USE CASE: OTHER CRIMINAL ACTIVITY

OVERVIEW

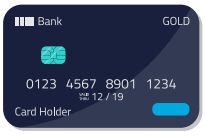
No matter how synthetic identities are used in fraud, this type of criminal activity is illegal. In addition, it can have significant implications for individuals whose information was used in the synthetic creation.

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.

Synthetics can be used in many ways to commit fraud. Some are for very specific outcomes, such as:

- **Fraud for living –** This occurs when a synthetic identity is used to apply for employment or services such as utilities, housing or bank accounts. This is done because an individual is unwilling or unable to do so with his/her own PII elements. Typically, the individual has no intent to default on payment, but rather, needs the new identity to establish or secure employment or services.

- **Credit repair –** To appear creditworthy, an individual creates a synthetic identity and begins using it to build a more positive credit history and/or obtain additional purchasing power.



- **Payment default scheme –** A common use of synthetic identities is to obtain goods, cash or services with no intent to repay over a period of time. This could take the form of a large, one-time purchase or a series of purchases that often total a substantial amount.

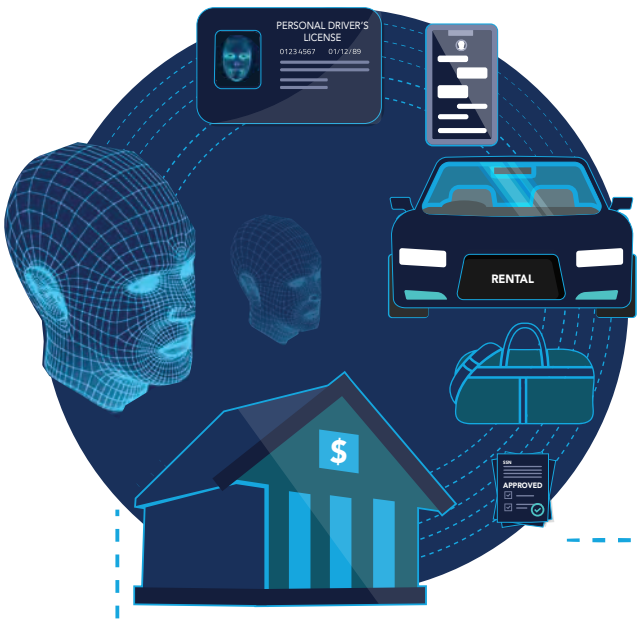
USE CASE: OTHER CRIMINAL ACTIVITY

In addition to fraud for living, credit repair and payment default scheme, there are many other ways synthetics can be used to facilitate a means to an end, often as part of another illegal act. These illegal acts can include:

- Avoiding legal responsibilities (e.g., paying child support)
- Conducting money laundering, including acting as a money mule
- Defrauding insurance companies to receive payouts or services
- Facilitating human and/or narcotics trafficking
- Organizing and financing terrorist attacks

***According to a study conducted by the Center for Identity Management and Information Protection**, criminals perpetrate synthetic identity fraud as a way to hide or abscond from authorities. Furthermore, creating synthetic identities enables offenders to take on an identity, which does not link to their tarnished identity and does not completely overlap with a different, real person's identity (the signature of identity theft).*

Any of these activities can be conducted by a wide variety of criminals, ranging from individuals to transnational organized crime groups. These activities generally, but not always, include the transfer of funds from illicit sources through the payment system using the cover of synthetic identities to evade detection of the related illegal acts.



USE CASE: DRUG SMUGGLER EVADED AUTHORITIES

A criminal in Denver, Colorado faced charges related to drug smuggling and other crimes. He was apprehended and immediately imprisoned, then posted bail before his trial. The felony charges carry a minimum jail sentence of 15 years. Recognizing his guilt and the likelihood of an unfavorable sentence in the upcoming trial, he proceeded to enact a plan to disappear.

He decided to create a synthetic identity and then leave town.

USE CASE: OTHER CRIMINAL ACTIVITY

He developed the synthetic identity using a made-up name, his father's date of birth, a randomized nine-digit number to serve as the Social Security number (SSN), and an out-of-state address belonging to his brother.

He then proceeded to create fictitious identity documentation, including a fake driver's license to further validate his synthetic identity.

He activated a new cell phone and rented a car using the synthetic identity.

He also opened a bank account as the synthetic identity, withdrew money from all other bank accounts associated with his real identity and deposited the funds into this new account.

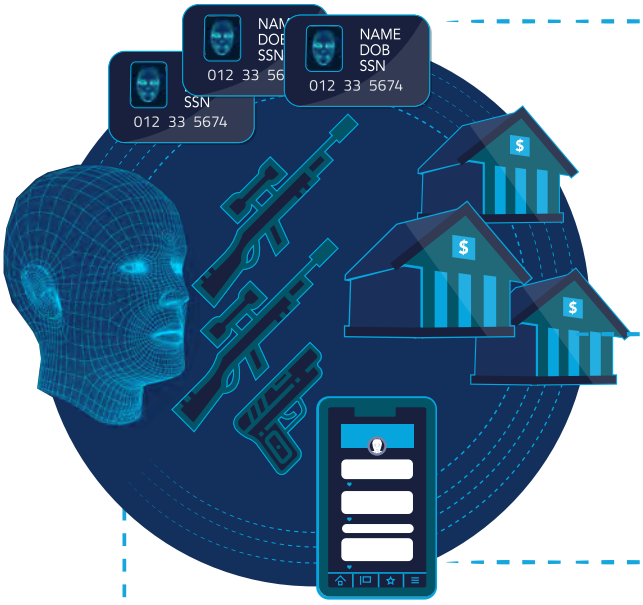
Leaving all traces of his old life behind – including his apartment, car, mobile devices, etc. – he moved across state lines undetected and settled in Minneapolis, Minnesota.

He used the funds from his newly opened bank account to open several secured credit lines, and then groomed each of those accounts to increase his creditworthiness under his new (synthetic) identity as he began his new life in Minneapolis.

USE CASE: OTHER CRIMINAL ACTIVITY

USE CASE: MONEY MULE ACCOUNTS AND ILLEGAL FIREARMS

A criminal accumulated more than $200,000 in cash proceeds from the sale of illegal firearms. He wanted to move these proceeds through the payment system to invest in additional firearms. Recognizing that large cash deposits would raise suspicion, he decided to leverage multiple synthetic identities to open various bank accounts at different financial institutions to receive the cash proceeds and fund additional purchases.



He purchased 30 SSNs off the dark web – including those belonging to children and the incarcerated. He did this to maximize the chance of avoiding detection as these SSN owners would not be likely to actively use their credit in the near term.

He created an associated identity for each of the 30 SSNs, using names from his social media connections, his legitimate address and his real mobile number.

He applied for 30 demand deposit accounts (DDAs) at different institutions online using the 30 created identities.

Each of the accounts were successfully opened.

He proceeded to deposit between $6,000 and $7,000 in each account, depositing the original $200,000 in aggregate.

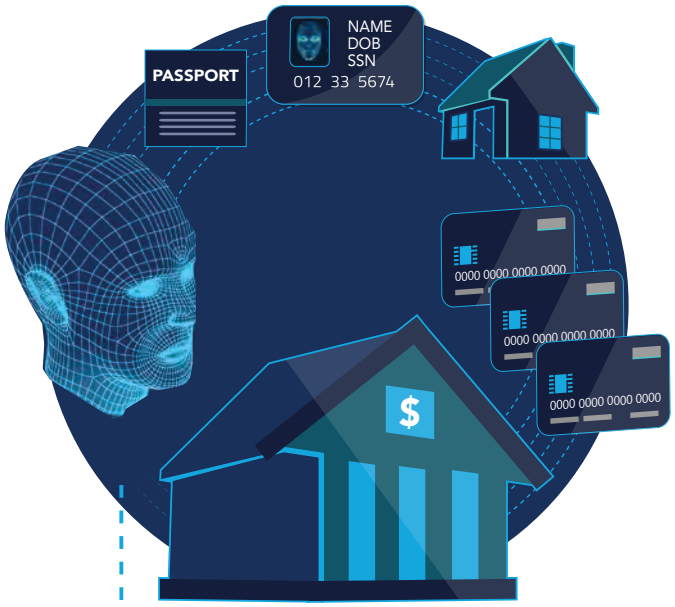
He then conducted additional purchases of firearms using funds from these new accounts.

He sold those illegal firearms on the black market, received the proceeds, and began the process all over again of creating mule accounts using synthetics to hide illegally obtained funds.

USE CASE: OTHER CRIMINAL ACTIVITY

USE CASE: FACILITATION OF TERRORIST ACTIVITIES

Since the September 11th attacks, law enforcement officials and financial institutions have prioritized investigations into terrorist financing. Terrorist organizations need to raise money, which is often accomplished through illicit or fraudulent means. Additionally, terrorist networks need to obfuscate or mask the identities of their members. Both can be accomplished with the use of synthetic identities. A terror network or terrorist financing operation can use fraudulent tactics such as ID identity theft and synthetic identity fraud to raise funds for operations. Travel expenses, mobile phones and safe houses can be procured through a synthetic identity.



Synthetic identity fraud adds an additional layer of protection for terrorist networks because the associated victims may not be aware their information is used for some time. Synthetic identities are comprised of a combination of real and fictitious identifiers or entirely fictitious identifiers. Victims may not be alerted for years that their identifiers have been compromised. Accordingly, terrorist organizations see this type of fraud as a way to circumvent government watchlists, Office of Foreign Affairs Control (OFAC) sanctions, no-fly lists and other controls. Consider the following scenario:

- *There is an exchange program that allows students and others from foreign countries to temporarily live and work in the United States.*
- *Under this program, students are issued a J-1 visa, which provides them with a valid Social Security number (SSN).*
- *The students temporarily reside in the U.S. to work. After their returns to their home countries, the students' SSNs are likely to become dormant.*

USE CASE: OTHER CRIMINAL ACTIVITY

A terrorist organization purchases personal information from the J-1visas from the Program coordinator who illegally sold the data.

SSNs from the visas are combined with new names and physical addresses to create new synthetic identities.

The terrorist organization opens several credit card accounts and bank accounts with these synthetic identities and procures driver's licenses for each identity from the dark web.

Using the synthetic accounts, illicit credit card purchases are used to further the extremist objectives of the organization, funding members' living expenses and purchasing supplies. As a result, financial institutions lose tens of thousands of dollars.

In addition, synthetics' bank accounts are used to funnel money to the terrorist network and potentially, launder funds obtained illegally.

Importantly, some of the synthetic identities are used by several members of the organization who are currently on a no-fly list or an OFAC watchlist. Accordingly, members who are otherwise precluded from travel and conducting business with U.S. banks are now free to do so under the auspices of their newly created identities.

Consequently, the group is able to travel, fund and potentially carry out terrorist attacks.

AFTERMATH

While all synthetic identity fraud is a criminal activity, there are some truly horrific uses of synthetics. The ability synthetics provide a criminal or fraudster to go undetected is well-recognized and heavily utilized for a variety of illegal acts. This unsettling truth further emphasizes the need for the payments industry stakeholders to work together to collectively mitigate this type of fraud to reduce the monetary impacts and help preserve the safety and security of human lives.