Socure

CASE STUDY

How a top five U.S. bank identified risk associated with synthetics and potential mules in its customer accounts

Discover how a bank gained crucial insights into its portfolio of customer accounts to avoid severe financial and compliance penalties.

Lacking portfolio insights during a turbulent time

Did you know that a notable number of open deposit accounts in the U.S. are held by synthetic identities, likely acting as money mules to fuel fraudulent money movement?

There's a full expectation that regulatory changes will eventually transform how banks and fintechs operate specific to these types of accounts. To combat risks such as synthetic identity fraud and money mules to their organizations, leaders must scrutinize the consumer identities within their existing accounts with tools that allow them to identify these synthetic and mule accounts – all while continuing to fine tune customer onboarding strategies and fraud controls. Rates of synthetic identity fraud only continue to grow. Effectively addressing this threat starts with understanding the book of business that comprises your portfolio, who your customers are, and how those accounts are used and potentially abused for money mule activities.

Deposit, investment, and savings accounts are frequently used by money mules to launder money and fuel fraudulent money movement through P2P, wire transfer, ACH and other real-time payment rails. The fraudsters can use real people who are either aware or unaware of the scam, synthetic identities created using stolen or fabricated information and other fraudulent identity types to aid in the money movement. Synthetic identities are particularly challenging to detect because they often use valid Personal Identifiable Information (PII). Fraudsters can use synthetic identities to open bank accounts, apply for loans or credit, and conduct other financial transactions.

When a top five U.S. bank wanted to identify customer accounts that could cause financial or reputational harm to their organization, it turned to Socure.

Problem

- Economic and regulatory pressure
- Lack of insight into current risk within existing customer base

Solutions

- Through a Portfolio Scrub, Socure identified risk attributes to support periodic or perpetual Know Your Customer (KYC) or Customer Risk Rating (CRR) data points
- Performed data quality reviews to support deceased, contact, and new move updates that can impact current accounts
- Pinpointed risky identities hiding within a portfolio, including synthetic identities and third party fraud that may have slipped through account onboarding defenses

Results

- Out of ~2 million records, Socure found that ~2% of the bank's open accounts were high risk for KYC compliance or identity fraud
- 30,000 of the reviewed accounts were opened by manipulated or fabricated synthetic identities

Synthetic fraudsters are attacking deposit institutions at an increasing rate. Socure analysis shows that 1-3% or more of open deposit accounts in the U.S. are held by synthetic identities, likely acting as money mules to fuel fraudulent money movement.

Socure Portfolio Scrub

As the leader in digital identity verification and fraud prevention solutions, Socure's Portfolio Scrub helps fintechs and traditional banks uncover fraud and compliance risks that may have slipped through the cracks at, or after, account opening. This includes third-party and synthetic fraud risk, account takeover, high risk addresses, SSNs, emails, phones, and more.

The Portfolio Scrub analysis includes:

- Identification of risk attributes to support periodic or perpetual Know Your Customer (KYC) or Customer Risk Rating (CRR) data points.
- Data quality reviews to support deceased, contact, and new move updates that can impact current accounts.
- Identification of risky identities hiding within a portfolio, including synthetic identities and third party fraud that may have slipped through account onboarding defenses.

Accounts that may have been previously taken over

These valuable insights help organizations identify and understand their largest potential risk areas and receive individual, customer-level treatment strategies and remediation recommendations to reduce risk.

Socure's impact

Working with Socure's data science experts, this top-tier bank provided and tested ~2 million records of existing customer data for both credit cards and deposit, originating from digital and non-digital onboarding, as well as digital credit card businesses. Socure then ran the records through our Sigma Identity Fraud, Sigma Synthetic Fraud, Verify, and Email, Phone, Address RiskScores and Correlation Value modules.

Socure found that ~2% of the bank's open accounts exhibited high risk for either KYC compliance issues or identity fraud. These accounts exhibited invalid email addresses, phone numbers known to be associated with fraud, addresses for commercial reshippers, and a host of other signals highly correlated with fraud.

Additionally, 30,000 of the ~2 million accounts tested were opened by either a manipulated or fabricated synthetic identity, with a higher percentage of fabricated synthetic identities, which are known to incur significantly higher losses for banking institutions.

While analyzing the individual risk signals returned in the form of Socure's proprietary reason codes, the team found that 0.76% of SSNs across the bank's three lines of businesses were invalid, associated with a deceased individual, or did not resolve to the originating PII. Additionally, 25% of addresses being used as an individuals' address were either invalid or commercial, dual-purpose, or prison addresses.

Socure Reason Code	Percentage of Accounts
R972 - Address is a commercial mail receiving agency or commercial mail drop	~0.2%
R709 - Address labeled as commercial or dual-purpose	~2%
R916 - Address labeled as invalid or does not exist	~6%
R932 - Address identified as correctional facility	~0.01%

Socure Reason Code	Percentage of Accounts
R901 - SSN does not resolve to individual	8%
R907 - SSN reported as deceased	.25%
R913 - SSN invalid	.06%

Socure found that 30,000 of the bank's ~2 million accounts tested were opened by either a manipulated or fabricated synthetic identity, with a higher percentage of fabricated synthetic identities

Moving forward

Alone, these individual PII elements may not have flagged an account as high risk. However, financial institutions can't afford to lack awareness of the potential risk within their portfolio.

Armed with real insights into the risk of its existing portfolio, this bank worked with Socure to implement custom remediations such as additional account monitoring or step-up authentication such as eCBSV, as well as using Socure's DocV solution for document and live selfie validation.

It's critical to understand and reassess current onboarding strategies to prevent invalid information or risk, in any form, from coming into your ecosystem. Now is the time for responsible financial institutions to take a deep look at the consumer identities of account holders to tease out financial and compliance risks, before the potential reality of a changing regulatory and economic landscape puts them further at risk.

Bank records tested

Records with high KYC or identity fraud risk

Records created with manipulated or fabricated identities

Who's lurking in your portfolio?

Learn how Socure can help →

About Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN, and the broader internet to verify identities in real time. The company has more than 2,700 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries, including four of the top five banks, 13 of the top 15 card issuers, the top three MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers, and over 250 of the largest fintechs. Marquee customers include Chime, SoFi, Robinhood, Gusto, Public, Stash, DraftKings, State of California, and Florida's Homeowner Assistance Fund. Socure customers have become investors in the company including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, and Synchrony. Additional investors include Accel, T. Rowe Price, Bain Capital Ventures, Tiger Global, Commerce Ventures, Scale Venture Partners, Sorenson, Flint Capital, Two Sigma Ventures, and others.

CS_4828941172 120424

Socure