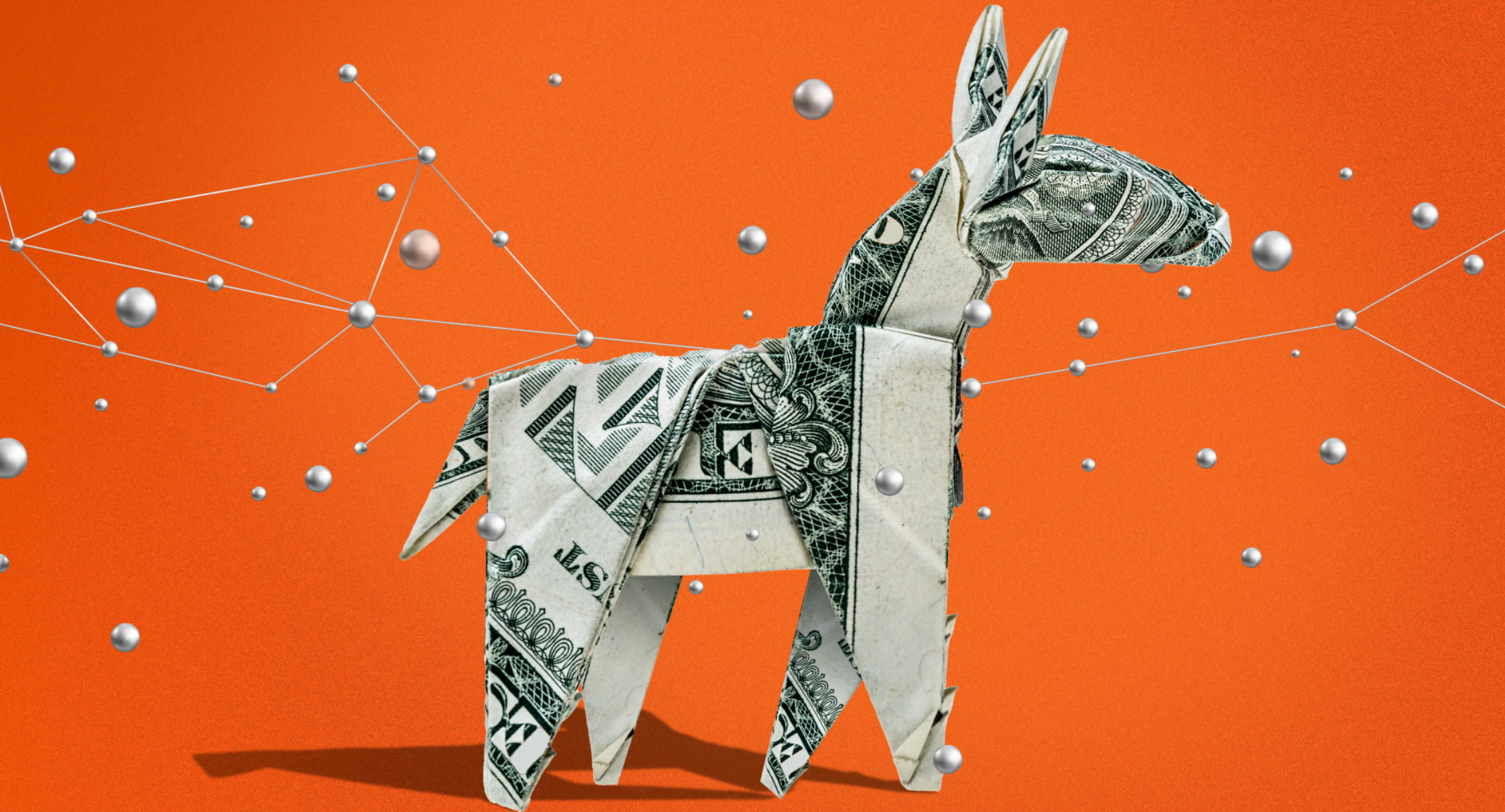


The Hidden Risk of Money Mules

Who's lurking in your portfolio?



Money Mules: An unwitting, active fraud participant?



.....
Regardless of their level of involvement, money mules are critical to fraud because they fuel fraudulent money movement.
.....

Hard-to-detect money mules have become an increasingly popular way for fraudsters to move money stolen from consumers and government in P2P and other scams. In an exploding and risky real-time payments landscape, the increase in money mule activity creates ample opportunities for bad actors. These fraudsters victimize unwitting individuals, participate with real consumers who knowingly take part in the scam, and develop synthetic identities to help them operate stealthily.

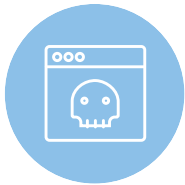
During COVID, fraudsters increased their efforts to open deposit accounts at high rates with fake, or synthetic identities, to move money without arousing suspicion. In fact, anywhere from 1 to 3% or more of open, active demand deposit accounts (DDAs), and savings and investment portfolios are synthetic identities being used as money mules to fuel fraudulent money movement. This trend has continued and even gathered strength following the bank failures in the first half of 2023.

Financial institutions may be missing the extent of this issue within their own portfolio. This is a dangerous path to take, as the risks associated with money mules and synthetic identities are real and should not be ignored. It's critical to understand these hidden risks – and know how to effectively fight back.

We know synthetic identities are an issue, but how big is the problem?

With the help of synthetic identities and money mules, criminals are laundering money, conducting illegal activities such as human and drug trafficking, and putting financial institutions at risk of compliance penalties and significant financial loss.

Here's the tricky part – these risks are often hidden and have gone undetected flying under existing defense controls, in some cases, for years. Fraudsters may stay dormant in accounts, waiting for the right moment to strike, also known as a “bust out.” Whether it's accounts that have been taken over or money mules and synthetic identities fueling fraudulent money movement, these identities create dramatic financial and compliance risks for financial institutions.

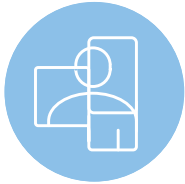


.....
Fraudsters are not just busting out once they make it through a financial institutions' onboarding – they're staying around and actively creating havoc for consumers and the U.S. financial system.
.....



Shifting fraud patterns led us here.

These concerns are heightened by uncertain financial forecasts that could lead to a substantial economic downturn and subsequent credit tightening, or new proposals from regulatory bodies like the Consumer Financial Protection Bureau (CFPB), which is considering proposals to redirect peer-to-peer (P2P) financial losses away from consumers and toward the banks and fintechs that hold the accounts.



.....
According to the U.S. Department of Justice, synthetic identity fraud is the fastest-growing financial crime.
.....



Economic uncertainty

Continued supply chain challenges, inflation, and turmoil in the banking sector are creating uncertainty in the market. Lenders and depository institutions are making plans to tighten credit controls and are increasing their focus on potential fraud that already exists within their account base.



Increased regulatory scrutiny

Since July 2022, the CFPB and several U.S. senators have been pressuring banks and fintechs to absorb the fraud losses resulting from P2P scams, which are currently shouldered by consumers. This increased regulatory scrutiny has prompted institutions to look closely at their customers' identities and pinpoint potential risks.

FinCEN regulations are also seeking to tackle the issue of synthetic identities and their role in the financial crime ecosystem. Changes are expected to better detect synthetics at onboarding and throughout the Anti-Money Laundering (AML) lifecycle. Additionally, the CFPB has signaled that "the receiving bank" will be liable for the loss in P2P scams if they pass new regulations.



Growing synthetic identity fraud

According to the U.S. Department of Justice, synthetic identity fraud is the fastest-growing financial crime, with fraudsters often using fake Social Security numbers (SSN) to obtain loans and credit cards. In fact, the Pandemic Response Accountability Committee traced \$5.4 billion in COVID-19 relief funds back to synthetic identities using fake SSNs that were disbursed to applicants between April 2020 and October 2022.

\$1,000

Average loss per P2P scam, according to the FTC's Sentinel Report

1%

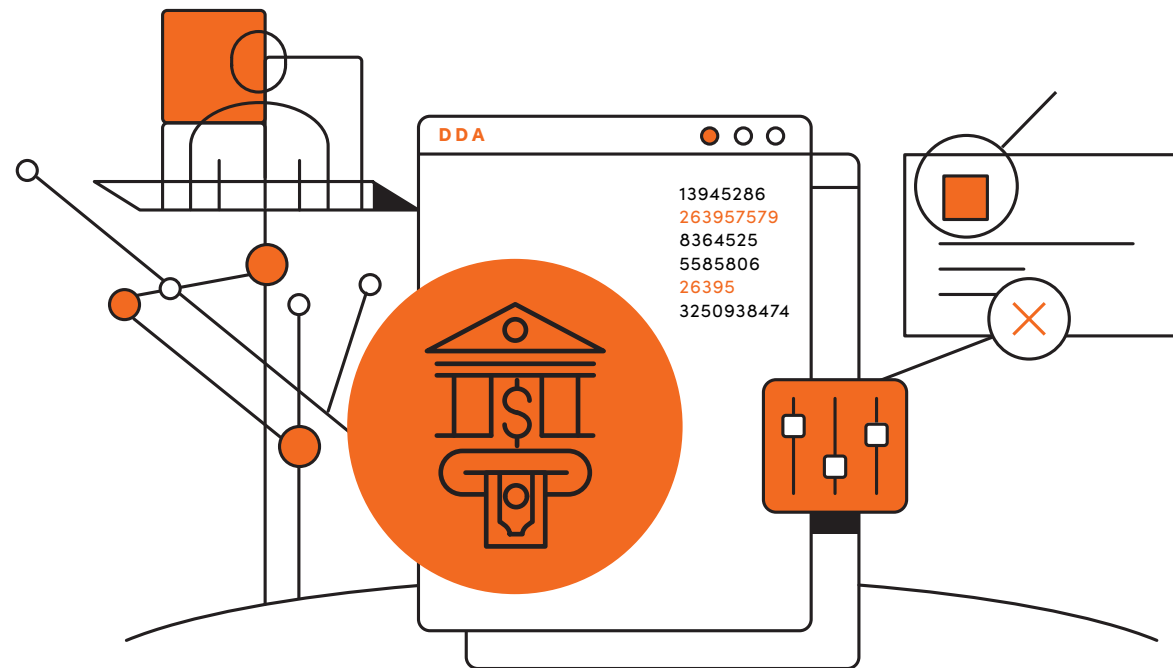
Average rate of synthetic identities in deposit accounts

**\$2.8M
to \$4.8M**

The CFPB proposal could double the financial loss of synthetic fraud per year

Socure analysis shows that synthetic fraud has shifted drastically, especially in deposit accounts, where synthetic identities are the new “money mules.” Assuming an average loss of \$1,000 per P2P scam, per the FTC’s Sentinel Report, and a conservative average rate of 1% synthetic identities in deposit accounts, the CFPB proposal alone could almost double the financial loss of synthetic fraud, from \$2.8 million per year to \$4.8 million, almost overnight.

Responsible lenders must take a deep look at the consumer identities of account holders to identify financial and compliance risks before the potential reality of a changing regulatory and economic landscape puts them at risk.



Who's in your current book of business...

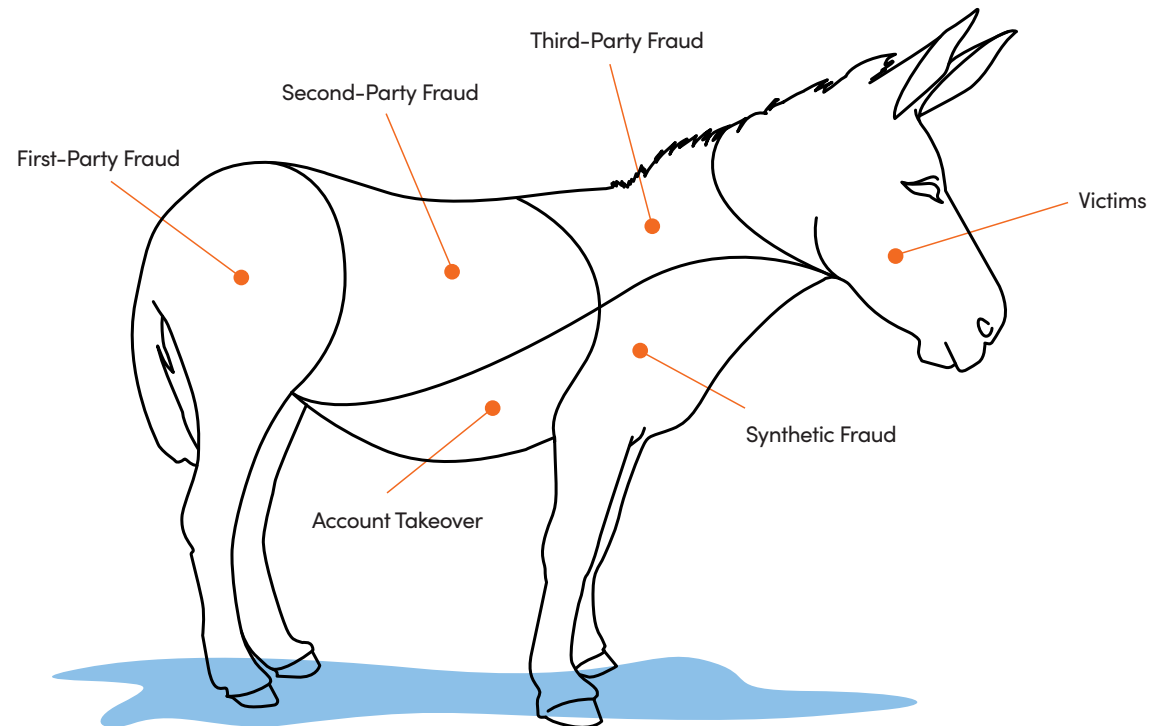
...and what are they doing there?

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.

Deposits, investments, and savings accounts are frequently used by fraudsters as money mules. The fraudsters can use either real people who are unaware of the scam, or synthetic identities created using stolen or fabricated information. Synthetic identities are particularly challenging to detect because they often have valid personal identifiable information. Fraudsters can use synthetic identities to open bank accounts, apply for loans or credit, and conduct other financial transactions.



.....
It is crucial for financial institutions to identify and prevent money mule activities to protect themselves and their customers.
.....



How do money mules slip through fraud controls?



Customer identification program (CIP)

Banks use CIP programs, which are designed to verify the identity of the individual opening the account. However, this approach does not always detect synthetic identities because fraudsters use a combination of real and fabricated information, making it difficult to distinguish them from legitimate customers. Additionally, synthetic identities are developed and strengthened at the credit reporting agencies, whose data is used to drive the majority of CIP solution offerings. Additionally, synthetic identities are developed and strengthened at the credit reporting agencies, whose data is used to drive the majority of CIP solution offerings.



Account takeover

Fraudsters use this tactic to turn an account into a money mule. In this scenario, the fraudster gains access to an existing account and changes the account details to use it as a money mule. This approach is challenging to detect because the account's legitimate owner may not be aware of the fraudulent until it's too late and often, banks and fintechs may not be as rigorous as they should be when updating non-monetary changes to PII of an account.



Third-party fraud

In this case, fraudsters open up accounts using some form of a true consumer's identity. These attempts can be detected by a sophisticated solution like Socure's Sigma Identity model, but can slip through weaker defenses and ultimately become a money mule operating with your portfolio.



First- and second-party fraud

Real consumers can knowingly participate in the scam, either alone acting as a first party, or teaming up with bad actors and actively participating in the scam, often called second-party fraud. Because these users are the real consumers, they are almost impossible to detect.



Victims

Unfortunately, real consumers can unknowingly fuel fraudulent money movement without their knowledge.

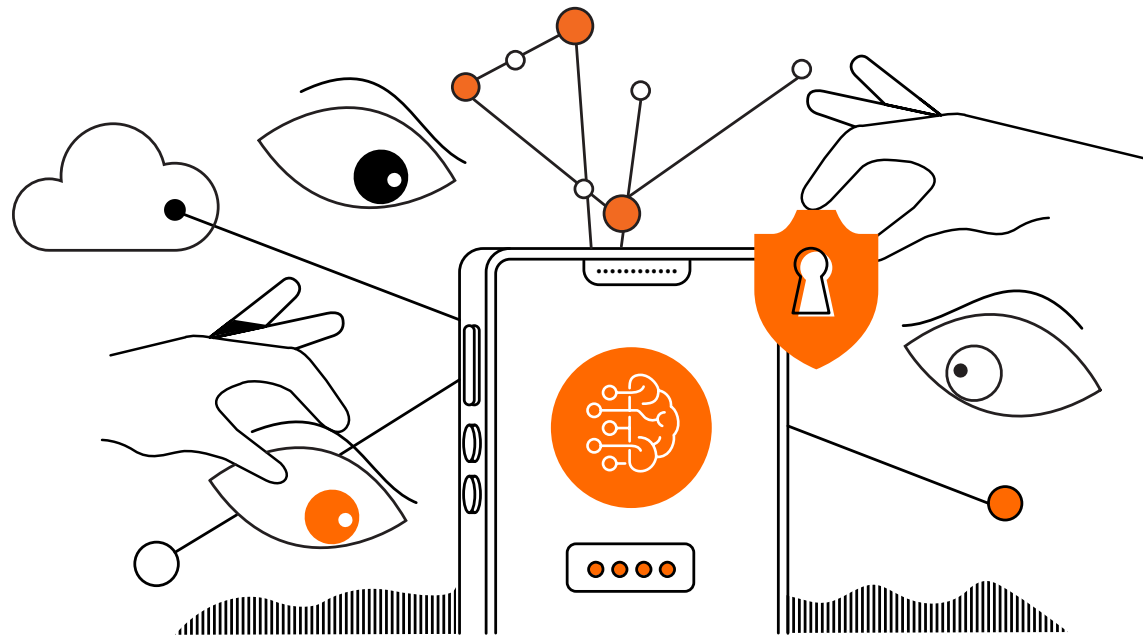
To address these issues, financial institutions must have strong behavioral and identity fraud prevention measures in place.

Institutions should, and often do, regularly review their account activity to identify unusual patterns or suspicious transactions. These reviews should include an assessment of the customer's behavior, such as whether they are frequently transferring money to unknown individuals or entities.

Financial institutions should also employ advanced fraud detection technologies at point-of-origination and on all non-monetary changes to a customer's contact elements, such as address, email, and phone number. By combining an identity-centric approach with traditional account behavioral analysis, banks and fintechs can super fuel their abilities to identify fraudulent money mules operating within open active accounts.



.....
Financial institutions should employ advanced fraud detection technologies at point-of-origination and on all non-monetary changes to a customer's contact elements.
.....



Money mules aren't always a top concern — but they should be.



.....
 By using money mules, fraudsters can move illicit funds more easily and avoid detection.

Money mules may not always be at the top of the list for financial institutions when it comes to fraud, but they are a growing threat that can have a significant negative impact.

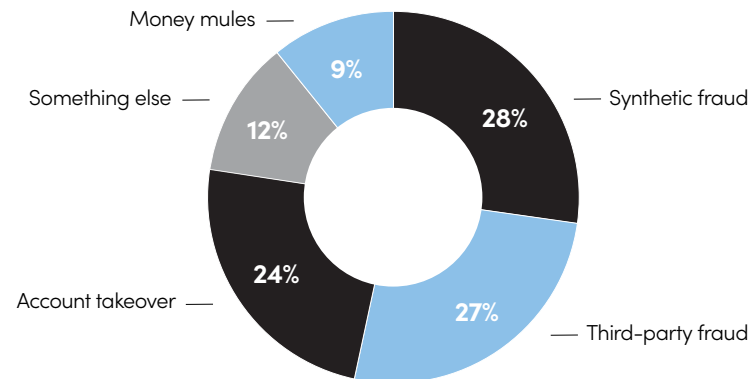
Synthetic identities are often used as a screen for fraudulent activity or other illegal transactions, including human and drug trafficking. Synthetic identities are also frequently used to obfuscate the source of funds for money laundering purposes. By using money mules, fraudsters can move illicit funds more easily and avoid detection.

The use of money mules can cause significant financial loss and compliance penalties for banks, savings and investment entities, and other businesses. Not only can these activities harm an organization's reputation, but they can also result in regulatory scrutiny and potential fines.

Research by Socure suggests that between 1 to 3% or more of deposit accounts may be held by synthetic identities, and fraudsters are increasingly targeting deposit institutions.

Socure polled more than 750 fraud operations and strategy managers, and concern for money mules was at the bottom of the list.

Q: What was the biggest fraud concern in 2023-2024 for your organization?



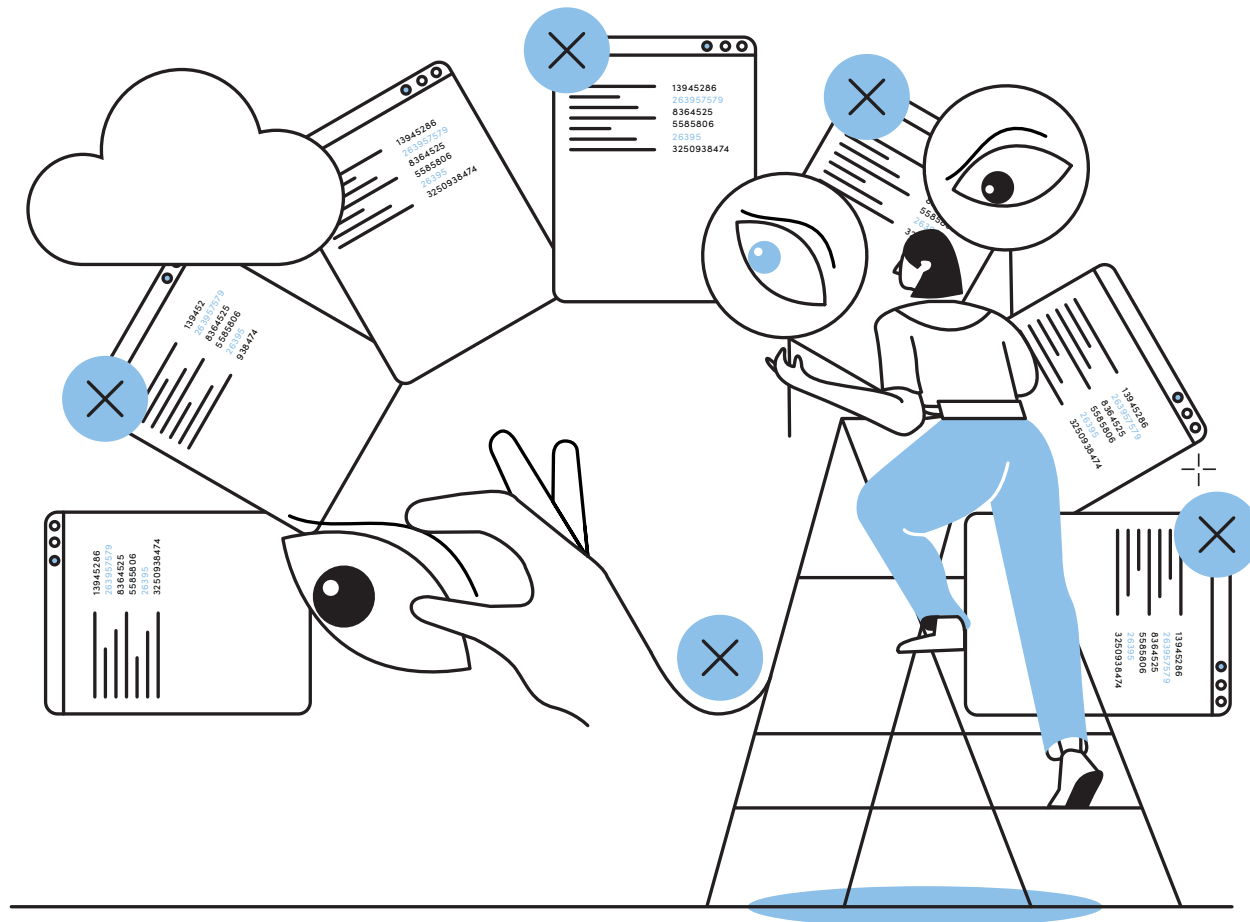
Ready to fight back against money mules?

It's time to scrub your portfolio.

Undertaking a portfolio scrub will identify and eliminate synthetic identities that have already been approved and exist within your customer portfolio.



Institutions should regularly review account activity to identify unusual patterns or suspicious transactions.



Fraud detection is a complex task, and few organizations do a good job of labeling it.

It is both an art and a science to accurately identify and prevent fraudulent behavior. Fraudsters are always evolving their tactics and strategies, which means that fraud detection models must also evolve in order to stay ahead of them.



.....
A portfolio scrub is especially important in light of proposed regulations that could make organizations liable for P2P fraud losses.
.....



Socure's synthetic fraud models leverage machine learning, predictive analytics, and expert fraud investigators to identify patterns of fraudulent behavior associated with synthetic identities.



These models are trained on a massive amount of data, including identity data, financial transaction data, and behavioral data, in order to accurately detect and prevent fraudulent activity.



Socure's Portfolio Scrub solution takes this one step further by applying these models to an organization's existing customer portfolio, helping to identify and eliminate synthetics from the account systems before they can cause more damage.

A portfolio scrub is especially important in light of proposed regulations that could make organizations liable for P2P fraud losses. This means that organizations must take proactive steps to identify and eliminate money mule accounts from their systems to prevent future financial loss and compliance penalties.

Rooting out 100,000 synthetic identities in 2023.

Identifying and eliminating synthetic identities from your portfolio can help reduce the amount of scams perpetrated by bad actors against consumers. With fewer places to receive and send fraudulently earned dollars, fraudsters will have a harder time carrying out these scams.

Of course, identifying and eliminating synthetics from your portfolio is only one part of the solution. **Organizations must also prevent synthetics from entering their ecosystem in the first place.** This requires a comprehensive fraud detection and prevention strategy that includes both proactive and reactive measures.

Proactive measures such as verifying identity information at account origination, analyzing behavioral patterns to detect anomalies, and leveraging third-party data sources to supplement internal data can help stop synthetic identities at the door. Reactive measures such as real-time transaction monitoring, manual reviews of flagged transactions, and reporting suspicious activity to law enforcement can spot fraud in your existing portfolio.

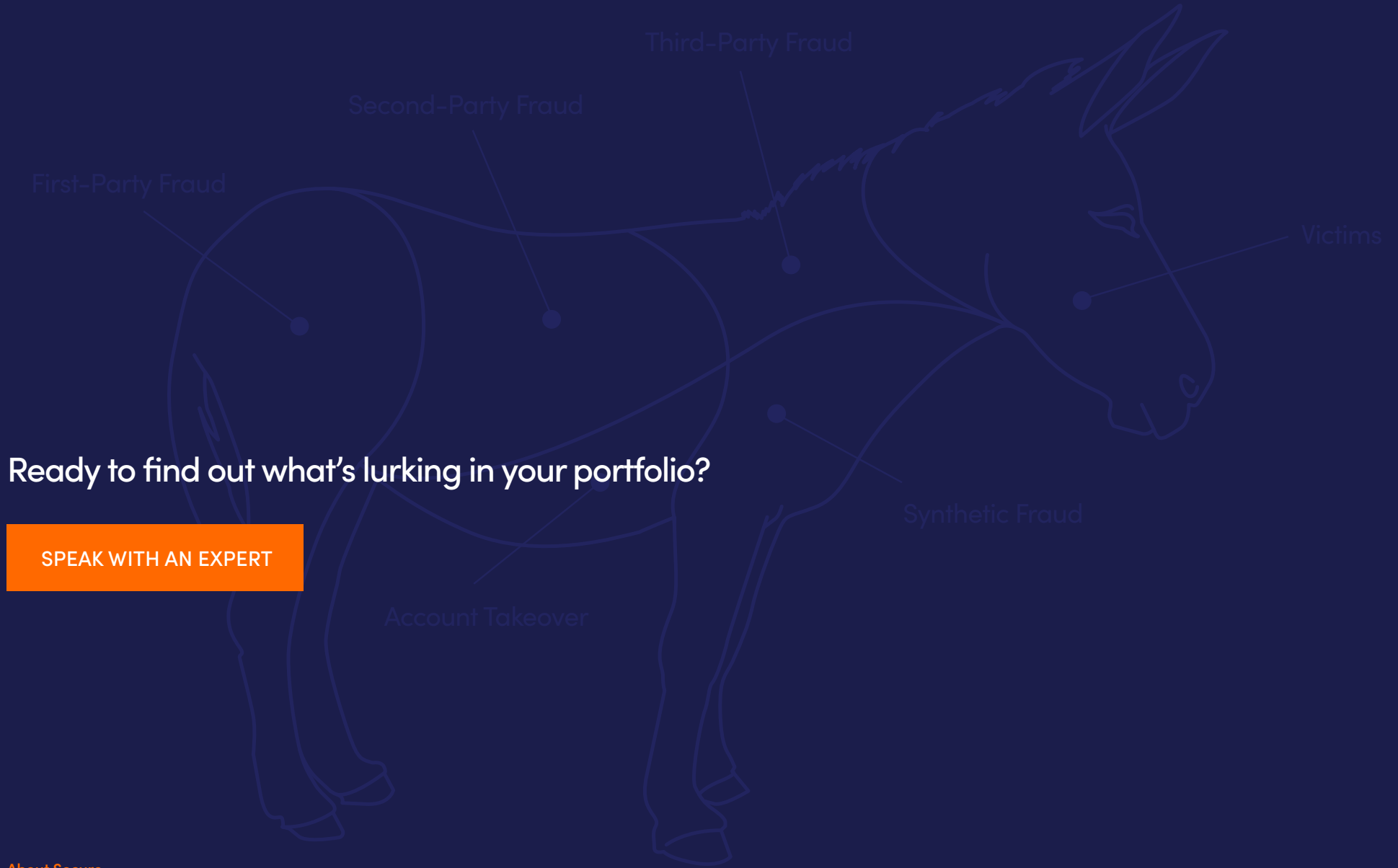
As a result of the subsequent uptick in synthetic identity fraud following the global pandemic, Socure has taken a public stand to eliminate, track, and report on the progress of reducing fraud in the U.S. financial system. **Socure is committed to rooting out 100,000 synthetic identities in 2023**, as part of its larger action plan for eradicating synthetic fraud.

Money mules are a hidden risk that organizations must address, but that's only one part of a comprehensive fraud detection and prevention strategy. By taking these proactive steps to prevent synthetics from entering your ecosystem in the first place, organizations can protect their customers, bottom line, and reputation



.....
By preventing losses and compliance penalties, organizations can protect their brand reputation and maintain customer trust.
.....





Ready to find out what's lurking in your portfolio?

[SPEAK WITH AN EXPERT](#)

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 1,800 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.