Aite Novarica

SEPTEMBER 2021

2021 IMPACT INNOVATION AWARD IN FRAUD

SOCURE

TRACE FOOSHÉE
+1.857.406.3515
tfooshee@aite-novarica.com

This report provided compliments of:

Socure

IMPACT BRIEF

SOCURE

Founded in 2012, Socure provides identity verification solutions that help companies comply with Know Your Customer (KYC) regulations and empirically optimize the balance between fraud mitigation and customer acquisition throughput. Its diverse product portfolio is API based and orbits around a predictive analytics platform applying an ensemble of risk models developed with a variety of machine learning techniques to predict the likelihood that the applicant is who they claim to be.

Socure's platform differentiates itself from the burgeoning range of competitors in the identity verification market. Its identity resolution engine analyzes over eight billion records and more than 530 million good and bad identities. It also evaluates streaming data, credit bureau history, utility data, telecom history, higher-education records, and over 200 other data sources to establish a multidimensional view of applicants. The products within its integrated product portfolio are both API and SDK based. They are built around a rigorously managed and highly automated model performance monitoring process to produce an array of outcomes that provide customers with options for finding the right balance between fraud prevention and client experience and/or acquisition objectives. Today, they are among the industry's leading identity verification and KYC solution providers, with deployments among four of the five largest U.S. banks, seven of the 10 largest credit card issuers, top buy now, pay later (BNPL) providers, top crypto exchanges, and the largest online gaming operators. Socure's Sigma Synthetic fraud product was designed specifically to detect the use of synthetic identities by criminals looking to establish an account from which they either intend to incubate an identity or to use it to commit one of several forms of synthetic identity fraud.

MARKET CHALLENGES AND NEED

Synthetic identity fraud is an umbrella term that applies to a variety of illegal activities conducted by someone using an identity fabricated or manipulated for the purpose of committing illegal or fraudulent acts. Table A lists some of the most common types of activities commissioned by those using synthetic identities.

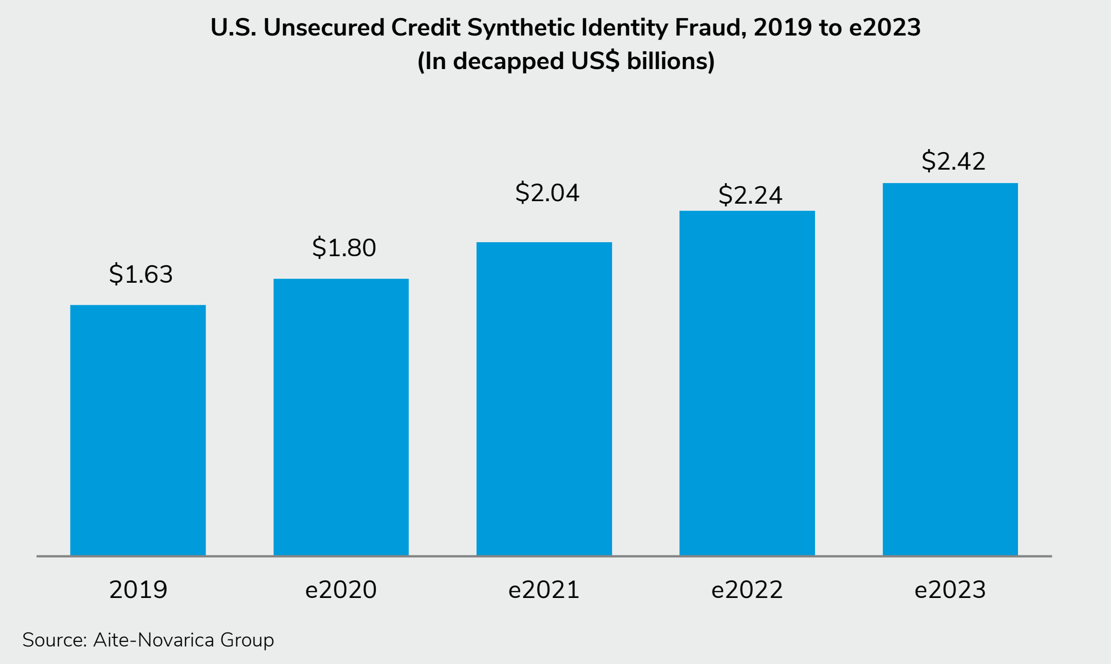
TABLE A: COMMON WAYS THAT SYNTHETIC IDENTITIES ARE USED TO COMMIT FRAUD

ACTIVITY	DESCRIPTION
First-party fraud	The fraudster opens an account to take money credited to them, either by way of a credit line or by way of advanced funds for a deposit that hasn't completed clearing. In either case, the fraudster takes the money with no intention of returning it.
Mule activity	The account holder opens the account to move money obtained from—or intended for—one or more criminal activities, including theft, fraud, terrorist financing, human trafficking, drug trafficking, illegal arms trafficking, and smuggling.
Incubation	The fraudster takes advantage of credit repair companies or existing account holders who are seeking a little money on the side or are altruistically motivated to help repair others with little or no credit history by putting them on to their account so that the fraudster can establish a credit history prior to establishing their own fraudulent account.

Source: Aite-Novarica Group

Synthetics have proven to be exceptionally appealing to criminal groups largely because they are a cost-effective means of generating revenue and provide an attractive alternative to outsourcing mule accounts to an unwieldy network of conscripted or coerced money mules. As the frequency and severity of data breaches have increased over the years, criminal marketplaces have been inundated with the raw material that fraudsters need to fabricate synthetic identities, driving the cost of fabrication down and making them a viable means of operating at a larger scale. This, in turn, has led to an expansion of the estimated amount of synthetic fraud losses at financial institutions (FIs), as illustrated by Figure 1, which estimates total unsecured credit losses resulting from synthetic identity fraud.

FIGURE 1: ESTIMATED UNSECURED CREDIT SYNTHETIC IDENTITY FRAUD LOSSES IN THE U.S.



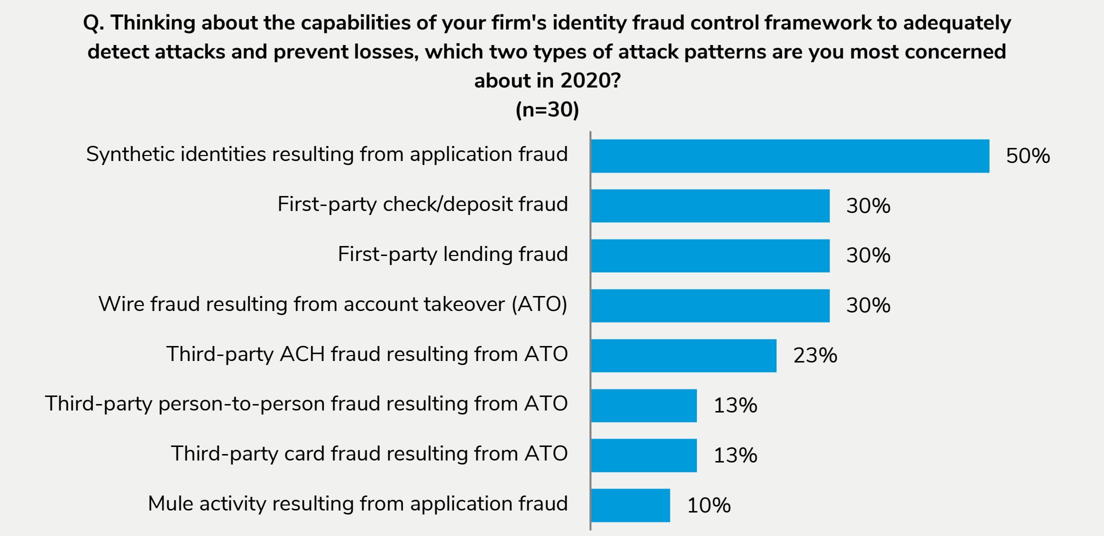
Source: Aite-Novarica Group

The scale of mule activity is difficult to estimate since most FIs do not formally track it.[1] Still, most fraud executives agree that detecting synthetics is not only challenging[2] but is also one of the greatest concerns that they have in shoring up their identity fraud control frameworks (Figure 2).

[1] See Aite-Novarica's report Mule Activity: Find the Mules and Stop the Fraud, April 2020.

[2] See Aite-Novarica's report Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise, February 2021.

FIGURE 2: CONCERN AMONG FRAUD EXECUTIVES REGARDING SYNTHETIC IDENTITY FRAUD



Source: Aite-Novarica Group Survey of 46 financial services fraud executives, September 2020

As criminal groups have expanded their dependence on synthetics, the demand among FIs for a cost-effective means of detection and prevention has followed suit. However, the catch is that distinguishing a synthetic identity from a legitimate identity has been an exceptionally difficult nut to crack. There are many reasons why this has been such a challenge, but two are worth considering to illustrate the contours of the issue. The first is that many synthetics are engineered to defeat many legacy identity verification control solutions. Specifically, the fraudsters incubate synthetics in a way specifically designed to create just enough of a credit history to make them appear legitimate to legacy identity verification solutions that rely heavily on the applicant's credit header information to verify the applicant's identity. The second is that most FIs have been under great pressure to acquire new customers. Many have pursued acquisition strategies that rely heavily on pursuing the "underbanked" segment of the public. People in that applicant segment often appear to have little or no credit history, creating an excellent opportunity for synthetic identities to blend in with the crowd.

While no FI wants synthetics in its portfolio, there haven't been many good options purpose-built specifically to control for them either. Most methods employed by FIs seeking to examine their portfolios for synthetics and establish filtering agents within their identity verification control frameworks have leaned heavily on internally developed analytics-based approaches. This depends upon having an analytics unit and the capacity to acquire and transform the data necessary for the exercise—resources inaccessible to all but the largest FIs. Most others have had little choice but to contract with a consultancy until a cost-effective and accurate detection system emerges.

INNOVATION: SOCURE'S SIGMA SYNTHETIC FRAUD

Recognizing the expanding market opportunity for a modular identity verification solution designed specifically to detect synthetics, Socure began developing its Sigma Synthetic product in 2020. The product launched in October 2020. It has been gaining attention among FIs interested in a cost-effective and accurate means of distinguishing synthetics from legitimate cohorts, especially among the ranks of the underbanked segment of the banking public where most synthetics are believed to hide. Because the solution is modular, it works well when deployed in isolation or in concert with an existing phalanx of identity verification controls. Socure's synthetic fraud solution has been optimized to work in concert with Socure's companion solutions—Sigma Identity, KYC, and Document Verification, in particular. The combined solution provides a robust end-to-end suite of identity verification controls (Table B).

TABLE B: SOCURE SIGMA SYNTHETIC FRAUD INNOVATION SUMMARY

CATEGORY	DETAILS
Innovation	Socure Sigma Synthetic
Official launch date	October 2020
Description	Sigma Synthetic is purpose-built and trained with consortium data from Socure's largest FIs to tackle targeted fake, randomized, and synthetic patterns to produce highly accurate real-time actionable reason codes and risk scores.
Implementation time and approach	The solution's API-based architecture enables most FIs to begin with a proof of concept (POC). Therein, they can customize the targeted set of synthetics indicators and experiment with various ranges of parameters enabling them to empirically triangulate the range of performance characteristics that optimally fits with their risk tolerances. Once the POC has achieved the targeted performance thresholds, the transition from POC to production-ready filtering is restricted only by the FI's capacity to begin processing alerts.

CATEGORY	DETAILS
Key differentiators	• A range of over 400 data sources power Socure's real-time identity verification and risk detection • More than 8,000 predictive signals for known good and bad identities • A blend of supervised and unsupervised clustering techniques to determine well-labeled synthetics • Network consortium feedback, including synthetic tags, constantly improves model training and management of emerging threats across various industries and channels • Graph-based techniques extracting topological, velocity, and personally identifiable information (PII) interaction features

Source: Socure

Socure invested heavily in feature engineering and data source analysis, and used both supervised and unsupervised learning models across numerous industry verticals to derive a common definition of synthetic identity fraud.

TARGET MARKET

Socure's target market for this product is primarily financial services, both traditional institutions and fintech firms. However, fraudsters who use synthetic identities do not target financial services exclusively. So there are market opportunities among automotive finance, property rental, utilities, and telecom companies,[3] just to name a few sectors that depend on establishing accounts tied to a verified identity. Given the widespread nature of the challenge and the scale of the losses associated with the unsecured lending segment of the financial services industry alone, it's clear that there is no shortage of market demand for purpose-built synthetic identity fraud detection solutions.

HOW IT WORKS

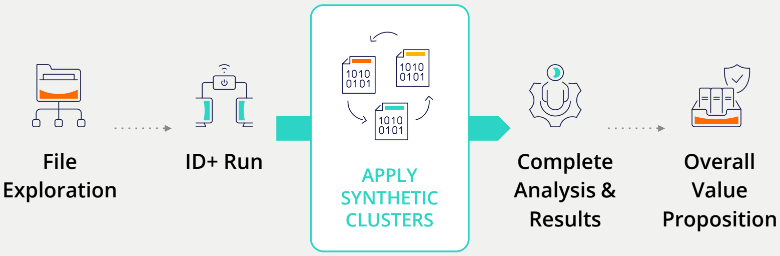
Before examining the mechanics of how the product works, it's important to establish one characteristic of the solution more rooted in Socure's approach to deployment than in the system's functionality. To make a compelling business case for acquiring a

[3] See Aite-Novarica's report Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise, February 2021.

synthetic fraud solution, an FI must first come to agreement on whether the problem exists, and second, the degree to which that problem damages profitability. While this sounds straightforward, anyone familiar with managing the highly competitive process for securing funding inside a modern FI can attest to just how complicated and challenging it can be to win investment committee approval. Like mules and scams, synthetics make for a tricky business case, largely because there is typically little agreement between security leadership, product leadership, and channel leadership as to the scale of the damage these activities have on profitability. This is precisely where Socure's approach is not just innovative but also vital to its capacity to build traction in the market.

The value proposition for Sigma Synthetic starts with a POC exercise (Figure 3) intended to empirically reveal the scale of the FI's synthetic identity problem prior to collaboratively building the internal business case and imperative for addressing it.

FIGURE 3: SOCURE'S POC METHODOLOGY

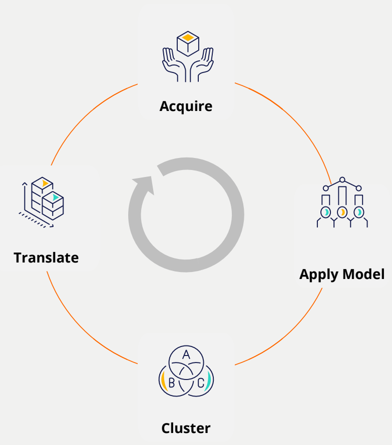


Source: Socure

It's important to understand that most FIs have done very little analysis to reveal the extent to which they have a problem with synthetics. As a result, many stakeholders often claim that the problem is either nonexistent or small enough to justify opposing investment in a specific solution. Socure's objective diagnostic of the problem is a clever first step. However, the diagnostic would be dead-on-arrival if it weren't for Socure's ability to easily adjust the features that the clustering models leverage to define what qualifies as a synthetic, as well as the type of synthetic (e.g., compiled, manufactured, or fabricated). This means that the FI can establish a range of definitions for synthetics, which goes a long way toward overcoming objections from those who might argue, for example, that the scale of the problem is exaggerated by those biased toward more restrictive risk tolerances that would have a chilling effect on acquisition volume.

Of course, the diagnostic must actually be able to effectively distinguish between a synthetic and a legitimate applicant identity for the investment decision-making factions to come to agreement, much less pass judgement. It is, therefore, helpful to examine the analytical underpinnings of the solution to better understand the mechanics of how the solution detects synthetics. As the methodology for the diagnostic POC suggests, the solution relies on automating the labeling process—normally, this is a manual process conducted by fraud analysts. The clustering agents in the solution are the product of many years of data science plus an extraordinary database of over 8 billion rows of identity records and over 530 million known good and bad identity profiles acquired from a consortium compiled from hundreds of FIs. Figure 4 illustrates the process that Sigma Synthetic utilizes to develop and automate performance monitoring and tuning of the clustering agents at the heart of the system's capacity to distinguish between legitimate and synthetic identities.

FIGURE 4: SIGMA SYNTHETIC OPERATIONAL PROCESS FLOW



1

Acquire
Acquire consortium synthetic data sets from variety of clients expanding multiple industries

2

Apply Model
Apply Sigma Synthetic Model to understanding decisioning trees branches and leaves

3

Cluster
Cluster together similar leaves as dictated by independent variables to properly group similar leaves from the supervised model

4

Translate
Select clusters that maximize the bads and minimizes the goods, and then translate these into business interpretations

Source: Socure

In terms of its impact on the client experience, Socure's Sigma Synthetic product integrates directly into the FI's new account application platform through a set of available APIs. As a result of this behind-the-curtain API integration, there is no hint to the applicant that their identity is being analyzed.

KEY QUANTITATIVE AND QUALITATIVE RESULTS

Socure has received positive feedback from clients that have partnered for POCs on Sigma Synthetic's synthetic detection capabilities and accuracy in distinguishing synthetics from legitimate applicants. Overall, Socure reports that Sigma Synthetic auto-captures 90% of synthetic fraud in the riskiest 3% of users, with an area under the curve (AUC) of 97.5%. The term AUC refers to the accuracy in classifying good applicants from synthetic applicants. Table C provides a sample of actual results from POCs with clients that have used Sigma Synthetic to diagnose the rate of synthetic applicants.

TABLE C: SOCURE SIGMA SYNTHETIC RESULTS

RISKIEST	OVERALL	CLIENT 1	CLIENT 2	CLIENT 3	CLIENT 4	CLIENT 5
0.50%	20.93% (29:1)	15.27% (40:1)	27.59% (21:1)	10.98% (39:1)	10.12% (36:1)	40.00% (24:1)
1%	33.09% (37:1)	25.29% (48:1)	36.60% (33:1)	19.21% (42:1)	22.78% (33:1)	52.38% (37:1)
2%	49.30% (50:1)	41.34% (59:1)	52.08% (47:1)	33.00% (31:1)	39.87% (38:1)	66.66% (59:1)
3%	59.50% (62:1)	53.01% (70:1)	60.96% (61:1)	42.36% (58:1)	55.06% (41:1)	71.42% (83:1)
5%	71.56% (86:1)	66.09% (94:1)	74.96% (82:1)	60.34% (68:1)	67.72% (56:1)	80.95% (123:1)
AUC	**95.44%**	**94.69%**	**96.38%**	**95.67%**	**96.56%**	**96.11%**

Source: Socure

FUTURE ROADMAP

The product roadmap for Socure's Sigma Synthetic is designed to further enhance the solution's data sources and add model features and labels:

- In four months, Socure will incorporate the results of testing of more than 4,000 new variables, including device characteristics, to enhance prediction accuracy and effectiveness.
- Over the following 12 to 24 months, Socure will continue to innovate in both manual and automated labeling, add data sources, and layer behavioral analytics into Sigma Synthetic scores.

AITE-NOVARICA'S TAKE

While there are competing identity verification solutions in the market that claim to protect against synthetics, a couple of things differentiate Socure's Sigma Synthetic solution. First, the degree of rigor in its approach to model development and performance management and its emphasis on growing and diversifying the unique blend of data sources make Socure's solution appealing. Specifically, the multiple supervised and unsupervised ensemble of machine learning models developed to compete with one another exclusively to hone and improve the accuracy and flexibility of clustering and segmenting applicants makes the performance of its solution highly competitive. This is particularly important for practitioners who find themselves making the case for investing in a solution to combat synthetics. As previously discussed, it can be an uphill battle just to arrive at a mutually agreed upon definition of the problem, much less a dependable estimate of the scope of it.

Second, the modularity and configurability of the solution distinguish it from its competitors. Since most FIs already have made heavy investments in their identity verification control frameworks, it's appealing that Sigma Synthetic can be deployed as a stand-alone module or integrate into an existing stack of systems without disruption. That it also provides the capacity to improve the efficacy of the solution and expand upon it with additional layers of control is an added bonus for those still in the early stages of maturing their application fraud controls.

IMPACT INNOVATION AWARDS IN FRAUD & AML

The world is changing rapidly, and sustaining effective financial crime risk management has become extremely challenging and complex. The breadth and capabilities of fraud and AML technology solutions must now go beyond traditional offerings to address new market forces, fight financial crime, and achieve regulatory compliance while elevating the customer experience and operational efficiency.

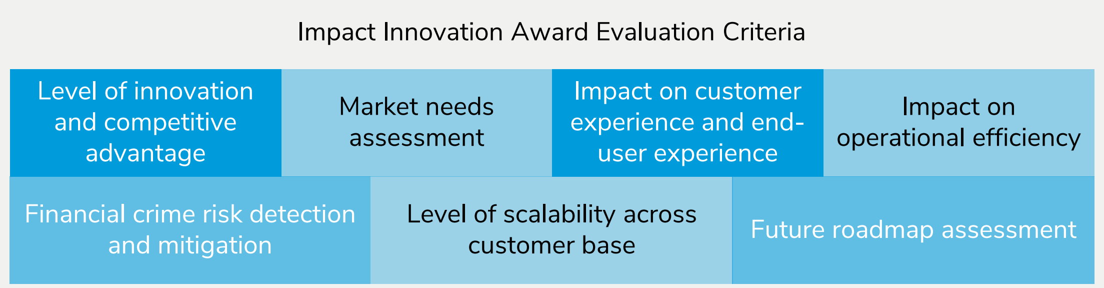
Aite-Novarica Group's inaugural Impact Innovation Awards in Fraud & AML are designed to recognize and celebrate innovations that are disrupting financial crime. Award recipients are leading the industry by identifying and implementing new products, capabilities, or levels of automation and effectiveness that bring our financial services industry one step closer to next-generation fraud and AML innovation. They are the FIs and technology providers, regardless of size or region, that others will follow.

QUALIFICATION AND EVALUATION METHODOLOGY

Aite-Novarica Group solicited nominations for its 2021 Fraud & AML Impact Innovation Awards from May to the end of June 2021. All nominated initiatives were required to be in production and must have been implemented within the last two years.

Analysts from Aite-Novarica Group's Fraud & AML practice reviewed all fraud nominations and narrowed the field to the top submissions. Along with Aite-Novarica Group Fraud & AML analysts, an external panel of subject matter experts and industry thought leaders determined the winners of three distinct fraud innovation categories: risk mitigation, operational efficiency, and customer experience. Each fraud nomination was evaluated on seven individual criteria (Figure 5).

FIGURE 5: IMPACT INNOVATION AWARD EVALUATION CRITERIA



Impact Innovation Award Evaluation Criteria

Level of innovation and competitive advantage

Market needs assessment

Impact on customer experience and end-user experience

Impact on operational efficiency

Financial crime risk detection and mitigation

Level of scalability across customer base

Future roadmap assessment

Source: Aite-Novarica Group

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

RELATED AITE-NOVARICA GROUP RESEARCH

Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise, February 2021

Mule Activity: Find the Mules and Stop the Fraud, April 2020