Socure

Sigma
Synthetic Fraud

Synthetic identity fraud represents the next wave of complex fraud and financial theft online. As early as 2016, synthetic fraud accounted for 20% of total credit losses in U.S. lender portfolios.

Synthetic IDs are created when a fraudster applies for an account using a combination of real and fake, or sometimes entirely fake, information. The act of applying establishes a credit file, so the identity may appear to just be a "thin file" consumer.

Synthetic identities are cultivated over time—months or even years—where criminals build up a decent credit score, open multiple accounts, make payments on time, and appear to be a good customer while going undetected. At some point, they "bust out," by depleting all available credit lines and then disappear.

Four main factors contribute to burgeoning synthetic ID fraud: the vast amount of compromised PII which is available for exploitation, the growth of digital account onboarding and services on the internet, Social Security number randomization, and the prioritization of customer experience and revenue growth with the rise of digital commerce.

Defining the Challenges

Synthetic ID fraud is difficult to detect because it lacks a common dependent variable classification and definition upon which to build reliable fraud models. Furthermore, it is a victimless crime that lacks a real individual to alert financial services providers that someone is using their identity to open accounts. Sometimes institutions are unaware of the magnitude of the problem hiding within their portfolios because synthetic identities often look benign or even very good, with FICO scores of over 750.

Socure solves these challenges with a multi-layered approach that looks beyond PII elements at digital entry points and leverages advanced analytics and diverse, deep data sets to gain conviction on the applicant's identity. In addition, deploying machine learning to detect synthetic IDs creates efficiencies and avoids manual reviews and human error, without degrading customer experience.

The Socure Approach

Sigma Synthetic Fraud was developed for a digital-first environment. Socure invested heavily in feature engineering and data source analysis, and used both supervised and unsupervised machine learning models to derive a common definition of synthetic identity fraud. Socure leveraged this definition to develop classification models that have proven effective in combating this elusive type of fraud.

Below are examples of a few of the many predictive features used in the Sigma Synthetic model:

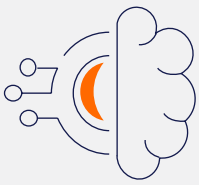
- High number of inquiries across all credit reports
- Randomized SSN issued after 2011
- Inability to match and/or verify an identity across all PII elements
- High risk associated with a phone number
- High risk associated with an email address

Customers of Sigma Synthetic Fraud receive the benefit of leveraging Socure's broad network insights and feedback file data sets, which continuously enhance the synthetic fraud engine, resulting in the most accurate and performant solution on the market.

Superior Model Performance

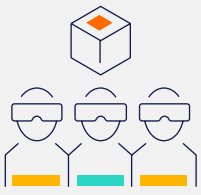
Sigma Synthetic Fraud achieved an average AUC of 97.44% with a synthetic capture rate as high as 90% in the top 3% of riskiest users. Specific reason codes enable clients to clearly understand hidden patterns of synthetic fraud.

How It Works

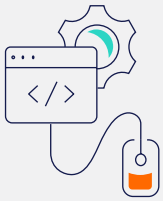


Socure employs a highly sophisticated approach with supervised and unsupervised machine learning that achieved average AUC of 97.44%

Rich data sources with best-in-class utility, credit, telephone, energy and public records data sources and the largest database of known good and bad identities



Tenured data science team of fraud experts focused on producing successful solutions for similar fraud challenges



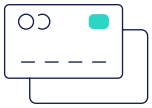
Curated set of solutions via a single API with just 4 lines of code

One API, Many Solutions

Sigma Synthetic Fraud is offered both standalone and as part of an integrated identity verification and fraud mitigation platform, Socure ID+, alongside Sigma Identity Fraud, Compliance, and DocV. This new module effectively manages synthetic ID fraud risk without slowing down new business growth or turning a blind eye to potentially risky accounts. When applied at account enrollment or to an existing customer portfolio, Sigma Synthetic quickly assesses the risk of synthetic fraud and provides a decision in a fraction of a second. It can also reduce the number of applicants requiring a second, more costly and time consuming review, such as the consent-based eCBSV. Sigma Synthetic and all Socure products are accessible via one single API that powers the entire Socure ID+ platform.

Use Cases

New Accounts



Credit Cards

Auto Lending

Unsecured Loans

Telecommunications

Healthcare

Insurance

Ecommerce and Marketplaces

Government Benefits

Real Estate

Experience the Advantages

Companies fighting synthetic ID fraud need to recognize the limitations of strictly evaluating static identity elements. Instead, Socure achieves a multi-dimensional view utilizing sophisticated machine learning models trained with consortium data from across the industry—resulting in the ability to pinpoint synthetic fraud patterns accurately within milliseconds. Sigma Synthetic Fraud gives you more control over your entire operation and reduces manual reviews to save time and money.

Contact **sales@socure.com** to learn more about how Socure can transform your business.