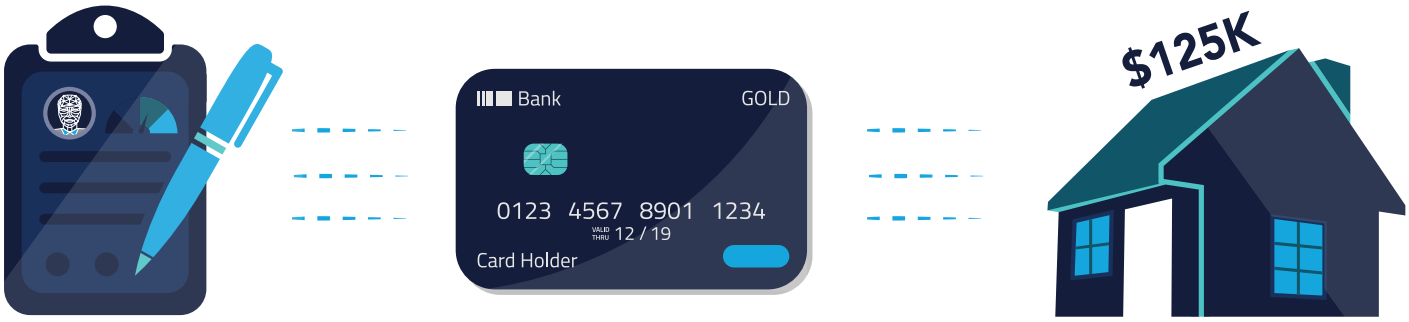
WHAT'S HIDING IN YOUR PORTFOLIO

Synthetic identity fraud is reported to be one of the fastest-growing types of financial crime. However, many organizations are not aware it exists, and therefore, are not looking for it. Even organizations that are familiar with synthetic identity fraud often struggle to identify and mitigate it. For these reasons, it is important to take another look at the topic as this type of fraud continues to seriously impact the financial services industry.

SYNTHETIC IDENTITIES OFTEN EVADE DETECTION

Unlike other types of fraud, payment behavior is not always indicative of synthetic identity fraud. Once a synthetic identity enters a portfolio, its account activity often mimics that of a normal – and even upstanding – customer, with timely and in-full payment history. At first glance, a loss generated by a synthetic identity generally does not show indicators that fraud occurred, but rather, the customer appears to be unable to pay off the credit balance.

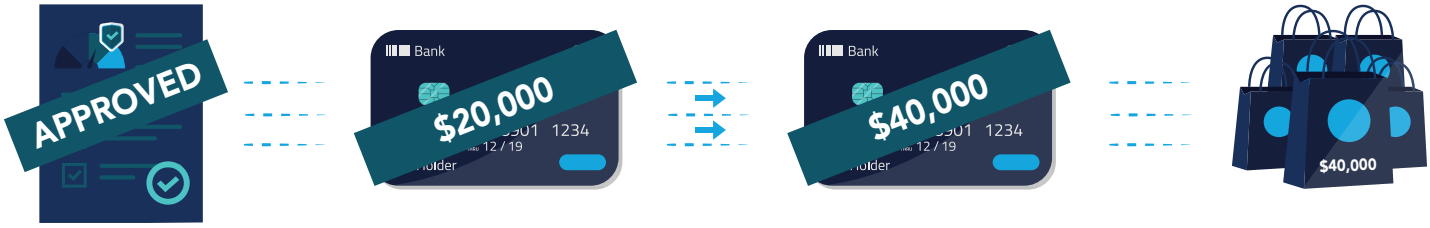
Consider the following example of synthetic identity fraud:



An application for a credit card included the following information:

- *FICO score of 750*
- *Oldest tradeline was 20 years old, but was an authorized user tradeline*
- *The only types of tradelines reported on the applicant's credit file were unsecured lines of credit*
- *The applicant's credit file showed eight new inquiries for credit*
- *Reported Adjusted Gross Income (AGI) was $125,000*

WHAT'S HIDING IN YOUR PORTFOLIO



Upon review, the application was approved, and a credit line of $20,000 was issued. For three years, the customer never missed a payment, and therefore, the credit line doubled. Suddenly, the $40,000 credit line was maxed out and not repaid.

-$40,000 CREDIT LOSS

As there were no indicators of fraud, the $40,000 was charged off as a credit loss by the financial institution and never reported as fraud.

RECOGNIZING THE LIFE SPAN OF A SYNTHETIC

It is important that these accounts be investigated and identified as fraudulent. When synthetic identity fraud is written off as a credit loss, these accounts are presumed to belong to real people who simply defaulted on their credit. As a result, fraudsters can reuse the synthetic or repurpose the associated personally identifiable information (PII) to create new synthetic identities affecting your organization. Data points that are known to be associated with synthetic identity fraud (e.g., name, Social Security number, email address, phone number) can be used to flag future account openings utilizing the same criteria. In addition, an organization can assess other relationships in the portfolio to see if they are using some of the same known bad information.

WHAT'S HIDING IN YOUR PORTFOLIO

A SYSTEMIC ISSUE: WHAT HAPPENS WHEN SYNTHETICS GO UNDETECTED, ARE CATEGORIZED INCORRECTLY OR ARE UNDERREPORTED?

While fraud losses due to synthetic identity fraud are ***estimated at $20 billion in 2020***[1], many industry experts believe this number is underreported. In part, this is due to related losses being miscategorized as credit losses, similar to the above example. The account is often never known to be fraudulent and is written off as a credit loss, so the synthetic remains undetected. In other cases, it is later discovered that a synthetic identity was in use but the loss is never recategorized as fraud.

Miscategorizing known fraudulent accounts makes it difficult to quantify the magnitude of synthetic identity fraud or know where to implement mitigation practices. Beyond learning what's hiding in your portfolio, a broad understanding of the challenges of detecting, categorizing and reporting synthetic identity fraud can help the industry address it more effectively.

LEARN MORE

What are you currently doing in your organization to look for synthetic identities?

[1] ***2021 Synthetic Identity Fraud Report***