HOW SYNTHETIC IDENTITIES ARE USED TO COMMIT FRAUD

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.

Synthetic identities can be used in many ways to commit fraud. While some people simply use them to get a job and make a living, others are financing international terrorism. While not everyone is acting with malicious intent, any dishonest use of PII is considered fraudulent.

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 establish or secure employment or services with his/her own PII elements. Typically, the individual has no intent to default on payment.

Example: does not have a Social Security number (SSN) – An individual immigrated to the U.S. and sought honest employment to provide for his family. As a non-citizen, he did not have an SSN issued by the Social Security Administration. He purchased an SSN from an organization claiming to help provide employment services for immigrants. The SSN he purchased rightfully belongs to an elderly person who was not actively using credit. The immigrant applied for and secured employment, earning wages under his name and the purchased SSN.

Example: unwilling to use SSN – An individual who was the victim of domestic violence left home for a fresh start. She attempted to hide her new address from being discovered by using a fake name and made-up SSN to apply for housing and set up a new bank account. She didn't realize the made-up SSN is a real SSN that rightfully belongs to another individual.

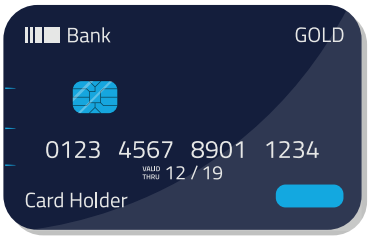
HOW SYNTHETIC IDENTITIES ARE USED TO COMMIT FRAUD

An individual may want to qualify for a large purchase or line of credit – or simply rebuild credit for future use – but cannot do so due to a previous negative credit history or bad debt. To appear more creditworthy, the individual created a synthetic identity and began building a more positive credit history and/or increased purchasing power through this new identity.

Example: Following a personal bankruptcy, an individual sought help for rebuilding his credit. An organization posing as a credit repair agency guided the individual to rebuild his credit by applying for new credit under his full name, date of birth and a randomized nine-digit number instead of his actual SSN. This number, called a Credit Profile Number or Credit Privacy Number (CPN), is positioned as a legitimate way to disassociate the individual from his bad credit history. Often unbeknownst to the individual, these CPNs are really SSNs belonging to other individuals and using them is illegal. Often unbeknownst to the individual, many CPNs are SSNs not tied to an active credit file, such as those belonging to children or the elderly. There is nothing legitimate about CPNs and if using one for credit repair, that consumer has engaged in identity theft. Using a CPN on a credit application is a violation of federal law and can result in prison time and/or substantial fines.

HOW SYNTHETIC IDENTITIES ARE USED TO COMMIT FRAUD

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.

Example: fraud conducted over time – An individual opened a consumer credit card using a synthetic identity. For several years, the individual made small, frequent purchases and paid off the balance on time and in full every month. Because of the long, positive payment history, the credit line on the card increased to $20,000. At this point, the individual maxed out the credit line and ceased to make any payments. The credit card company was left with no "real" individual from whom to seek payment.

Example: fraud that occurs up front – An individual secured an auto loan using a synthetic identity. He purchased a new car and drove it off the lot. No payments were made on the loan and there was no "real" individual from whom to seek payments, so this essentially became a stolen vehicle.

HOW SYNTHETIC IDENTITIES ARE USED TO COMMIT FRAUD

OTHER CRIMINAL ACTIVITY

Synthetics can be used to facilitate a means to an end as part of other illegal acts.

These acts are pervasive in nature and impact many industries outside of the payments industry, such as the insurance, healthcare, government and telecommunications industries.

Examples of illegal acts:

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

Criminals conducting these illegal activities range from individuals to transnational organized crime groups.

Regardless of the motive or industry, synthetic identity fraud is a crime. By understanding more about how synthetics are used, organizations can be better prepared to detect potential synthetic activity and individuals can better understand how to protect themselves from this type of fraud.