

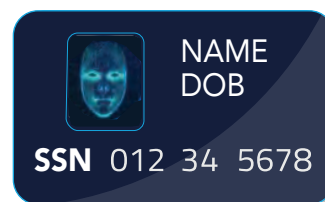
# ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION



While the execution of synthetic identity fraud can be quite complex, certain factors aid in the creation of synthetic identities, often making it more attractive to fraudsters than many other types of fraudulent activity. From the foundational way the United States approaches identities to the processes in place to build and foster credit, fraudsters zero in on opportunities to not only create, but quickly establish a synthetic identity in the payment system.

## USE OF SOCIAL SECURITY NUMBERS AS A PRIMARY IDENTIFIER

Synthetic identities tend to be more prevalent in the United States than in other countries due in part to a strong reliance on Social Security numbers (SSNs) as identifiers.



SSNs were initially created by the Social Security Administration (SSA) for a very specific purpose: tracking earnings histories of individuals for use in determining Social Security benefits. Over time, the use of SSNs has expanded substantially to become an almost de facto universal identifier in the United States.

The problem with reliance on a static national identifier, such as the SSN, is that a compromised SSN can be used by fraudsters to take over an identity, or in the case of synthetic identity fraud, create a new identity under the guise of an existing SSN. SSNs also are hard to validate, as there is not currently a real-time mechanism for institutions to confirm the provided SSN matches other customer information on an application.

Then, beginning in 2011, the randomization of SSN assignment affected SSN validation processes. **According to the SSA**, randomization was implemented to protect the integrity of SSNs and to extend the pool of nine-digit SSNs available nationwide. Randomization eliminated the geographical significance of the first three digits of the SSN (also called the area number), which financial institutions previously used when attempting to determine the SSN's state of origin.

# ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

## IMPROVED SSN VERIFICATION ON THE HORIZON

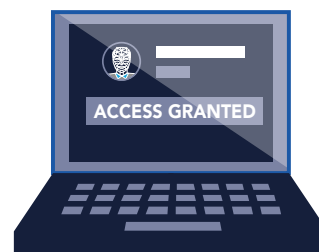
To help control fraud related to SSNs, the SSA introduced a written **Consent Based Social Security Number Verification (CBSV)** service in 2008. This service enables paid subscribers to verify a name, date of birth and SSN match the SSA's records with written consent from the SSN holder. A challenge of this paper-based process was the requirement of a physical, or "wet," signature from the SSN holder. This often took time to obtain and submit for verification processing. An **electronic version of this verification process** was introduced as part of a pilot program by the SSA in 2020, allowing the use of electronic signatures for consent and therefore, quicker submission and processing times for verification. The pilot program initially launched with a limited number of permitted entities (10) but expanded rollout in 2021. The ability for institutions to validate key identity elements of a customer when processing an application will enable them to better identify potential synthetic identities up front, preventing them from entering the institution's portfolio.

## SOME SSNS ARE MORE ATTRACTIVE TO FRAUDSTERS

In the creation of synthetic identities, fraudsters often will leverage an SSN that is not tied to an active credit profile. This includes SSNs issued to children, the incarcerated and the elderly, as fraudsters rely on the fact that these populations do not regularly use or monitor their credit.

## FREQUENT DATA BREACHES / INCREASED AVAILABILITY OF PERSONAL INFORMATION TO FRAUDSTERS

A record number of data breaches over the past few years have placed valuable personally identifiable information (PII) at fraudsters' fingertips. According to **the Identity Theft Resource Center**, records of more than 300 million individuals were exposed in 2020 alone as a result of data breaches. The information obtained from these data breaches is often shared among criminals on the "dark web" - a subset of the internet inaccessible by traditional browsers and search engines, and where content and activities are anonymous. Information readily available for purchase includes bank login credentials, account information, driver's license numbers, credit card numbers and SSNs. Other popular means for obtaining PII include social engineering or simply collecting information shared on social media. There is no shortage of data available to fraudsters wishing to create a synthetic identity using real or modified information.





# ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

## CREDIT APPLICATION PROCESSES WORK TO THE FRAUDSTER'S ADVANTAGE

- **Credit file creation:** After the initial creation of a synthetic identity, certain required credit processes can help facilitate the introduction of the synthetic identity into the payment system. Upon initial creation, the synthetic identity has no purchasing power, so the fraudster often initiates a credit application. Even if a credit application is rejected, the credit reporting agencies (CRAs) automatically create a new credit profile, since the applicant is considered to be both new and a real person. (This is a requirement of the **Fair Credit Reporting Act**, which mandates that CRAs create a profile for an individual if none exists.) The new credit profile creates an identity marker which becomes the synthetic identity's so-called "proof" of existence. The fraudster then continues to apply for credit until eventually approved. The credit bureau assumes the first applicant using a given SSN is legitimate. Any other individual who applies for credit using the same SSN then must prove his or her identity - including the actual person whose SSN was stolen.
- **Credit scoring and authorized users:** Several considerations factor into a credit score, including payment history, credit utilization and length of credit history. While fraudsters may choose to build up a synthetic's creditworthiness over time, they also may act on more immediate ways to boost the identity's credit score. "Piggybacking" involves becoming an authorized user to another individual's account with good credit. In many cases, the authorized user then acquires the established credit history of the primary user, rapidly building a positive credit score. Fraudsters will go as far as to pay to be added as an authorized user to unsuspecting consumers with good credit, which expedites the credit boosting process. For the less patient fraudsters, this approach provides a more profitable synthetic in a shorter amount of time.




## LIMITED VERIFICATION OF IDENTITIES

Synthetic identities typically will exhibit payment behavior mimicking an upstanding customer. As such, the key to detection is looking at the identity itself. However, current practices involve a limited degree of identity verification.

- **Customer onboarding:** During the onboarding process, institutions often will validate some customer information (such as name, date of birth, address and SSN), but this is not considered a thorough identity verification and often leans on a limited number of source documents that are easy to fabricate.





# ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

- **Ongoing authentication:** Once an account is opened, institutions tend to rely on the account opening process for identity verification and do not complete any subsequent validation or authentication of the identity. In effect, once a synthetic enters a portfolio, it can conduct activities without being identified until it's too late and a loss has been incurred.

## TAKE ACTION

It is important to recognize how easy it is for fraudsters to create synthetic identities and yet, how difficult it is to detect them. If you observe fraudulent payment activity by a customer, consider the fact that your customer might not actually exist. By educating your organization about these processes, you are one step closer to helping mitigate this complex type of fraud.

*The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.*