Socure™

REPORT

# The State of Synthetic Fraud: Evolution, Trends, and How We Will Eradicate It By 2026

# Contents

# Executive Summary

Their methods vary. Some combine stolen, but real, personally identifiable information (PII) with completely fake credentials to create a fictitious person, known as a fabricated synthetic identity, in order to commit financial crime. Others tumble their own PII and combine it with fake data to create a fictitious person, known as a manipulated synthetic identity, to hide poor credit histories or criminal backgrounds.

Whatever method bad actors employ to create synthetic identities, synthetic identity fraud has become the fastest growing type of financial crime in the US according to the U.S. Department of Justice. FinCEN calls synthetic identity fraud a national security priority because of its potential to be used for cyber attacks, anti-money laundering, and terrorist funding.

This report explains the evolution of synthetic identity fraud, analyzes methods being used to perpetrate it, identifies trends in synthetic identity activity including impacts from COVID and follow-on stimulus efforts, and ultimately offers strategies for combating this rapidly growing threat and eventually eradicating the plague of synthetic fraud.

**Highlights:**

- How bad actors who create fabricated synthetic identities to fraudulently open accounts tend to use patterns of birth months, locations, and familiar names.
- Ways the early definitions of synthetic fraud have broadened to include manipulated synthetic fraud, which are consumer generated to hide a criminal past or poor credit history.
- The substantial shift in the behavior of synthetic fraud over the last 20 years away from instant gratification of fraudulently gained goods and credit bust-outs to the development of synthetic identities for money movement through synthetically created money mules.
- How synthetic fraudsters have gained a substantial foothold in banking and fintech DDA, savings, and investment accounts.
- The differing opinions in private commercial entities and public sector groups around the seriousness of synthetic identity fraud, and how we can move forward.
- How Socure research found that the global pandemic had a significant impact on the DDA and lending industries and that the second wave of PPP loans may have had more of an impact on the growth of synthetic fraud in investment accounts. Additionally, consumers hurt by the economic downturn increased their use of fraudulently manipulated identities to gain access to credit card and personal lending loans.

Synthetic fraud is no longer a surprise attack on America's financial and commerce systems. The problem has existed for over 20 years, and we in the industry and government sectors have allowed it to reach an alarming level.

There are now exceptional educational programs in place. The patterns of synthetic fraud are well understood and the profiles of manipulated and fabricated subtypes have been teased out, which will aid in stopping synthetic fraud during follow-on step-up efforts. When solution providers work with the industry to develop consortiums of reported synthetic fraud, we can drive incredibly precise models. These models have overcome many of the issues related to false positives and no longer add unnecessary friction to those younger consumers, the underbanked, and immigrants who have a light information footprint and therefore appear synthetic.

Socure strongly believes that, as an industry, working together with the government, we can eradicate the problem of synthetic fraud completely by 2026 and stop the damage that bad actors are committing against consumers and our financial system.

**We can eradicate the problem of synthetic fraud completely by 2026.**

# A Short History of Synthetic Identities

In early 2000, fraud investigators began to notice patterns in credit card applications where the Social Security number (SSN) of the applicant did not match the name to which it was issued. While there wasn't a proper name for it yet, fraud historians have cited secured credit cards as the first attack point for synthetic identity fraud, while others identified patterns of fake identities mainly in the unsecured credit card and telecommunications sectors.

But wherever it started, fake identities exploded onto the scene, and large numbers of fraudsters began opening new credit card accounts, which they used to quickly run up balances and then abandon before ever making a single payment. The vast majority of these charge-offs were written off as credit losses by the issuing banks. This scheme evolved as bad actors showed more patience by making on-time payments for the purchases made using the cards. They would then charge the card over the credit limit and "bust-out" (max out the card without ever paying another cent), which allowed them to amass fraudulent proceeds beyond the credit limit.

At the same time, mobile phones were being given away for free in the U.S. to consumers with long-term carrier commitments. Fraudsters realized they could steal one or two phones fairly easily with fully fake identities and then sell them in Europe for thousands of U.S. dollars. A byproduct of this type of fraud was that it enabled new fraudulent accounts to be opened using the original phone numbers of these stolen phones. Bad actors eventually learned how they could manufacture a fake small business or act as a sole proprietor, which could yield them dozens of phones with a single application and allow them to falsify identities at the same time.

In 2004, the term "synthetic" identity was coined. Later, the examples above would get a clearer definition: fabricated synthetic identities. These earliest fraudulent identities were completely fake, and many of the patterns used to establish synthetic identities 20 years ago are still being used today, including:

- Fake identities created using a stolen or even the fraudster's own SSN and date of birth (DOB) combination with a different name. Some employed tumbled SSNs, which allowed bad actors to create thousands of fake identities in a single day.
- Names involving the use of variations of first and surnames that were similarly spelled and then often switched first and last names.

**Bust-Out**

A credit-related fraud event where an individual applies for and gains a new account, establishes a normal usage pattern and repayment history, and then maxes out the available credit with no intention of repaying the balance.

Phone numbers, that were almost always mobile numbers as there were no voice-over-internet-protocol (VoIP) numbers at the time. Email addresses were rarely collected on originating applications.

For employment validation, which was a staple of credit issuance at the time, a work phone number was generally tied to a large organization, like a hospital, where employment verification involved a maze of extensions and was difficult to achieve and therefore not pursued with discipline.

Its origins may not have involved much fanfare, but synthetic identity fraud has plagued nearly every industry in every corner of the planet since it began.

## The emergence of manipulated synthetics and the meteoric rise of synthetic identity fraud

Manipulated synthetic identities were not detected in earnest until the mid-2010s. These identities are typically based on real people but created by transposing or tumbling one or more identity elements within their name, SSN, and/or DOB. The most common reasons for creating a manipulated synthetic identity are to bypass a bad credit history or hide from a criminal background.

Distinctive differentiators of manipulated synthetic identities include:

- A manipulated synthetic identity is based on the consumer's real identity, where he or she may use a true name and DOB combination with a "new" SSN, whereas a fabricated synthetic identity is completely made up.
- A manipulated synthetic identity may or may not have malicious intent to commit financial crime, whereas a fabricated identity always maintains intent to reap personal financial gain or move money fraudulently.
- A manipulated identity often collides with the true identity, which can make them easier to detect.


**Tumbled**

A synthetic fraud practice where an SSN number is manipulated repeatedly across numerous account applications and "tumbled" many times.

**A view into transposing or tumbling PII to form a manipulated synthetic identity:**

| Name | SSN | Date of Birth | |
|---|---|---|---|
| Jane Mary Doe | 123-45-6789 | 4/1/1985 | Real identity |
| Jane Mary Doe | 123-45-7689 | 4/1/1985 | Real name, real DOB, transposed SSN |
| Mary Jane Doe | 123-45-7689 | 4/1/1985 | First and middle name tumbled, real DOB, transposed SSN |
| Jane Doe | 124-35-7689 | 1/4/1985 | Middle name as first name, transposed DOB and SSN |

## The inadvertent impact of synthetic fraud on first-party fraud

First-party fraud, or the use of one's own true identity or parts of that identity to falsely apply for credit with the intent to commit fraud, occurs when an individual enters into a monetary agreement or exchange of goods and services with no intent to pay. This can include loan proceeds, auto financing, credit card purchases, account overdrafts, and more. When a customer refuses to pay or stops paying altogether, the account goes to collections and ends up being written off as a credit loss, which siphons bottom-line growth.

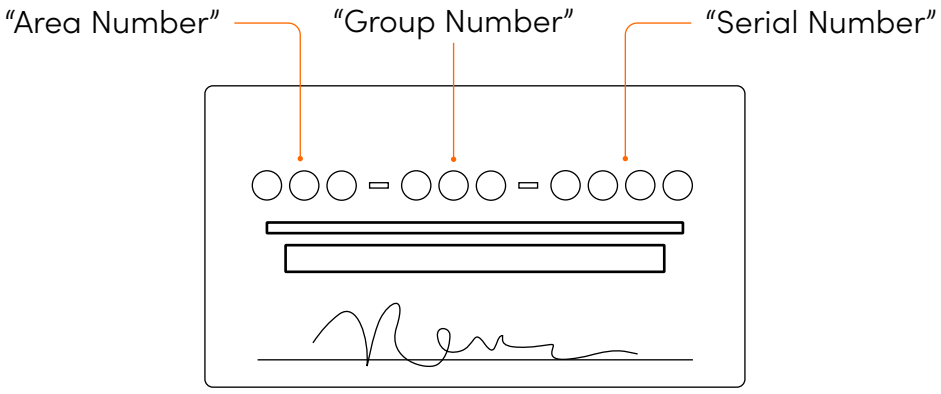
Because first-party fraud and manipulated identity fraud behave similarly, many organizations end up, often unwittingly, identity fraud as first-party fraud. This means the account goes to collections without the institution ever knowing about the fake identity. Money mule accounts — or when illegally acquired money is transferred between accounts on behalf of another person — often include synthetic identities and are often considered first-party fraud.

Detecting and blocking a synthetic identity earlier in the customer lifecycle, before they've even entered an organization's ecosystem, can vastly reduce organizational losses and prevent reputational damage. Curtailing this activity also means that resources unnecessarily tied up in collections can be reallocated to other strategic initiatives. Moreover, organizations can proactively prevent harm actively prevent harm, such as impersonator scams, from being inflicted on other consumers.

## SSNs: The broken foundation of synthetic identities

SSNs first emerged in 1936 for the purpose of tracking the earnings of U.S. workers and to determine Social Security eligibility and benefits. Since the board that developed the SSN controlled the issuance of the account numbers, which were to be distributed geographically, the group was in a position to also control which geography would use which numbers. Beginning with the first three numbers of the SSN, called the "area number," lower numbers were assigned to the Northeast and increased as they moved across the country to the Northwest.

The remaining SSN numbers also had meaning. The middle two numbers are the "group number" which ranged from 01 to 99 but are not assigned in consecutive order. For administrative reasons, group numbers first used the




ODD numbers from 01 through 09 and then EVEN numbers from 10 through 98, within each area number allocated to a given state. After all numbers in a group within a particular area have been issued, the EVEN numbers 02 through 08 are used, followed by ODD numbers 11 through 99.

The last four digits of the SSN are called the "serial number" and run consecutively from 0001 through 9999.

For more than 70 years, this numbering scheme held true until a research paper was published by Alessandro Acquisti and Ralph Gross in 2009 titled *Predicting Social Security numbers from public data*. In this paper, the authors showed that by combining publicly available data about a consumer's identity with the Social Security Administration's (SSA) SSN range tables, a person could guess another person's SSN within a relative distance.

The study's authors discovered: "With just 10 or fewer attempts per target, the inquiries associated with 9.2% of all SSNs issued after 1988 could be accepted as valid by Credit Reporting Agencies (CRAs) and 29.1% of those issued in the 25 states with fewer births."

The researchers used the CRAs as proving ground for their analysis because CRAs allowed a two-digit differential in the accuracy of an SSN to match consumer records, plus the SSN was the identifier used most often to determine creditworthiness, even though it was never intended to be used that way.

This is the regression model used by Acquisti and Gross to predict the SSN value for individuals who came from the Death Master File (DMF) and had died between January, 1973 and December, 2003:

$$SN_i = \alpha + \beta_1 dd_{i,vw} + \beta_2 ANGN_{i,vw} + \varepsilon_{i,vw}$$

**Detecting and blocking a synthetic identity earlier in the customer lifecycle, before they've even entered an organization's ecosystem, can vastly reduce organizational losses and prevent reputational damage.**

It was due to the Acquisti and Gross research that the SSA began to rethink how randomly assigned numbers would help to protect the integrity of the SSN. It also recognized that by changing the assignment methodology, the SSA would benefit from a more extensive pool of nine-digit SSNs.

The new assignment methodology launched on June 25, 2011. These numbers are now known as "randomized" SSNs.

At first, this "randomized" structure created trouble for bad actors who needed SSNs to commit fraud because the random range was easy to spot and few SSNs had been issued.

Over time, more randomized SSNs were generated for newborn Americans and the growing immigrant population. Today, it's common to see a randomly-generated SSN on a credit application, making it more difficult to recognize fake identities from real ones. Bad actors take advantage of this and now often use randomized SSNs to create synthetic identities.

## Lack of definition

The first step to addressing any problem is to define it. For more than 20 years, synthetic identity fraud lacked a common definition. This led the Federal Reserve System to create a group of industry fraud experts to develop a standardized definition to allow banks and other organizations to identify, classify, and combat this complex, widespread issue.

In 2021, the Boston Federal Reserve announced an agreed-upon definition of synthetic identity fraud to improve its detection, measurement, and mitigation across the industry in a similar manner: **"Use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain."**

The definition also includes primary and supplemental elements, including:

**Primary elements** – Identity elements that are, in combination, typically unique to an individual or profile (for example, name, date of birth, SSN, and other government-issued identifiers).

**Supplemental elements** – Elements that can help substantiate or enhance the validity of an identity but cannot establish an identity by themselves (for example, mailing or billing address, phone number, email address, or digital footprint).

**Synthetic Fraud**

Use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

The Federal Reserve also included two subtypes of synthetic identity fraud in their definition that are discussed in this report, fabricated and manipulated.

## eCBSV to the rescue?

In 2020, the Social Security Administration (SSA) launched the Electronic Consent-Based Verification Service (eCBSV.) eCBSV allows permitted entities to verify if an individual's SSN, name, and DOB combination matches Social Security records.

While eCBSV has helped individual consumers get needed access to financial inancial services — including new-to-country immigrants or those with thin-file credit histories — it has not been the "magic bullet" to ensure that bad actors don't use stolen SSNs, and it's not the answer to eradicating synthetic identity fraud.

Simply put, eCBSV provides a "yes" or "no" response to whether a submitted name (first initial and last name), DOB, and SSN combination matches the information in the SSA's Numerical Identification System, or "Numident," the source of truth for Social Security records. This means that if a submission doesn't provide the name exactly as it appears on Numident, and contains a typographical error or a name with a different first initial, the system will reject the inquiry—which could mean rejection of legitimate, or "good," customers.

**eCBSV**

**A fee-based Social Security number (SSN) verification service operated by the Social Security Administration. eCBSV allows permitted entities to verify if an individual's SSN, name, and date of birth combination matches Social Security records.**

# Here Come the Synthetic Profiles

## Who is Michael Smith?

What does the "average" synthetic identity profile look like? Socure wondered that too, so our engineers and data scientists looked at years of tagged synthetic fraud data to identify patterns by name, demographics, habits, location, and other behaviors to help guide organizations in identifying and combating synthetic fraud. While fraud can be managed by deploying a synthetic-specific solution, we want to help companies become more knowledgeable about the foundation of this complex fraud so they can understand both the myriad ways it can be perpetrated and the potential economic and customer benefit when it is managed effectively.

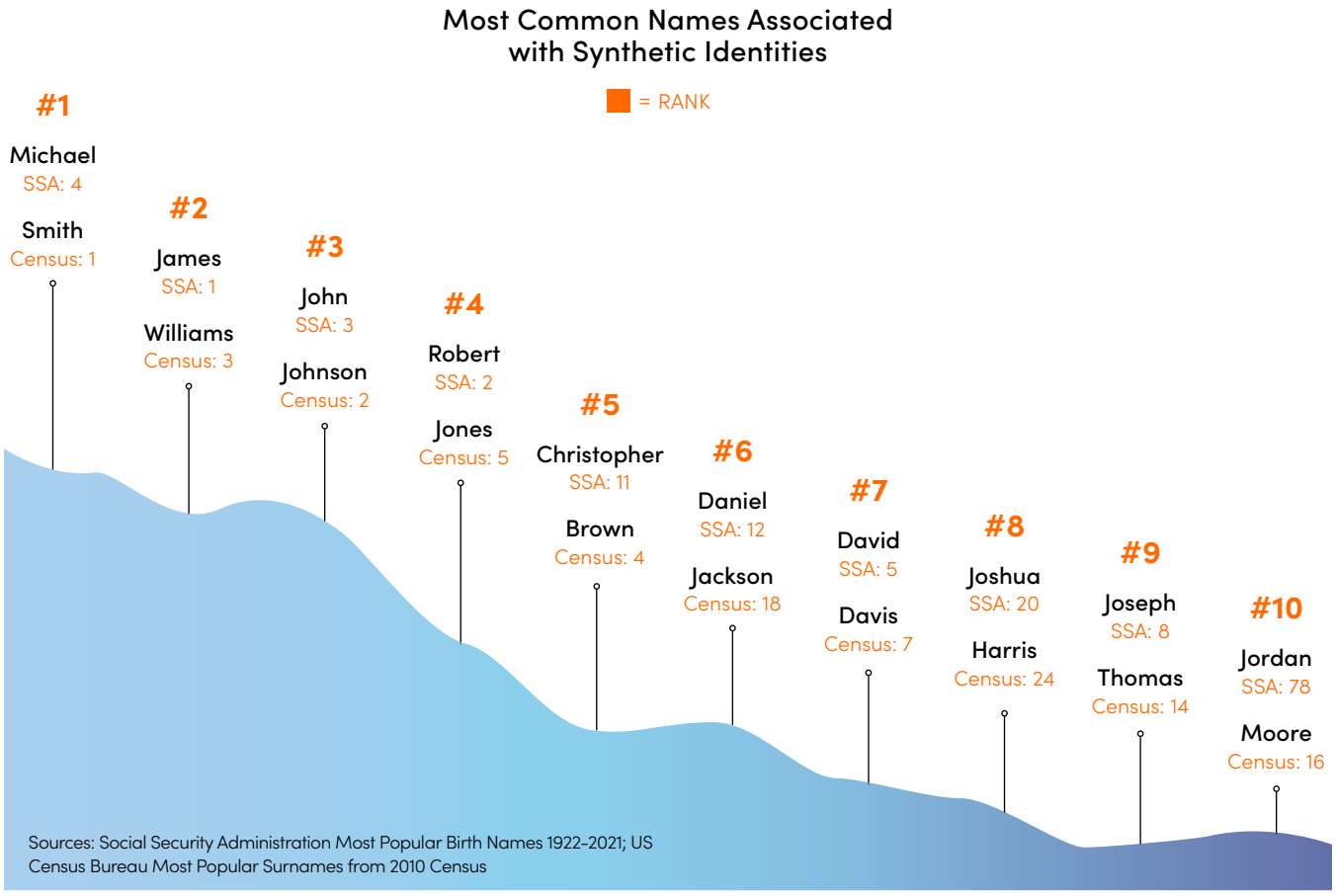
Fraudsters have always been shrewd and crafty, and the data confirms it. It turns out that by analyzing the patterns for first names and surnames, we see very common choices, which leads us to believe that bad actors are strategically creating fabricated synthetic identities to blend in with the population.

In particular, the top four first names used in synthetic identities follow the top four first names in the SSA's list of the most popular birth names in the last 100 years—although not in rank order. The remaining top 10 first names all rank in the top 20, with one exception.

When looking at surnames, the top five most used synthetic surnames follow the top five surnames in the U.S. Census Bureau's ranking of popular surnames from the 2010 Census—also not in rank order. The remainder of the top 10 surnames all rank in the top 25.

When combining the most popular first name and surname for synthetic identities, we establish the most common full name for synthetic identities: Michael Smith.

**The top four first names used in synthetic identities follow the top four first names in the SSA's list of the most popular birth names in the last hundred years.**



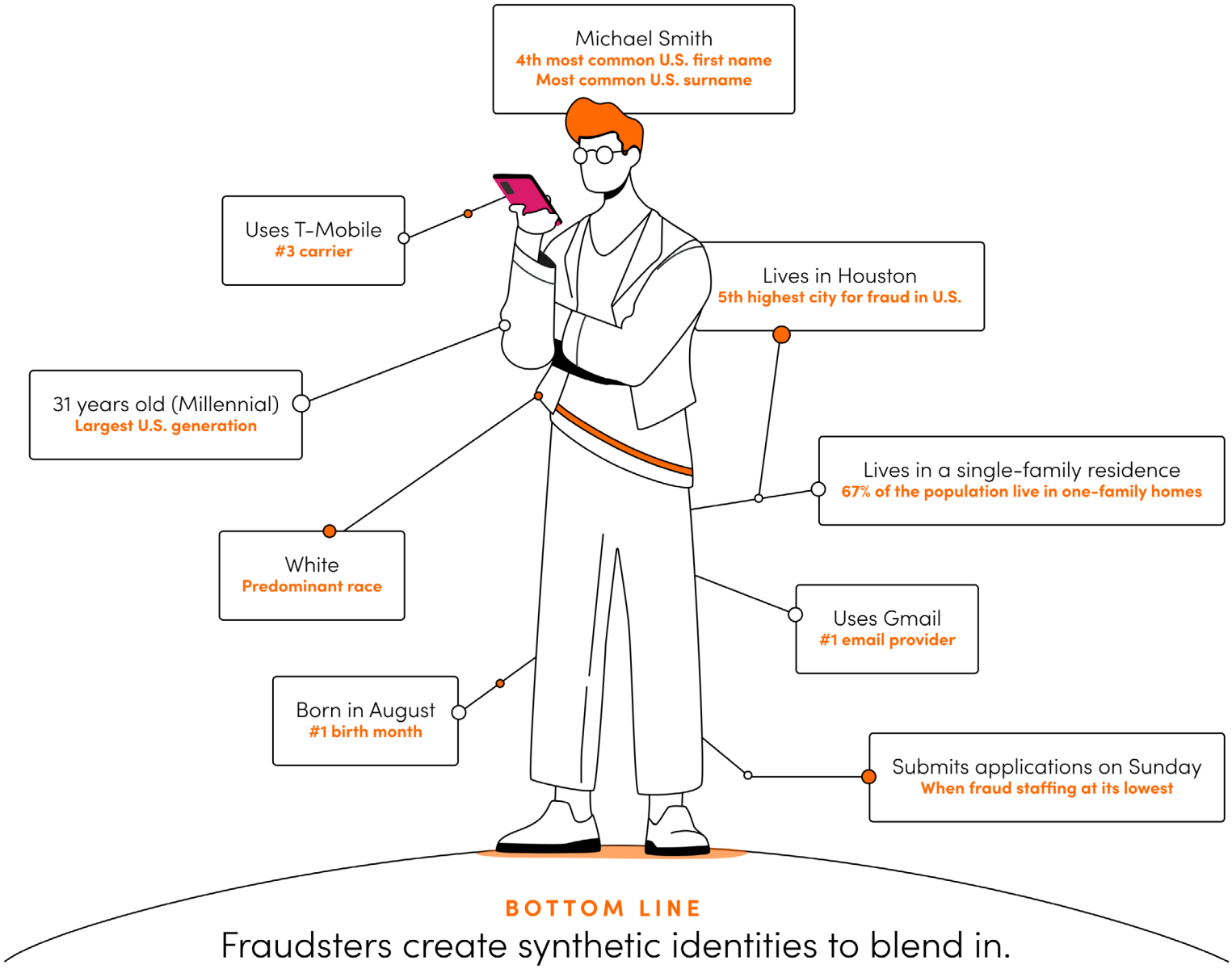

The question becomes: How many Michael Smiths does the average portfolio contain as opposed to any other name? Any of these combinations could be suspicious:

- Michael Williams
- Michael Johnson
- Michael Jones
- James Smith
- James Williams
- James Johnson
- James Jones
- John Smith
- John Williams
- John Johnson
- John Jones
- Robert Smith
- Robert Williams
- Robert Johnson
- Robert Jones

The goal to "blend in" doesn't end with names. It's a trait shared by the remainder of patterns tied to these fabricated synthetic identities as well. Age, location, residence, and other elements all follow very common sequences.

In every case, the choices being made to create synthetic identities fall into the most common demographics and consumer traits, even selecting Sunday as the day of the week to submit applications because it's known to be the day when fraud staffing is at its lowest.

Knowing that bad actors are using automated technology to supercharge their fraudulent activity, it's not a stretch to presume that their software has been programmed with these popular elements to mix and match traits to create synthetic identities.




**BOTTOM LINE**

Fraudsters create synthetic identities to blend in.

# Synthetic Identity Fraud Today

The problem of synthetic fraud will not go away on its own. Quite the opposite – it is exhibiting shifting patterns and increasing in scope.

## Shifting patterns

As we discussed previously in this paper, in the early days of synthetic fraud, the attack patterns and the fraudsters' motives were transparent: fast money. Credit cards and mobile phones were the prize, and bad actors created fabricated synthetic identities which could clear identity verification and fraud checks and get a quick payout by either running up the card balance or fraudulently gaining access to mobile phones that could be resold overseas for fast profit.

After a few years, synthetic fraudsters realized they could double down on their efforts by "busting out" on the card balance. A "bust-out" occurs when an individual gains a new credit account, establishes a normal usage pattern and repayment history, and then maxes out the available credit with no intention of repaying the balance. By doing that, bad actors realized higher profit by taking the card issuer for losses above the set credit limit. It also allowed them to act as a small business and dupe mobile operators for more than a single phone, sometimes stealing dozens with a single synthetic identity.

**While these past patterns sound sinister, the more recent pattern shifts are even more chilling.**

The long-held opinion by many industry professionals has been that deposit accounts—outside the credit card, mobile device, and auto financing segments—were fairly safe from synthetic fraud attacks. However, that has been proven to be wrong over time.

At some point between 2010 and 2020, bad actors began attacking demand deposit accounts (DDAs), traditional savings accounts, and investment accounts more aggressively using synthetic identities. The recent rise in fraud within these types of bank accounts is driven because synthetic identities are a key element in transnational criminal organizations and those identities facilitate money laundering and financial crimes that are the predicate source of funds. This is the reason why synthetic identities have become of such high importance to FinCEN and regulators.

**Attack Rate**

**The rate at which a company is attacked by fraud. This rate is measured using scores or rules as a proxy.**

According to Socure analysis comparing industries with the highest attack rates, retail banks and fintechs offering checking, savings, and investment accounts made up 49.4% of the grouping of customers who see the highest attack rates. That means, of the specific lending and servicing companies tested spanning across all types of industries, banks and fintech, DDA accounts were attacked substantially more than any other industry tested. Why? Two significant reasons stand out:

1. **It's easy, unfortunately.**

   Almost without exception, businesses are driven by making a return on investment (ROI) on the dollars they spend for goods and services, and this holds true in banking as well. However, when evaluating outside vendor solutions to help stop synthetic identity fraud from entering their banking ecosystem, the math is completely wrong.

   To evaluate ROI for a potential vendor solution, an organization needs two numbers:

   - The value of a "good" account to the organization.
   - The cost of a "bad" account to the organization.

   By applying those numbers to a false positive rate generated by an analytical model, the organization can determine how much unnecessary friction would be caused to potentially good and profitable customers in the effort to identify and stop a fraudulent account from entering the bank's ecosystem. While adding friction to a potential fraudulent transaction is the right thing to do, adding friction to a "good" applicant will slow down the application process and create a risk that dropoff may occur.

   Today, the annual value of a good banking customer is roughly the same as the negative cost of a fraudulent account: roughly $250 to $400, depending on the banking or fintech organization. Here's where the math is wrong: the downside cost of a fraudulent account doesn't consider the financial losses to consumers from impersonator scams and peer-to-peer (P2P) scams, nor the enforcement fines from regulators due to nefarious activities like money laundering, human and drug trafficking, and terrorism.

**Good Account**

A bank account which has been established by a legitimate consumer.

**Bad Account**

A bank account which has been established fraudulently by a bad actor under false pretenses.

**False Positive**

A false positive means that a person has been flagged falsely as suspicious. False positive rate is calculated as the ratio between the number of negative events wrongly categorized as positive and the total number of actual negative events, regardless of classification.

To add to the problem, many bank executives believe that their customer identification program (CIP) will identify fake identities. Unfortunately this is not true, as most CIP programs use credit header data solely as the "authoritative" source to fulfill CIP requirements. Synthetic identities are alive and well.

While the Consumer Financial Protection Bureau (CFPB) and other agencies are considering shifting liability from consumers who are defrauded through P2P and impersonation scams to the receiving bank to absorb the losses, today this statement remains true: ROI is computed in such a way to disincentivize bank and fintech organizations that offer DDAs from preventing synthetic fraud from entering the front door.

2 **It allows synthetic fraudsters to use the fake identities they create as scapegoats and money mules.**

The pace of money movement has never been faster, and that's an advantage for synthetic fraudsters. With the push for FedNow and widespread consumer adoption of real-time funding platforms like Zelle, where money is sent and the account is funded in real-time, the demand for and use of instant payments will only continue to speed up.

The upside for fraudsters is that they bear little liability of being captured because accounts are easy to establish using synthetic identities. Further, bad actors employing this scheme have also discovered they can significantly scale using synthetic identities as money mules. It's a lucrative business model, since they don't have to pay outsiders to be involved.

The most alarming dynamic here is that organizations are keenly unaware of this shifting landscape. Socure polled recent webinar attendees in both the public and private sectors about their concerns related to different types of fraud. The results are reported in the table below. Synthetic fraud is of greater concern to the private sector than the public sector and ranks as the top choice. Three other types of fraud outrank synthetic fraud with the public sector group. Most critical, however, was that neither group is very concerned about money mules.

**Friction**

Any unnecessary effort, incremental step, or inconvenience that significantly slows a consumer's action or leads them to consider abandoning an application or transaction. Judicious use of friction can serve the purpose of confirming that an applicant or account holder is who they claim to be.

**Money Mule**

Someone who transfers or moves illegally acquired money on behalf of another person, in order to make the ill-gotten funds harder to trace.

**FedNow**

Enables individuals and businesses to send instant payments through their depository institution accounts.

Money mules, which are often synthetic identities, are used to perpetrate financial crimes against consumers, the US government, and other organizations and are acting as the high- speed tracks to move ill gotten gains.

| Greatest Concern | Private Sector | Public Sector |
|---|---|---|
| Synthetic fraud | 33% | 11% |
| Money mules | 10% | 2% |
| Third-party Fraud | 24% | 43% |
| Account takeover | 23% | 28% |
| Something else | 10% | 16% |

October 2022

## Synthetic fraud losses will more than double previous reports in the coming years

Federal Deposit Insurance Corporation (FDIC) research indicates there are 124 million U.S. households with at least one bank account. By analyzing transaction data, Socure estimates that synthetic identities make up between 1-3% of financial institution and fintech DDAs. Assuming one account per household (an ultra-conservative estimate) from the FDIC data and that 2% of those accounts were established by synthetic fraudsters, that means there are **more than 2.48 million synthetic identities hiding in open U.S. bank accounts currently.**

One of the most common types of synthetic identity fraud comes in the form of P2P scams. The 2022 FTC Sentinel Data report shows that scams are up substantially; consumers report more than $2.7 billion in losses last year due to imposter scams, up from $2.4 billion in 2021. The median loss per imposter scam is $1,000, according to the FTC. Multiplying that rate by 2.48 million bank accounts hiding synthetic identities drives a total loss for DDAs of $2.48 billion, should the CFPB and others make those organizations responsible for the loss instead of consumers.

There are over **2.48 million synthetic identities** hiding in open US bank accounts currently.

Synthetic fraud not only creates losses with DDAs but is also a big problem for the credit card sector. Aite-Novarica Group, an advisory firm to banks, insurers, payments providers, and investment firms, reports that synthetic fraud in the unsecured credit card sector for 2022 is estimated at $2.4 billion. To date, Aite-Novarica's numbers have been the industry's sole barometer for synthetic fraud. However, by combining the Aite-Novarica credit card losses of $2.4 billion and the $2.48 billion loss estimate for DDAs, **it bumps total synthetic losses to $4.88 billion—more than double the gauge commonly used by the industry.**

To be clear, this total includes the expected increase to synthetic fraud losses associated with just DDAs and unsecured credit cards. Once we are able to study the investments, lending, and other sectors more closely, we anticipate this estimated figure will climb.

**$4.88B**

Estimated combined losses from synthetic fraud in 2022

# COVID-19 Drastically Increased Synthetic Fraud

To understand the impacts that COVID-19 and follow-on unemployment and stimulus programs may have had on synthetic fraud growth, Socure's data scientists studied longitudinal data for attempted synthetic fraud account opening for 2020 through 2021. We looked at applications from a consistent set of companies across DDA, investment, lending, and credit card sectors and used Socure's highly precise fraud score as a proxy for synthetic account opening attempts.

Beyond account openings, the data reveals shifting patterns around how fraudsters attempting to open those accounts intended to deploy manipulated and fabricated identities and the underlying signals divulged by the application data over the two-year analysis.

**We found that the global pandemic had a significant impact on the DDA and lending industries and that the second wave of Paycheck Protection Program (PPP) loans may have had more of an impact on the growth of synthetic fraud in investment accounts.** The credit card industry did not see much of a noticeable spike from COVID-19, although there was indeed an increase over time.

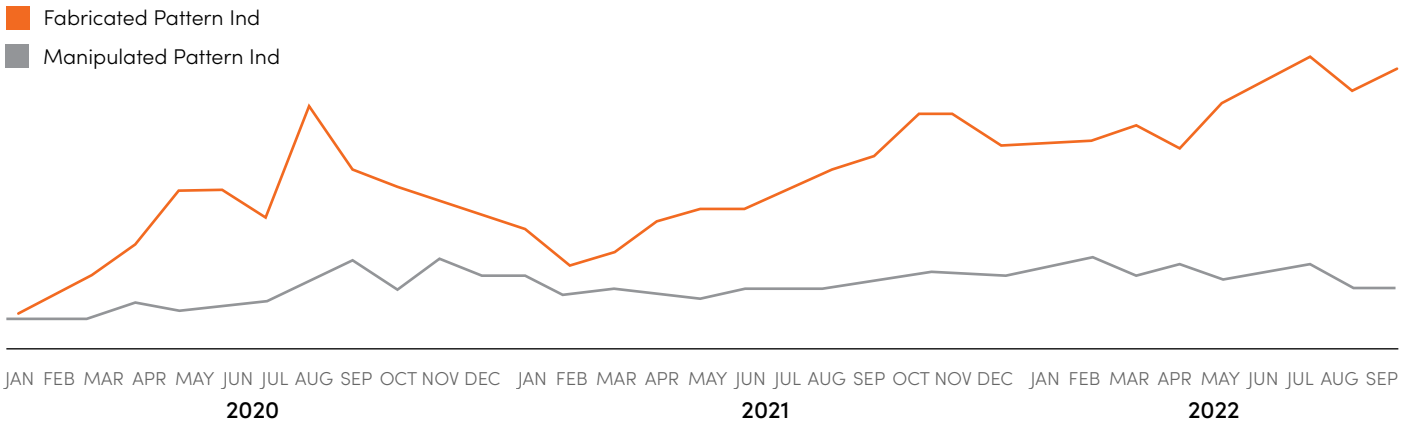
Among the industries we researched, DDA had the earliest increases in synthetic fraud attempts following COVID-19, and we saw a sharp spike in fraudulent account opening attempts from March 2020 to November 2020 (see graph A below.) The spike came from fabricated synthetic fraud types beginning in March 2020 and climbed substantially to their peak in August 2020. While there was a decline in fabricated synthetic fraud from August 2020 to February 2021, we saw another sharp and steady climb to September 2022, where the increase continues.

From the graph of DDA synthetic fraud attempts during the same time period, the data also shows that the number of manipulated synthetic fraud attempts during the test period remained fairly flat, with some increase beginning after July 2020.

This supports our suggestion that synthetic "DDA" accounts are mainly opened by fraudsters creating completely fake or fabricated identities in an attempt to establish money mule accounts to carry out nefarious money movement activities.

GRAPH A

**DDA SYNTHETIC FRAUD ATTEMPTS**

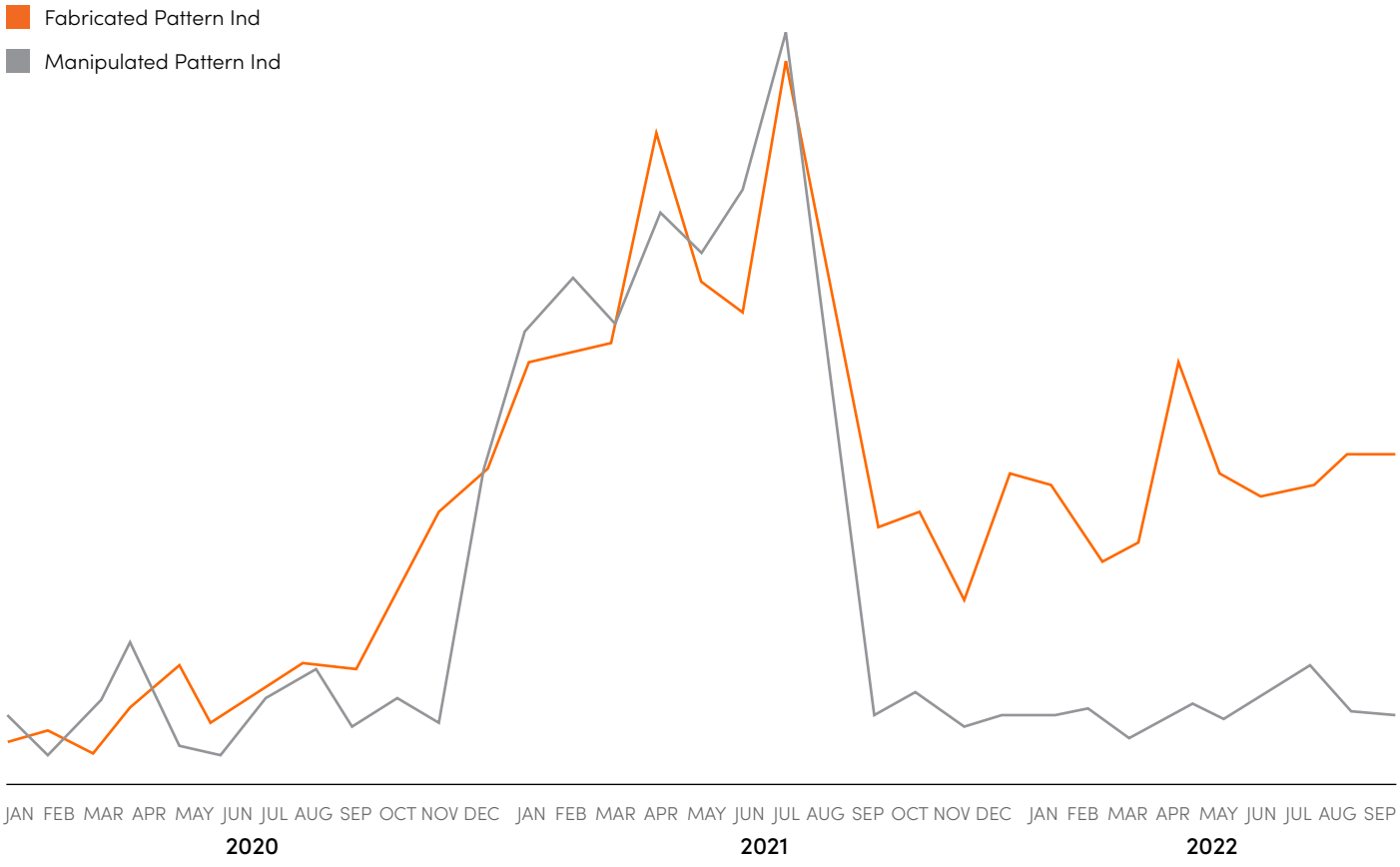


Synthetic fraud attacks to lending portfolios acted similarly to fraudulent DDA account opening efforts. Graph B below, shows a slightly later beginning to the peak of fraudulent synthetic account opening efforts in lending products, with the growth in attempts starting in July 2020.

There are two sizable differences when comparing the synthetic fraud attempts to DDA. First, the peak is substantially higher and grows at a much sharper rate than the spikes in DDA. We believe this spike in fraudulent attempts to open lending accounts reflects the desire to get access to fast cash and instant gratification (fabricated synthetic fraudsters) or needed cash for individuals who were impacted by the economic downturn committing manipulated synthetic fraud as "fraud for a living."

GRAPH B

**LENDING SYNTHETIC FRAUD ATTEMPTS**



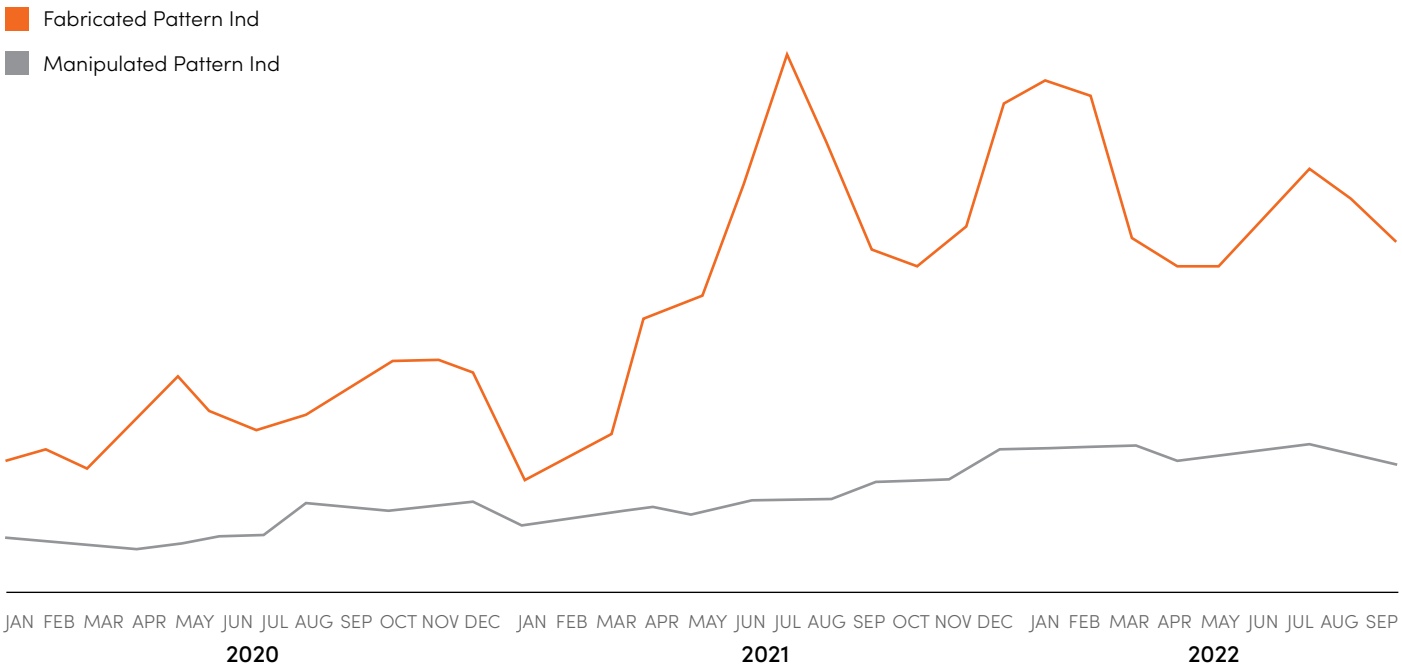
The second difference we noticed compared to DDAs is the similar growth in both fabricated and manipulated identities, suggesting that both consumers and criminal fraudsters were taking advantage of lending products during the COVID-19 period. While attempts by consumers who manipulated their identities to open accounts fraudulently have dropped sharply, with attempts almost returning to pre-COVID norms, fraudsters are still fabricating identities in an effort to open lending accounts fraudulently.

Interestingly, our research shows a much different pattern in fraudulent attempts to open synthetic investment accounts, with peaks tying more closely to the third wave of PPP stimulus, rather than the beginning of the pandemic. As shown in Graph C, the peak in investment fraudulent account attempts started much later than in the other two sectors. Beginning in March 2021, fabricated synthetic fraud attempts broke through their normal attack range and peaked three times: in July 2021, January 2022, and July 2022. The first two spikes happen to coincide with PPP stimulus and the third spike with the 2021 tax filing season.

Manipulated synthetic fraud attempts began to rise in May 2021 and as seen from the graph, they continued to slowly increase through the remainder of the study period.

GRAPH C

**INVESTMENT SYNTHETIC FRAUD ATTEMPTS**

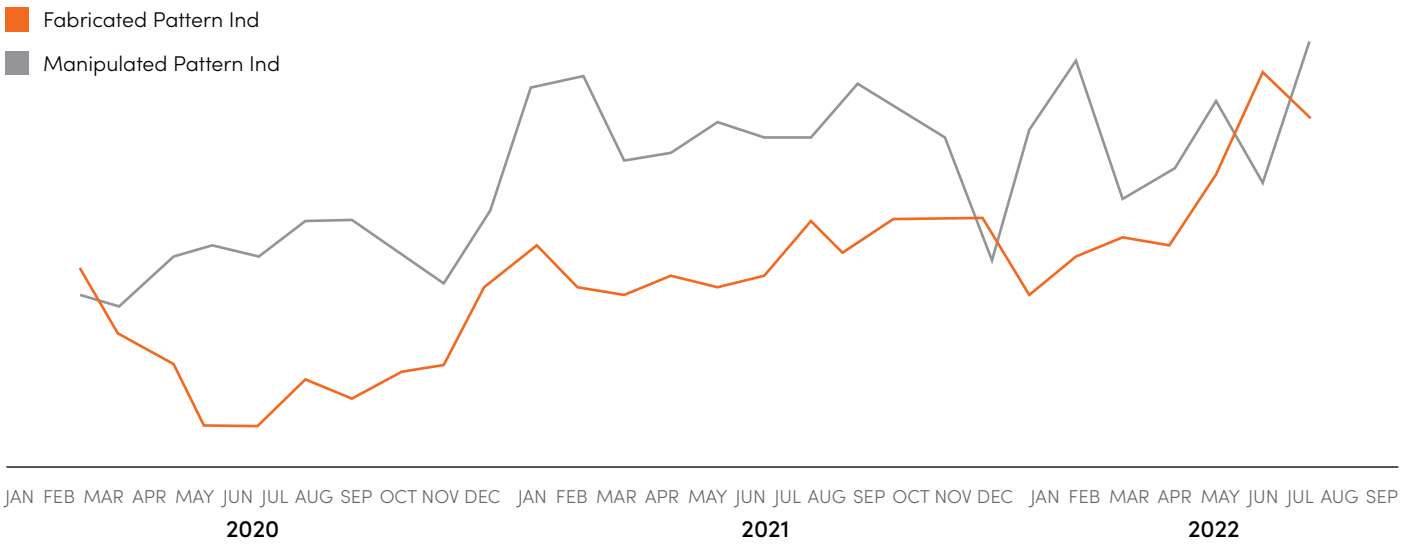


While there was indeed growth in synthetic fraud attempts to open credit card accounts during COVID-19, there were no significant peaks, and unlike the other sectors we studied, consumers' fraudulent attempts actually outpaced fraudsters' attempts to use synthetic identities to obtain credit card accounts.

Graph D reflects higher growth in manipulated synthetic attempts by consumers, with the exception of February and August 2022. We believe this is driven by the economic downturn and consumers' need to gain access to credit, either for "fraud for a living" or "credit repair," which will eventually result in a financial loss for credit card issuers.

GRAPH D

**CREDIT CARD SYNTHETIC FRAUD ATTEMPTS**




We believe this analysis shows that consumers and fraudsters alike are using synthetic fraud either for payment schemes or credit repair, which will result in a financial loss to lenders and harm to consumers, or for "fraud for a living." In either case, they are both fraudulent attempts to beat the U.S. financial system.

Socure has additional pattern analysis that was learned from the study. To keep this sensitive data out of the hands of consumers and fraudsters perpetrating synthetic fraud, Socure will make it available to banking and fintech companies upon request.

# What's on the Horizon?

Synthetic fraud will continue to plague the industry for the next several years. Socure, however, sees a day when the problem of synthetic fraud can be eradicated. **The way to completely solve synthetic fraud is to work collaboratively across industries.**

We need to start by addressing an important issue: **credit reporting agencies that are part of the solution are also part of the problem.** A synthetic identity profile gets created at the credit bureaus when several inquiries are made using the same set of PII. Then, these profiles are nurtured and strengthened which allows the account to mushroom and "pollinate." While credit reporting agencies exist to support legitimate consumers in obtaining credit, there should also be a way to resolve this dangerous practice.

Furthermore, the FTC's identitytheft.gov website is being abused by consumers looking to illicitly dissolve legitimate negative items on their credit report, using a process called "credit washing." Piggybacking tradelines is another unscrupulous practice that consumers use to better their advantage with the credit reporting agencies for account and credit approvals.

By far, the biggest reason that manipulated synthetic fraud continues to plague the industry is because of a lack of understanding of the nuances behind those identities and the subsequent omission of adequate protection at the point of account origination. What's needed are advanced analytics and an automated treatment strategy tailored to the particular subtype of synthetic fraud.

Fabricated synthetic fraud shares many of the same patterns described above, and fraudsters use many of the same tools outlined above. In some ways, fabricated synthetic identities are easier to spot and stop than their manipulated counterparts, which didn't used to be the case.

The reason synthetic fraud gained such a strong foothold in the early 2000s was because the development of fabricated identities was a surprise attack. At the time, no one, other than the fraudsters themselves, had even remotely imagined that a completely fake identity could establish a credit report, pass CIP checks, and go unnoticed. Even today, the vast majority of fabricated synthetic fraud is still charged off as a credit loss, since there is no victim to say, "Not me!" The bottom line is that it needs to be stopped at nearly any cost, especially as synthetic identities try to find their way into the traditional banking and fintech ecosystems and money movement platforms.

**Pollination**

A process that happens after a synthetic identity has built up a positive credit history and adds other synthetic identities as authorized users to its financial accounts to allow those additional profiles to also build positive credit histories.

**Credit Washing**

The fraudulent practice of fraudsters making false claims of identity theft to creditors. They seek to "wash" claims from their record, strengthen their credit score, and apply for new loans and other financial services.

# A proposal for eradicating synthetic fraud

1. **Educate the industry about the problem of synthetic fraud.** The Boston Federal Reserve has done an outstanding job of working with the industry to define synthetic fraud and roll out an exceptional educational program to teach professionals how it is created and how to stop it. Those efforts, along with additional initiatives contributed by partnering solution providers, like Socure, are a good start but don't reach far enough to educate every organization about the dangers of synthetic fraud. Even large and sophisticated financial services organizations ask fairly basic questions, so this effort must not presume any baseline level of understanding. These models should continue to evolve so they can serve the needs of every organization, irrespective of their level of understanding of the issues, or their preparedness in dealing with it.

2. **Stop synthetic identities before they can enter the front door.** Fighting fraud should not be done alone. And yet we still see companies that have significant synthetic fraud hiding in their portfolios when analyzed in a live test or proof of concept. Many do not participate in consortium efforts and do not employ an end-to-end synthetic fraud detection solution. It's critical that all organizations that are susceptible to synthetic fraud, no matter their perceived level of exposure, get aggressive about employing fraud detection and eradication strategies.

3. **Identify "manipulated" and "fabricated" identities and treat them appropriately.** It's not enough to identify a potential application as "synthetic fraud." While a good start, organizations must dig deeper into the patterns of synthetic identity creation to further confirm a synthetic identity as either "manipulated" or "fabricated" and to design an automated solution for follow-on treatment.

4. **Bring identity characteristics forward into account management.** Organizations need to put politics aside and integrate analytics to apply friction when a consumer application falls into scoring margins that make it look possibly synthetic. It could be a consumer with a small digital footprint or someone who just changed their name, or it may be a synthetic fraudster—all of whom flew under the radar of a higher, more risky score. In this situation, pass the characteristics that drove the score on to account management. These additional risk signals gained at the point of origination will reduce false positives and increase fraud capture rates, so that a smart company will identify a marginally scored synthetic identity sooner versus later in the account lifecycle. This will limit the risk and reputational harm that the synthetic identity inflicts and reduce operating costs.

5 **Apply rigid definitions to fraud, label each account, and share those labels with a noteworthy consortium.** Labeling synthetic fraud is more difficult than any other type of fraud, because there is no victim* to inform the bank that an account is fraudulent as when third-party identity fraud occurs. Often, synthetic fraud may not cause financial loss, so those accounts are not flagged. When financial losses on synthetic accounts occur, these accounts are often charged off as credit losses. Socure has developed clustering algorithms and deployed a "human-in-the-loop" machine learning (ML) model to detect synthetic fraud for both types of these accounts. Clean labels based on effective synthetic fraud definitions and shared with a noteworthy consortium is critical to aiding the industry in fighting and eventually eradicating synthetic fraud.

*Footnote: while there is no victim who will call and alert an institution that an account was opened fraudulently, there are indeed victims of synthetic fraud, including consumers who have been scammed through payment fraud, adolescents whose SSNs were stolen to enable synthetic fraud before they turned 18, other individuals whose SSNs were stolen to create a synthetic identity, lenders who face financial loss and reputational harm, and taxpayers and the US government who may be defrauded through benefit, unemployment, stimulus, and other similar programs.

6 **Remove the known tools of the trade whenever possible.** Credit washing (especially when done at scale by credit repair companies), piggybacking authorized user tradelines, and "boosting" credit scores using unscrupulous methods are all known tools-of-the-trade that synthetic fraudsters employ to strengthen credit histories. Credit repair companies are able to offer these services and hide in plain sight, because their methods, while unethical, are not illegal. To learn how easy it is to abuse this practice, enter one of the terms below in an internet search engine:

- How can I purchase an authorized user tradeline
- How can I buy someone else's tradeline
- How can I boost my credit score quickly
- How can I remove negative items from my credit report quickly
- What is the 609 loophole
- How do I manipulate my identity to create a new credit report
- How can I create a fake id

These searches should alarm and anger you. But, that's not the end of it. More information about how to create and nurture synthetic identities is available on the dark web in the form of "how to" guides. Until there is a way to limit or restrict these services and information, manipulated synthetic fraud will continue to proliferate.

7 **Provide eCBSV for all.** As mentioned above, eCBSV is not a magical solution for synthetic fraud; however, it's a great addition to your synthetic fraud-fighting toolbox. eCBSV is currently limited to use by a "permitted entity" only, which includes financial institutions as defined in Section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) and service providers, subsidiaries, affiliate, agents, subcontractors, or assignees of a financial institution, as described in section 215(b)(4). This broad coverage is sufficient for financial services organizations, but limits eCBSV availability for telecommunications, auto finance, and other sectors that are often targets of synthetic fraud attacks. By extending eCBSV availability to more industries, everyone will benefit from more comprehensive synthetic fraud detection tools.

8 **Require CIP solutions that don't integrate synthetic fraud detection technology to provide a disclaimer to users.** Organizations that use credit header files solely to fuel CIP solutions hurt the industry by giving users a false sense of protection against synthetic fraud. An added disclaimer, much like cigarette warnings, that states, "This solution does not detect synthetic identities and will mistakenly validate consumer identities that are fake," may help to push organizations and solutions providers to strengthen CIP offerings, as well as help educate lenders that CIP alone will not stop synthetic fraud.

9 **Identify and delete existing synthetic fraud out of the "machine."** When a synthetic identity is first created, it is easy to spot and more importantly, it might not be able to catch enough of a foothold to build itself to a necessary level to do harm in any financial or information system. However, given time and the creativity of a synthetic fraudster, accounts that slip through weak account origination defenses can do a great deal of financial and other harm. Companies who have not been protecting their front door from synthetic accounts would benefit from a one-time portfolio scrub to identify these accounts and shut them down before they do more harm.

10 **Systematically freeze credit reports for randomly issued SSNs at birth.** In 1987, the SSA implemented the Enumeration at Birth (EAB) pilot in three states (New Mexico, Iowa, and Indiana) to test the feasibility of assigning SSNs to newborns automatically, with the permission of the parents. The pilot, nationally implemented in 1989, was in use by 1997 in all 50 states, two jurisdictions, and Puerto Rico. Presently, over 90% of parents opt in to the program. Since 2011, SSNs issued through EAB have been randomly generated. Bad actors creating synthetic identities often use randomly generated SSNs. Because it is illegal to gain access to credit information on people younger than 18 years of age, it would make sense for the government (or through parent authorization through the Certificate of Live Birth process), to systematically submit a credit reporting "security freeze" to the national credit reporting systems. This credit freeze could be eliminated automatically at age 17, or at the parent's request, whichever comes first. While this would take some planning and regulation changes to implement, it would remove one of the synthetic fraudsters' tools, and protect the child from entering the credit ecosystem with an already negative credit report attached to their credit report.

A version of this process could also exist for Enumeration at Entry (EAE). Under the EAE program, any lawful permanent resident can apply for both an immigrant visa and an SSN by filing an immigrant visa application at a State Department office in their home country. If the visa is granted, then the State Department transmits the identifying information from the person's visa application to DHS. When the person is physically admitted to the United States, DHS sends the information to the State Department to assign an SSN and to issue an SSN card. These issued SSN ranges should be made available to solution providers to help reduce friction for recent immigrants who may try to obtain credit legally but appear to be a synthetic identity.

# The Path Forward

Synthetic fraud is no longer a surprise attack on America's financial and commerce systems. The problem has existed for more than 20 years, and we in the industry and government sectors have allowed it to reach an alarming level.

There are now exceptional educational programs in place. The patterns of synthetic fraud are well understood and the profiles of manipulated and fabricated subtypes have been teased out, which will aid in stopping synthetic fraud better during follow-on step-up efforts. When solution providers work with the industry to develop consortiums of reported synthetic fraud, we can drive incredibly precise models. These models have overcome many of the issues related to false positives and no longer add unnecessary friction to those younger consumers, the underbanked, and immigrants who have a light information footprint and therefore appear synthetic. Socure strongly believes that as an industry, working together with government, we can eradicate the problem of synthetic fraud completely within the next three years, and stop the damage that bad actors are committing against consumers and our financial system.

# Additional Resources


eBook

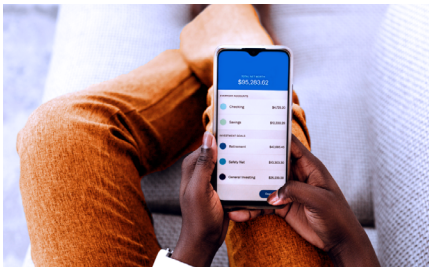
## The Hidden Risk of Money Mules

Download now →


Video

## Identity Insights - Fraud Trend Alert: Money Mules

Watch now →



Blog

## Your Last Chance to Avoid Billions of Dollars in Consumer Scam Losses

Read now →

## 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 governmentissued 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 1,700 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.



Socure