SYNTHETICS WITHIN A PORTFOLIO

Synthetic identities often appear to be legitimate customers. Fraudsters use them to open accounts that look and act the same as any other customer relationship, making it challenging to detect them. From a credit perspective, synthetics often build payment histories to increase their available credit lines prior to default. These accounts initially appear to be normal, frequently conducting small-dollar purchases and payments. There may not be any indications of suspicious activity or behavior prior to maxing out the line of credit with no intent to repay the amount. Much the same from a demand deposit account (DDA) perspective, account activity appears to be normal, with funds flowing in and out prior to the fraudulent transactions. By routinely monitoring accounts, financial institutions can help avoid reputational impact and losses from fraudulent activity related to synthetic identities.

Reviews vary by financial institution but may include a step-by-step automated or manual process to gather suspicious information based on risk indicators and escalate accounts for further manual review. The detection process may run continuously through multiple checkpoints and with an in-depth analysis of available data, including third-party information, to produce results for review. Monitoring also depends on the ability to compare account data to other data sources, such as public records, digital data information and internal customer data.

A HIGH-LEVEL APPROACH TO DETECTION OF SYNTHETICS SHOULD CONSIDER THE FOLLOWING:

1. **Look at products across the enterprise.**
    a. Data reviews can span checking and savings accounts, credit cards, loans, lines of credit (HELOC) and merchant services.

2. **Compare account holder details to other existing accounts.**
    a. If data matches, a relationship between accounts might be evident, such as products for the same person/identity, for members of the same family, or the same submitting location (device ID and IP address).

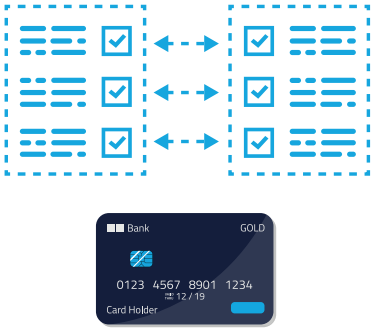
3. **Review account transaction details, including account contact changes, purchases and payment activity, new authorized users, account holder requests for credit increases and approved credit increases.**
    a. Verify that the account holder's IP address location (if available through online interactions) matches his or her mailing address/physical location; a mismatch could be a potential red flag.

IDENTIFYING EXISTING SYNTHETICS WITHIN A PORTFOLIO

4. Leverage alternative or third-party data, such as public records and digital data, to compare to the account holder information for name, mailing address, birthdate, phone number, email address and Social Security number.

a. Legitimate identities typically have a digital footprint that includes previous addresses, phone numbers and social media accounts.

COMPARE ACCOUNT HOLDER DATA TO OTHER ACCOUNTS TO IDENTIFY COMMON DATA



One detection approach is to compare account holder data to other existing accounts to find if the data matches. This approach is effective because criminals often re-use data, use data for a legitimate person or access accounts from a common device or IP address.

- Search by name, mailing address, phone number, email address, birthdate and Social Security number.
  - Compare contact information or other data that was updated after account opening.
- If authorized users were added to the account, search by their names and data.
- Identify the device ID and IP address (if available) used to access the account and cross-reference to find potentially linked accounts.
- Compare account holder data to the data tied to previously identified synthetic identity fraud losses to help identify additional potential suspicious accounts.
- Review account activity, such as payments or incoming credits, in comparison to other accounts.
  - Example: Were payments to the credit card made from the same external account remitting payments to other credit cards with different cardholder names?

Accounts with common data elements could indicate a higher risk of additional fraudulent activity.

IDENTIFYING EXISTING SYNTHETICS WITHIN A PORTFOLIO

REVIEW ACCOUNT TRANSACTION DETAILS FOR POTENTIAL DETECTION CRITERIA

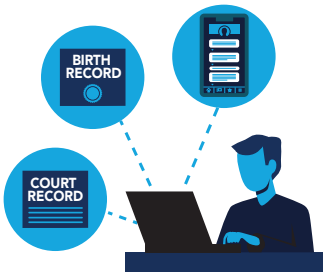
Building a profile to detect synthetic identities is typically based on confirmed or suspected fraud cases and the event details. Credit report information and the history of synthetic identity fraud cases can be used to create and refine detection rules.

NUMEROUS FACTORS CAN BE USED AS A BASIS FOR MONITORING, MANY OF WHICH MAY INDICATE INCREASED FRAUD RISK:

- Limited, brief or no credit history; history was based on secured credit lines.
- Applicant information from credit history, including authorized users' names and data.
- Authorized users were added to the account.
- Transaction activity volume and type, including merchants and types of transactions (example: big box retailers, grocery or drugstore chains or small shops).
- Payment method and source (e.g., card payments made from an external account at another financial institution or from an internal account, and any related activity for those accounts).
- Credit increases and dollar amount of the available credit line.
- Contact with the account holder during the relationship and the channel used.
- Request for credit increases and timing.
- Fraudulent check deposits.
- Claims submitted by the account holder.
- Other products opened for the relationship.
- Alternative data used to validate the applicant's identity at enrollment and the information used.

IDENTIFYING EXISTING SYNTHETICS WITHIN A PORTFOLIO

LEVERAGE ALTERNATIVE OR THIRD-PARTY DATA TO ASSIST DETECTION



Alternative or third-party data, such as public records and internet profiles, may be used to support the detection of synthetic identities within a portfolio. If this review was conducted at onboarding, check if the initial review was satisfactory and whether any account holder data has changed since that review. The use of a vendor application to access consolidated alternative or third-party data may have value for these searches.

PUBLIC RECORDS

Institutions may find value in comparing the application data to third-party data to detect any discrepancies. Data available through public records may be a useful resource to conduct a further review. A search of the mailing address provided could show other residents at the same address to determine if and how they are linked to the applicant. A search may show that the address is an office building and not residential, or no building exists at that address. The applicant's name and address may match to public records available online, such as:

- Landline phone number
- Property deed and property tax records
- Voter registration and voting records
- Criminal, arrest and court records
- Birth certificates
- Death certificates
- Marriage and divorce records
- Commercial licenses

Access to some records, such as birth and death certificates, may be restricted depending on state laws, although the information could be available through other public records.

IDENTIFYING EXISTING SYNTHETICS WITHIN A PORTFOLIO

INTERNET PROFILES

Detection strategies to find synthetic identity fraud within a portfolio may use customers' online presence, although it is important to recognize that fraudsters may create social media accounts to support synthetic identities and avoid detection. Social media accounts with frequent posts and activity, and that are connected to other profiles, are more likely to represent a real person. An online profile should be consistent with the customer's age and address, which can be partially validated with a resume posted to a career site or references to local events. A social media account linked to family members would help validate the identity. Also, changes to the account holder's online presence after onboarding could indicate risk, such as multiple deleted social media accounts. Online records for previous phone numbers and mailing addresses can be used as part of risk scoring. A digital footprint may not exist for every person, a point that can be evaluated as part of the risk review.

CONCLUSION

Financial institutions that can effectively detect synthetic identities within their portfolios can reduce fraud losses and reputational risk. There is no easily defined set of characteristics or behaviors to detect synthetic identities. A fraudster may deposit a bad check and deplete the account within a week, attempt a "bust out" within two years or less of account opening, or cultivate many synthetic identities for long-term use and to maximize the overall payout. The most effective detection strategies use multiple data sources and tools with varied approaches and refine the fraud detection rules based on an evolving fraud detection profile. Machine learning can enhance detection by processing large quantities of data. The ability to confirm a Social Security number matches the customer's name and date of birth gives financial institutions another identity validation tool. When synthetic identities are detected, the information and lessons learned from each event can be used to improve detection processes.