HOW FRAUDSTERS INCREASE THEIR PAYOUTS

Synthetic identities may be extremely lucrative for fraudsters, who can use them to receive a large payout or acquire expensive goods with no intention of paying for them. While a fraudster can set up multiple synthetic identities, the same synthetic can also be used multiple times, at the same or various institutions to increase the fraudster's payout. Fraudsters identify gaps to take advantage of, and when they do, they have the synthetic identities ready to capitalize on these vulnerabilities.

CLEARING THE SYNTHETIC IDENTITY OF PAST FRAUDULENT ACTS

You may think that once a synthetic is created and used, the same synthetic cannot be used because the associated Social Security number (SSN) is now associated with a fraudulent act or a bad credit history. However, the fraudster can pose as the victim in the situation and rehabilitate the synthetic identity.

- **Identity theft claim:** The fraudster may report his or her identity was stolen and ask that all negative credit history be removed. The irony is that there was never a legitimate identity in the first place, but this fact is typically still undetected at this point. An identity theft claim allows the fraudster to "reuse" the synthetic to apply for additional credit lines and/or increase existing ones.

- **Fraudulent charges report:** The fraudster also may report individual charges or a series of charges on a line of credit as fraudulent when, in fact, these charges were made by the fraudster. By doing so, this eliminates the synthetic identity's responsibility for paying off the charges. Additionally, if the unpaid charges affected the synthetic's credit score in any way, reporting the charges as fraudulent may help repair or improve the score. In turn, this would benefit the creditworthiness of the synthetic identity and enable the fraudster to secure additional credit.

  Based on the ***Fair Credit Reporting Act***, if a consumer disputes credit information directly with a credit reporting agency (CRA), the CRA then must contact the financial institution with a response on that case, which is required within 72 hours. This is vastly shorter than if a dispute is reported to the lender, in which the financial institution has 30 days to conduct an investigation. Fraudsters take advantage of this and contact the CRA directly to report disputed charges. This is done in hopes of a quick resolution (resulting in the charges being wiped from the account) versus a prolonged investigation.

HOW FRAUDSTERS INCREASE THEIR PAYOUTS

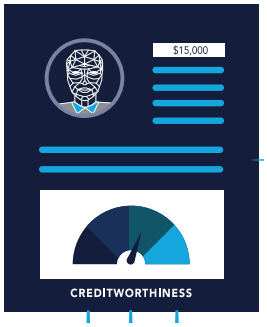
LEVERAGING OPERATIONAL PROCESSES TO INCREASE AVAILABLE FUNDS TO THE SYNTHETIC IDENTITY

In some cases, a fraudster will set out to double, sometimes triple, a credit line by taking advantage of lags in payment processes.

Note: These tactics are not specific to synthetic identity fraud. However, synthetics often are used in conjunction with these types of fraud.

Some payment types experience delays in fully reconciling and settling accounts. This leads to a discrepancy, or "lag," between account activities and the current account balance. Fraudsters take advantage of this lag to manipulate the perceived status and currency of a credit line, striking at just the right moment to max out that credit line more than once.

Consider this example:



An initial line of credit of $15,000 is opened using a synthetic identity.

The fraudster who created the identity first establishes a strong payment history on the account, paying the balance in full and on time each month.

HOW FRAUDSTERS INCREASE THEIR PAYOUTS

He or she does this for approximately a year before making a total of $15,000 in purchases in one month.

He or she pays the balance with an online check and within a day, the full line of credit is available once more,

so he or she makes additional purchases totaling $15,000.

However, the check used to pay the balance has not yet cleared and only does so two days later – when the lending institution discovers there is now no money in the account.

As a result, the fraudster has been able to utilize $30,000 – or twice the amount of the original credit line.

HOW FRAUDSTERS INCREASE THEIR PAYOUTS

MAXIMIZING REACH OF SYNTHETIC IDENTITY THROUGH MASS CREATION OR COLLABORATION WITH OTHER FRAUDSTERS

In looking at the various ways a single synthetic identity can be used and the associated payouts, it is important to recognize that many fraudsters don't stop at creating one synthetic identity. It is very common for a fraudster to create and manage multiple synthetics at any given time.

- **Creation of multiple synthetics:** When a fraudster obtains personally identifiable information (PII), they often receive multiple PII elements (as opposed to just one, or for one individual). This creates an opportunity for the fraudster to create multiple synthetics based on one data set. For example, a fraudster often will use a list of compromised, unique SSNs purchased on the dark web, but pair them with the same name and contact information. This enables the fraudster to open several accounts under different identities, but with a lighter lift in terms of securing additional information to create the identities.

- **Fraudster collaboration:** Fraudsters openly share information with one another and will collaborate on fraudulent events to maximize the impact of their actions and individual payouts. They often work together to create multiple identities, position them for use and make as many purchases as possible – all the while, meticulously coordinating the activities to avoid detection.

TAKE ACTION

Based on the various opportunities fraudsters have to capitalize on one synthetic identity, let alone multiple ones, it is imperative that we all work together to better detect, and protect against, this type of fraud.