Socure

FACT SHEET

Sigma Synthetic Fraud

Predict and prevent synthetic identity fraud before it happens

Sigma Synthetic Fraud uses predictive machine learning and diverse, high-quality third-party and historical data to uncover complex anomalies and connect behavioral patterns associated with synthetic identities, so you can capture fraud at the door — making way for more good customers.

Target fabricated and manipulated identities

Sigma Synthetic Fraud specifies the Federal Reserve's definition of manipulated or fabricated synthetic fraud types so you can create the best treatment strategies.

Access 400+ third-party data sources

Proof of life, credit inquiry, and hundreds of other authoritative data sources permit the model to corroborate input data and, when combined with cross-industry network intelligence, analyze anomalous PII usage that leads to greater fraud capture.

Leverage a powerful consortium database

A consortium network of more than 1,900 diverse customers enables Socure to understand identity elements based on outcomes for more than two billion known good and bad identities.

Outsmart synthetics with AI that thinks like a fraudster

The Sigma Synthetic Fraud model ingests cleanly-labeled feedback data that trains the system to think like a fraudster to accurately predict and detect evolving synthetic fraud threats.

Calculate a Sigma Synthetic Fraud Score

The model returns a predictive fraud score that gauges identity risk calculated on 4,000+ synthetic-specific features and patterns.

Employ interpretable technology

Simple-to-understand reason codes delivered with each fraud score provide explainable and actionable insight for each decision.

46.9% Fraud Capture Rate
1:1 False Positive Rate
in the riskiest 1% of users

Reduces overall false positives by 50%*

Captures 10% more fraud in the riskiest 1% of users*

Decreases false positives for younger demographics by 33%*

Reduces the overlap with Sigma Identity Fraud to 2%*

Achieves nearly perfect classification*

* Current V4 versus V3 model

Smarter synthetic identity fraud detection

To fight this insidious and growing form of identity fraud, Socure's approach applies layered defenses that correlate consumers' PII, events, and behaviors across businesses, locations, and devices using powerful, predictive machine learning trained for more than a decade on 400+ data sources and cross-industry network feedback from Socure's 1,900+ customers. Without the benefits of a robust consortium network, you have a limited ability to pinpoint tricky synthetic elements, exposing your business to unnecessary risk.

Socure Risk Insights Network

The Socure Risk Insights Network is the bedrock that powers Sigma Synthetic's best-in-class accuracy with trustworthy risk intelligence derived from proprietary cross-industry data, advanced ML, and robust identity graph resolution.

Human-in-the-Loop Labeling

Expert fraud investigators cleanse raw data to align with the Federal Reserve's definition of fabricated and manipulated synthetic fraud to assure that properly-classified data is being ingested to train the model.

Proof of Life Data Sources

Thin-file applicants with no consumer history look like synthetic fraudsters. Proof of life data confirms the existence of younger and immigrant demographics, thanks to driver's license, education, and property records — whereas synthetic identities are missing these forms of proof.

Enhanced Email Risk Intelligence

Enhanced email risk intelligence blocks email tumbling that is commonly associated with synthetic identities, which occurs when fraudsters create "alias" email addresses using punctuation marks and periods.

Synthetic-Specific Behavioral Features and Patterns

By mobilizing cross-industry data and advanced machine learning algorithms, the Sigma Synthetic Fraud model has generated 4,000+ features, patterns, and anomalies, including elaborate SSN and DOB signals, that indicate synthetic fraud behavior and make it possible to detect and prevent synthetic fraud in real time.

eCBSV and Digital Intelligence Add-ons

Sigma Synthetic Fraud paired with eCBSV and device and behavioral analytics boost synthetic fraud detection, while also auto approving more good customers.

Socure

Reap the extraordinary benefits

Adopt the synthetic fraud solution trained to think like a fraudster and apply this smarter intelligence to stop synthetic fraud from entering your ecosystem.

Employ proactive synthetic fraud detection

Predict and prevent synthetic fraud before it happens to avoid financial losses

Improve user experience

Decrease false positives and boost user satisfaction with quick and reliable approvals

Open more good accounts

Drive revenue growth by auto approving more good customers faster

Lower operational costs

Reduce manual reviews and operational expenses with a fully automated solution

Prevent reputational damage

Avoid enforcement action and fake account prosecution

Use cases for ever-evolving synthetic threats

Sigma Synthetic Fraud is an omnichannel solution that should be deployed at onboarding and can be used at other critical junctures in the user journey, including to capture synthetic identities that may be lurking in an existing ecosystem:

- New application
- Non-monetary account changes
- Funds disbursement
- Portfolio scrubs

For more information, contact us salesinfo@socure.com.

FS_5612134744-01

Socure