HOW TO SPOT A SYNTHETIC

While synthetic identity fraud is reported to be one of the fastest-growing types of financial crime, many organizations often struggle to identify it.

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.

Identities used in this type of fraud are created to look and act like a legitimate person or entity. This makes it difficult to detect these identities, as they may look valid upon first review, often passing initial identity verification checks and appearing to be creditworthy customers.

It is important to look deeper – both within the individual account as well as across accounts – to determine if the information associated with the identity makes sense. Below are some key characteristics to look for when detecting potential synthetic identity fraud.

WITHIN A CUSTOMER'S APPLICATION OR ACCOUNT

Several indicators within a customer's application or existing account could suggest a potential synthetic identity. As a general rule of thumb, any inconsistency in the customer's credit profile warrants additional investigation. While it may take some time to review the application or account in this context, early detection of a synthetic can help you potentially avoid significant losses in the future. Below are some of the more common characteristics of a synthetic identity:

- **A large amount of unsecured debt.** Consider the types of credit on the applicant's credit file, paying close attention to the amount of unsecured and secured credit.

  Fraudsters utilizing synthetic identities tend to focus on acquiring unsecured credit, such as credit cards, rather than secured credit, such as home mortgages, that would require much more validation of financial records and identity documentation. This does not mean that synthetic identities are not used in mortgage applications or other secured types of credit. It is just more common for synthetic identities to acquire unsecured lines of credit. A credit profile consisting of only credit cards and lacking other types of credit one may expect to see (such as an auto loan, student loans or a mortgage) may warrant additional review to validate the identity.

HOW TO SPOT A SYNTHETIC

- **High number of recent credit inquiries.** Review the credit profile for recent activity, with a close eye on credit inquiries.

  During the credit build phase of creating a synthetic identity, fraudsters will submit a high number of credit applications until one or multiple applications are eventually approved. Multiple recent credit inquiries can be indicative of this activity and therefore, of synthetic identity fraud.

- **Mismatch of anticipated and actual credit history.** One can usually estimate the duration of a credit history based on the account holder's age. If the consumer file depth does not match the anticipated credit history duration, it may warrant additional review.

  For example, it would be reasonable to expect a consumer born 30 years ago would have approximately 10 years of credit history beginning around the age of 18. If the consumer has only a few months of history, this would be considered a mismatch between the expected and actual credit history.

- **Inflation of credit file depth.** Review how the consumer built the credit history and whether the duration is solely under his or her name or linked to others. To build credit histories quickly, fraudsters will "borrow" the good credit history of established accounts by adding themselves as authorized users to well-established accounts, often with high credit lines. This process, termed "piggybacking," allows the synthetic identity to inherit the primary accountholder's strong repayment history, inflating both the duration and standing of the fraudster's account.

- **Suspicious mailing address listed.** Pay close attention to both the format and location of the address listed on an application.

  Fraudsters can use P.O. boxes to increase the difficulty of tracking them down if caught. Additionally, addresses that are close to international airports can be a red flag, as fraudsters find it convenient to stay near airports for the purpose of transporting goods as part of their fraudulent acts.

HOW TO SPOT A SYNTHETIC

- **Recently issued contact information.** Review how long the customer's contact information (e.g., email address or mobile phone number) has been registered or in existence.

  If contact information has been recently issued (within the past 6 to 12 months), this suggests someone may be using a synthetic identity, as most people already have an existing email address, phone number, etc. If all the contact information was issued recently, this warrants additional review of the applicant's identity.

ACROSS YOUR PORTFOLIO (OR MULTIPLE CUSTOMER ACCOUNTS)

While there are some synthetic identity characteristics you can identify within an account, at times, you also must look across accounts. Sometimes, something may not seem suspicious by itself, but certain red flags may begin to appear if you look at the information in aggregate. The biggest indicator is similar customer information across accounts. Specifically, you should look for accounts with:

- **Similar or matching contact information.** Review both your applications and accounts for similar contact information. Fraudsters tend to reuse account information, particularly contact information, for the creation of multiple synthetic identities. Common data elements to review include email address, mailing address and telephone number. If you find contact information is reused across multiple accounts, it may warrant additional review of the accounts and specifically, the associated customer identities.

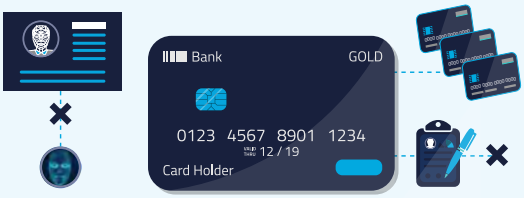
- **Matching Social Security numbers (SSNs).** Ensure your accounts have distinct SSNs for each of your customers. While likely not occurring as frequently as using the same contact information across synthetics, fraudsters can reuse an SSN. When doing so, the fraudster pairs the SSN with different names, dates of birth, etc. to create multiple synthetic identities.

- **Digital footprint.** If the same digital footprint is used to submit applications for multiple people, this could indicate fraudulent behavior, as this information is usually tied to only one person or household.

HOW TO SPOT A SYNTHETIC

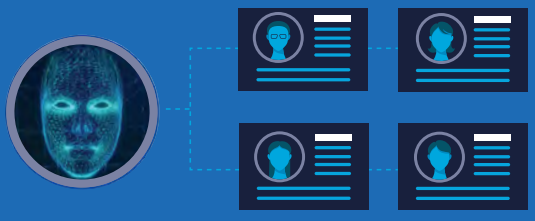
SOCIAL SECURITY NUMBER INFORMATION MISMATCH

- Multiple identities tied to the same Social Security number
- Social Security number issued after 2011, but customer date of birth is before this date (e.g., 1995)



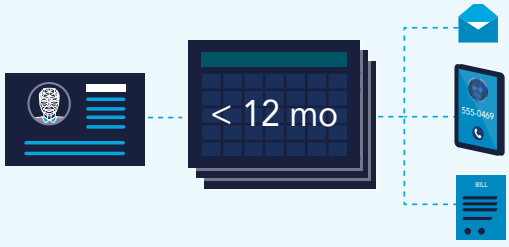
INCONSISTENCIES IN CREDIT PROFILE INFORMATION

- Anticipated credit file depth does not match customer information provided. For example, the customer lists a date of birth as 01/01/1980, but the credit file is less than 12 months old
- Use of secured lines to quickly establish credit, with no other tradelines
- High number of authorized user accounts with few to no individual liability accounts



CUSTOMER ACCOUNT INFORMATION LINKS TO OTHER, ALREADY ESTABLISHED ACCOUNTS BELONGING TO OTHER CUSTOMERS

- Same address, phone number or digital footprint information (such as IP address)



VELOCITY CHECKS AGAINST THE CUSTOMER INFORMATION PROVIDED: WAS THE CUSTOMER CONTACT INFORMATION RECENTLY ISSUED?

- Email address, phone number or other contact information that was issued less than 12 months ago may be indicative of a synthetic identity

HOW TO SPOT A SYNTHETIC

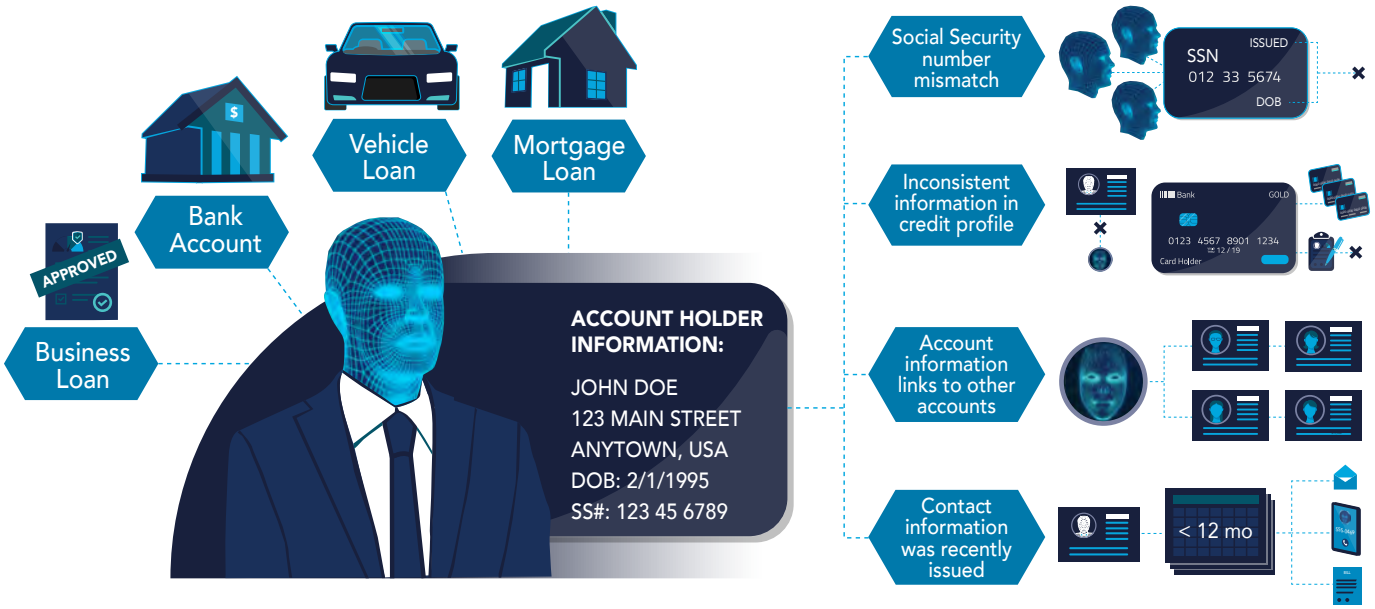
BE SURE TO LOOK AT MULTIPLE CHARACTERISTICS

It is important to look at multiple characteristics when trying to detect synthetic identities. This can be achieved by aggregating various data sets and sources to identify and detect anomalies more effectively. The danger of focusing solely on one characteristic to detect synthetic identity fraud is that it could lead to false positives, with an account appearing to be a synthetic when there is an explanation for that single characteristic. For example, looking only at the length of a credit history could unnecessarily disadvantage or deny credit to certain legitimate customers who had a valid reason for recently building their credit history.

In addition, looking at only one characteristic could make it more difficult to detect the synthetic identity. One aspect of the application or account may seem appropriate or legitimate, while in combination with other factors, it would suggest additional investigation is warranted.

In other words, there is not typically a single indicator that signifies a synthetic identity. Rather, it is the combination of multiple characteristics that can help suggest a potential synthetic that warrants additional review. Both awareness and review of these characteristics are critical for organizations to begin identifying synthetic identity fraud.

HOW TO SPOT A SYNTHETIC IDENTITY



HOW TO SPOT A SYNTHETIC

TAKE ACTION

Begin looking for these characteristics at your organization, both in new customer applications and across your existing portfolio. By doing so, you may be able to spot a synthetic identity before your organization suffers significant financial loss.

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.