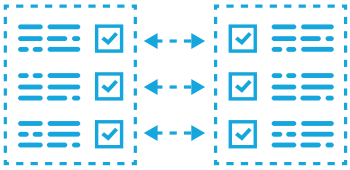
IDENTIFYING EXISTING SYNTHETICS POST-LOSS

Synthetic identities often appear to be legitimate account holders. From a credit perspective, these accounts appear to be normal, often with small dollar purchases and payments. There may be no indication of suspicious activity or behavior prior to the bust out. From a demand deposit account (DDA) perspective, there may be no indication of suspicious activity or behavior prior to intentionally overdrawing the account.

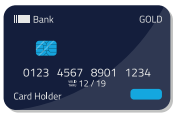
To mitigate losses, accurately report fraud and prevent future synthetic activity, when possible, financial institutions can review all credit losses to identify if synthetic identities were used. This review should include a data search to identify related accounts, respond/report and collect information about the characteristics of synthetic identities for use in future detection.

PART 1: MITIGATION – DATA ANALYSIS



Data analysis is an important tool to mitigate additional losses, as it can help identify related accounts for review.

Compare account holder data to other open accounts to identify common data



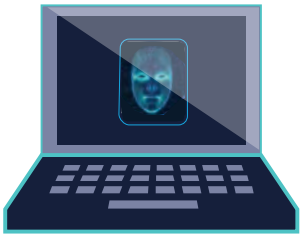
- Search by name, mailing address, phone number, email address, birthdate and Social Security number
- Compare with any applicant data that was updated after account opening, such as contact information
- Search names and data for authorized users added to the account after opening
- Identify the device ID and IP address (if available) used to access the account and cross-reference to find potentially linked accounts
- Compare the data to previously identified synthetic identity fraud losses to confirm linkage to known bad data
- Review account activity, such as payments or incoming credits, for comparison to other accounts
  - Example: Were credit card payments made from the same external account that remitted payments for other credit accounts? Were payments to the account made from the same external account remitting payments to other credit cards with different cardholder names?

Any accounts with common data elements could indicate fraudulent activity.

IDENTIFYING EXISTING SYNTHETICS POST-LOSS

PART 2: CHARACTERISTICS OF A SYNTHETIC IDENTITY

After the cross-reference of account and account holder data has been completed, the characteristics and activity of the account can be examined to help mitigate additional losses and further understand vulnerabilities. The below questions should be considered when reviewing each suspected synthetic fraud event to build the organization's synthetic fraud profiles and facilitate future fraud detection.



CREDIT REVIEW

- How long was the account open? Was the account open for less than two years, but enough time to increase available credit limits?
- Were secured credit lines initially used to build credit?
- Were authorized users added to the account?
- Was the bust out for the maximum available amount of credit?
- What information provided on the credit history at application may have indicated a synthetic identity?
- Was the payment activity minimal?
- When were credit increases made?
- What were the requirements to qualify for a credit increase and do these thresholds seem appropriate?
- How soon after the previous credit increase did the bust out occur?
- Was there any contact with the account holder during the relationship and if so, through what channels?
- Did the account holder request a credit increase?
- For credit card charges, did transactions occur at known, reputable vendors? Is further payment activity review needed?
- Was there any contact with the account holder after the bust out?
- Were any claims submitted by the account holder while the account was open?
- Did the account holder open other financial services products?
- Was the applicant's identity verified using alternative data, such as public records? What information was used? What was the result of the validation?

IDENTIFYING EXISTING SYNTHETICS POST-LOSS

DDA REVIEW

- How long was the account open?
- What documents were used to validate the identity at account opening (e.g., driver's license, passport)?
- What products were attached to the account, including checks, ATM/debit card, online banking/bill pay, person-to-person (P2P) payments, overdraft protection?
- What information provided on the application may have indicated a synthetic identity?
- Was the transaction activity minimal?
- What were the overdraft thresholds, and should these thresholds be reviewed?
- Was there any contact with the account holder during the relationship and if so, through what channels?
- Did any suspicious transactions occur prior to the overdraft?
- Was there any contact with the account holder after the overdraft?
- Were any claims submitted by the account holder while the account was open?
- Were any other accounts opened for the relationship?
- Was alternative data used to validate the applicant's identity and what information was used? If so, what was the result of the validation?
- How was the account overdrawn?
  - Through a check that was deposited, funds withdrawn and then check was returned
  - Checks written without funds to cover amounts
  - Cash withdrawals or debit card transactions
- Did the name and date of birth match the Social Security number on record with the Social Security Administration?

These answers can be used to find potential onboarding and ongoing account monitoring gaps to improve detection of synthetic identities. Risk indicators can be used more effectively to prompt review of existing accounts with the goal of avoiding future payment defaults.

IDENTIFYING EXISTING SYNTHETICS POST-LOSS

PART 3: DETECT AND REPORT FRAUD

The review of account data and characteristics can help determine if synthetic identity fraud may be present. If the loss was referred for collections, confirming if a real person was located for the account can help identify a synthetic. Reviewing the credit history data provided on the application to identify risk indicators can help mitigate similar risks in the future. Inconsistencies in the credit file depth and the customer age and credit history could benefit future detection. These factors often can help indicate synthetic identity fraud.

Lessons learned from each review can improve detection through machine learning and negative lists populated with known fraudulent data.

Notifying the credit bureaus is important to help mitigate the risk of these identities being re-used in the future. Reporting synthetic identity fraud losses is critical to support law enforcement investigations and fraud data tracking. When synthetic identity fraud is properly classified and reported, the full scope of the issue and impact on financial institutions becomes clearer. The expanded fraud data can aid in business case development for improved prevention, detection and reporting functions.

CONCLUSION

Synthetic identity fraud can be difficult to detect, as synthetics often initially imitate normal consumer activity. Reviewing both credit and overdraft losses can offer an opportunity to learn if the loss was caused by fraud and whether the fraud involved a synthetic identity. In addition, some synthetic identity fraud attempts are more complex, involving merchants or the creation of small businesses. Analysis to compare potential synthetic identity activity to existing account data in the portfolio is a good resource for detection. Completing the review and response actions to mitigate future fraud events is beneficial to financial institutions and the industry.