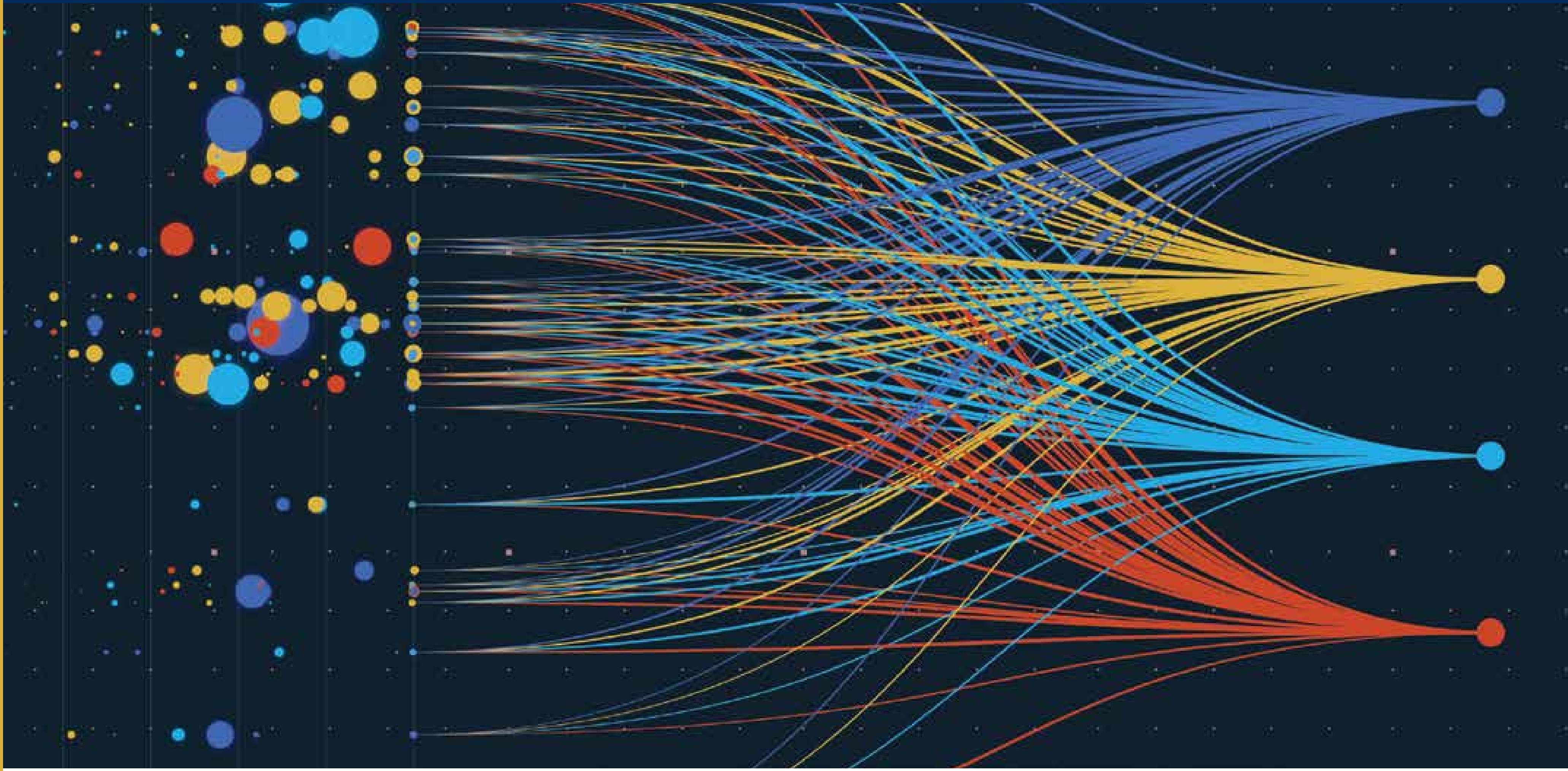
Research Overview

Synthetic Identity Fraud: Fighting Back



How Data Diversity, Industry Initiatives and Human Intelligence
Can Turn the Tide of Synthetic Identity Fraud

Synthetic identity fraud (SIF) is becoming more and more of a threat in our increasingly fragmented world of digitized identities.

Fabricating identities out of thin air is not a new tactic; however the frequency of SIF occurrences are causing industry experts to place greater scrutiny on this type of fraud.

In short, SIF is a perfect storm of fraud.

- It exploits institutionalized vulnerabilities in the legacy US credit system and identity structure.
- It is challenging to detect and track.
- Stolen funds are typically written off as a credit loss.
- Hard-to-define losses mean that the costs of solutions are difficult to justify.
- Fraudsters have a virtually never-ending supply of breached data to pull from for their schemes.

Due to its severity and risk, SIF has recently become the topic of industry awareness and education initiatives, including a prominent campaign spearheaded by the US Federal Reserve. Although there are no silver bullets when it comes to eradicating SIF and other advanced fraud methods, companies can take advantage of proven measures to effectively fight back against fraudsters and criminals.

Features:

This research overview features the latest SIF market data and trends as well as approaches to deter it. It will examine the current state of SIF using input from industry and business executives regarding the current levels of preparation to detect and protect against SIF as well as predictions about the severity of SIF relative to other schemes.

The report will also feature IDology system data to lend deeper, multi-dimensional texture to the dynamics of SIF and how solutions and fraud teams utilize human and artificial intelligence to capture and assess SIF today as well as how the Federal Reserve, regulators, and the Social Security Administration (SSA) are preparing to battle it.

Key Takeaways:

- How and why SIF is a growing concern and predicted to be a destructive force in the future.
- Market trends and transactional data that track SIF's prominence and potency and why comprehensive holistic countermeasures are required.
- How industry stakeholders, including the Federal Reserve, Law Enforcement, and Social Security Administration, are mobilizing with the private sector to address SIF.
- Why the strategy of "data diversity" along with an integrated multi-pronged, multi-layered approach and execution is the optimal solution to SIF deterrence and detection.

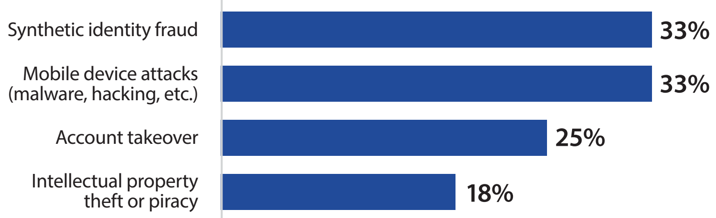
Synthetic Identity Fraud is Top of Mind More Than Ever Before

According to data from the 7th Annual Fraud Report, business leaders and fraud professionals across industries have cited synthetic identity fraud as a growing threat today and the most severe fraud risk type going forward.

This heightened level of concern is reflected in the increase in synthetic identity fraud they have experienced as well as the challenges they've encountered related to detecting, measuring, and resolving it in the last 12 months.

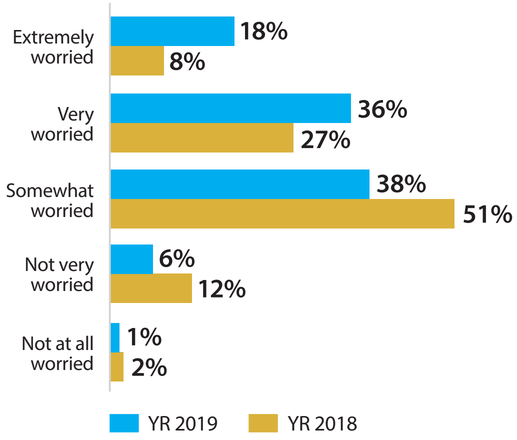
Across the board, executives do not feel prepared to deal with SIF. When asked what fraud vectors and schemes business executives think their industry is least likely prepared to detect and prevent, SIF shares the top spot with mobile device attacks.

What type(s) of fraud vectors or schemes do you think your industry is LEAST prepared to detect and prevent?



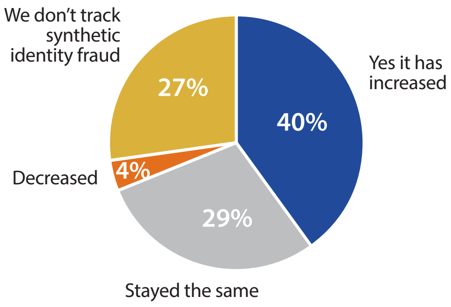
Source: 7th Annual Fraud Report, IDology, 2019

How concerned are you about synthetic identity fraud?



Source: 7th Annual Fraud Report, IDology, 2019

Have you noticed an increase in synthetic identity fraud at your organization over the last 12 months?



Source: 7th Annual Fraud Report, IDology, 2019

Although SIF is prominent in financial services, especially lending, nearly 30% of businesses across a spectrum of industries report higher levels of fraud compared to the prior 12 months. Just as alarming is the 27% that cannot or do not track it.

Concern over synthetic identity fraud is up from last year. Nearly one in five business and risk executives are extremely worried about SIF, and one in three are very worried.

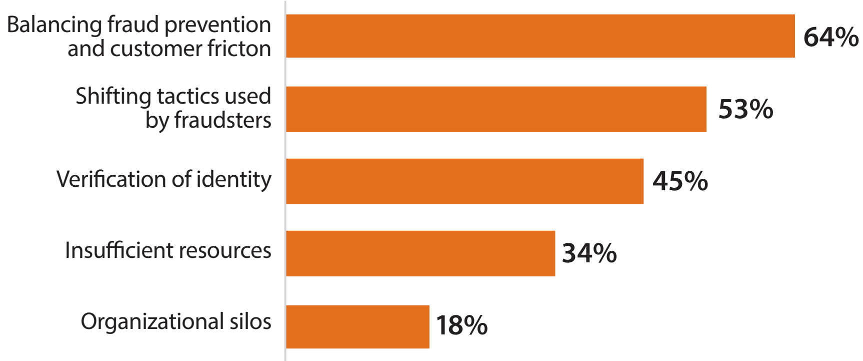
SIF differs from traditional identity theft because a synthetic identity does not completely correspond to a real person.

The home address associated with the identity might exist on a map, but the corresponding SSN is unrelated to the person living there.

As a result, companies hit by SIF usually end up taking a loss on the dollar amount of the fraudulent activity. With the Federal Reserve labeling SIF as the "fastest-growing type of financial crime in the United States," the impact is significant. Fraudsters sometimes claim that since synthetic identity fraud doesn't involve a real, living person, it is a victimless crime. The reality, however, is that SIF is far from benign – it impacts numerous organizations, people and the nation's credit and payment systems as a whole.

SIF Adversely Impacts Top Fraud Challenges Cited by Executives

What do you think are the biggest challenges to fraud deterrence within your industry? (Select all that apply) –Selected Choice



Source: 7th Annual Fraud Report, IDology, 2019

As firms tighten fraud controls to prevent SIF, they can also make onboarding more difficult. This results in friction and more customer abandonments, which is the biggest challenge facing businesses with respect to fraud.

Traditional methods of more tightly managing SIF may result in increased user friction, a top challenge for fraud professionals.

SIF will continue to evolve unless identity data pools are not diversified from data pools that are used to evaluate risk, such as databases of credit bureau identity information.

Financial institutions experience $50-$250MM in financial losses each year due to SIF, with estimated YoY growth of 10-15% from 2011 through 2016 and approximately $1B in credit card losses across all financial institutions in 2016.

Source: U.S. Government Accountability Office Forum, Panelists Input

SIF targets children, the elderly, and the homeless – people who infrequently access their credit files. For example, children's SSNs are 51 times more likely to be used in SIF schemes than adults' SSNs.

Source: Carnegie Mellon CyLab

SIF schemes account for 20 percent of credit charge-offs, where creditors determine that a debt is unlikely to be paid, and 80 percent of all credit card fraud losses.

Source: Gartner

Government agencies potentially vulnerable to SIF: Medicare, Medicaid, Unemployment Insurance, and Supplemental Nutrition Assistance Program (SNAP).

Source: U.S. Government Accountability Office Forum, Panelists Input

The Insidious Growth of Synthetic Identity Fraud

Synthetic identity fraud is growing because it's effective for criminals, hard to detect, and tough to manage.

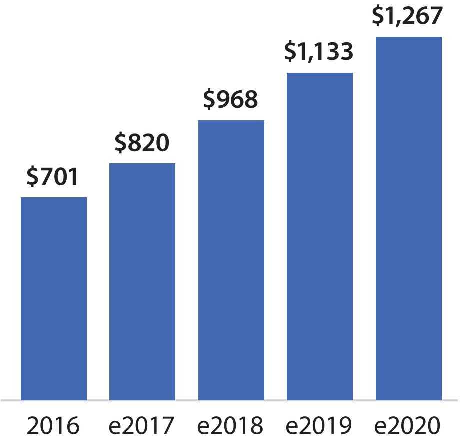
Fraudsters are innovative and constantly probing vulnerabilities such as static, single-layer identity verification systems and gaps in the credit creation process.

One of the biggest challenges is not knowing how many synthetic accounts are quietly incubating in the customer base. SIF is like a ticking time bomb. Not only can businesses not measure how many cases there have been, but they can't track how many currently exist or how many might be coming. Before fraudsters "bust out," synthetic accounts may appear legitimate and profitable, so business line managers may be less inclined to take aggressive action against them until it's too late. And while industry stakeholders, law enforcement, and the federal government take measures to improve awareness and education and develop tools to combat it, nearly half of fraud executives believe it will be the most severe form of fraud in the next three years.

And as Peter Drucker famously said, "You can't manage what you don't measure."

U.S. Synthetic Credit Card Fraud
(millions)

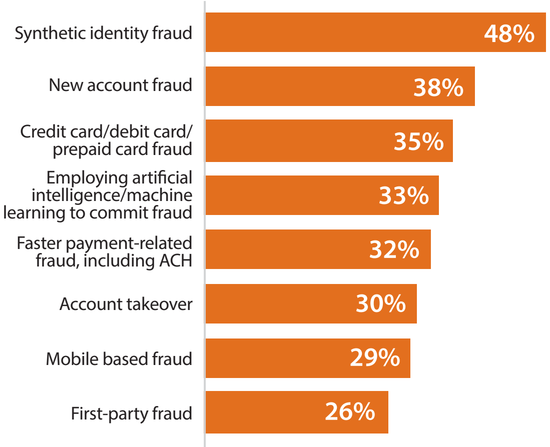
Projections indicate that synthetic credit card fraud could grow by 81% between 2016 and 2020.



Source: Aite Group

Top Fraud Types, Ranked by Predicted Severity Over Coming 3 Years

Executives and fraud professionals predict SIF will be the most severe form of fraud over the next three years.



Source: Seventh Annual Fraud Survey, IDology, 2019

SIF has been used to finance terrorists over long periods of time without being detected by law enforcement.

Source: U.S. Government Accountability Office Forum, Panelists Input

Synthetic identity fraud is the fastest-growing financial crime.

Source: McKinsey

Losses on fraudulent credit card applications can be up to 4.0 bps of card sales volume – and that loss rate is increasing.

Source: Accenture

Synthetic identity fraud "costs banks billions of dollars and countless hours as they chase down people who don't even exist."

Source: Accenture

Viewing the Growth of SIF Through the Multi-Dimensional Identity Attributes Approach

Criminals leverage multiple exploitation points to commit SIF.

The best way to view and attack the rise of SIF is via several integrated identity signals. Looking at data in the aggregate is the only way SIF can be detected and deterred.

In this graphic, masked IDology system transactional data shows several attributes and identity signals as a percent of incidence relative to overall transaction volume by month. These metrics – when analyzed together and over time – reflect past, current, and perhaps future growth of SIF. IDology deploys proprietary identity layers and alerts and synthesizes them to glean deeper levels of fraud intelligence to better detect and deter SIF.

The trends lines are extracted from client data sets over a 21-month period from March 2018 to November 2019. The sample set of millions of transactions was obtained from a consistent set of hundreds of companies over the time period.

These data signals are SIF macro indicators. Each of these data points are typically compiled from multiple sources for robust multi-dimensionality and intelligence depth.

Y1 Axis Data Points

- New ID Attributes Located – Elements such as provided addresses cross-referenced with updated data
- Identity Veracity – Depth of identity data available

Y2 Axis Data Points

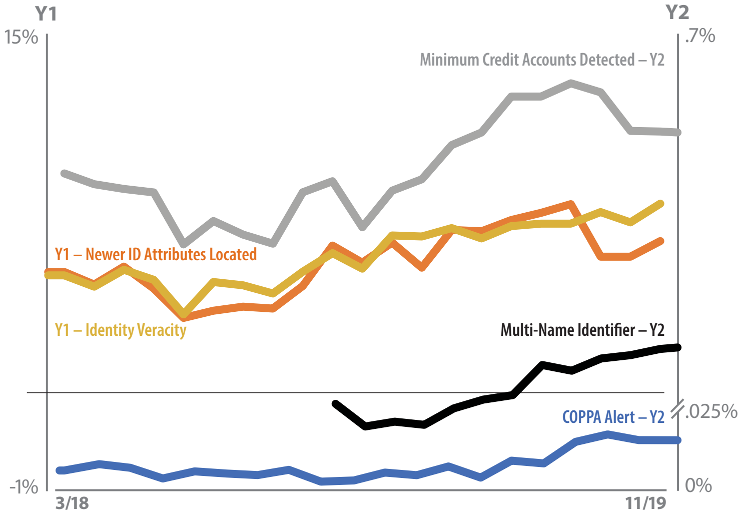
- Minimum Credit Accounts Detected – Signals low levels of data attributes available
- Multi-Name Identifier – More than one identifier tied to multiple names
- COPPA Alerts – Children's online privacy protection alerts for consumers age 13 or under

Taken together, the average compounded monthly growth rate for these metrics 1.8%. The average growth rate over the 21-month time period is 31.8% with the multi-name identifier metric increasing by 32.4%. As a percent of overall transaction volume among a constant number of clients, these consistently heightened numbers are reflective both of the SIF macrolevels and the optimal data intelligence methodology of evaluating and detecting SIF incidents at the micro level.

These identity signals alone may simply indicate more younger consumers applying for accounts or the overall strength of the economy attracting more account signups. When they're analyzed as a group, however, these points paint a broader picture of the issue at play.

Multi-Dimensional Identity Attributes Indicative of SIF Show Growth Over Time

Percent of incidence relative to overall transaction volume by month (March 2018 to November 2019)



Source: IDology Analytics, 2020

How Industry Stakeholders Are Fighting Back

- More law enforcement involvement (from the FBI, specifically) and ongoing
- SSA and eCBSV pilot
- Multiple layers of fraud deterrence, including precision locate tools and mobile authentication
- Consortium networks
- Machine learning and human intelligence

Industry Initiatives: Federal Law Enforcement and Federal Reserve

Encouragingly, a number of initiatives by federal entities are progressing. These developments may make strides in awareness, deterrence, and structural enhancements to combat SIF.

Federal Bureau of Investigation and US Postal Inspection Service

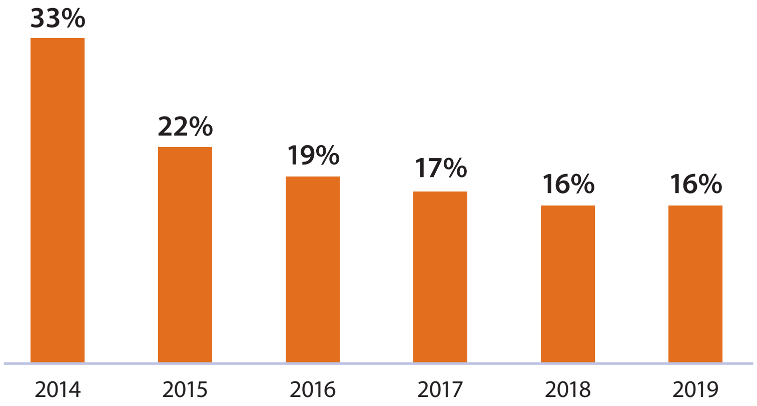
The FBI and the US Postal Inspection Service have stepped up investigations and case pursuits. Between September 2016 and January 2017, the FBI prosecuted four SIF cases as a result of a six-year, orchestrated theft of more than $13MM from 170 victims primarily based in the United States.

The FBI has also implemented proactive education for the private sector, regulators, and law enforcement. Data from IDology's 7th Annual Fraud Report shows that the percentage of businesses that cite difficulties coordinating with law enforcement as a barrier to fraud prevention is at the same low level (16%) as last year. This represents a steady decline from 33% in 2014.

FBI Supervisory Agent Zach Baldwin recently stated that the FBI's goal is "to investigate, disrupt and dismantle money laundering facilitators, criminal organizations and individual operations engaged in fraud schemes which target our nation's financial institutions – all of which are utilizing synthetic identities to commit fraud."

Percentage of Businesses Reporting Coordination with Law Enforcement as Biggest Challenge to Fraud Prevention

Law enforcement is tapering off as a reported challenge to fraud prevention.



Source: Annual Fraud Report, 2014-2019, IDology

US Government Accountability Office and US Federal Reserve System

The US Government Accountability Office (GAO) called and moderated an identity theft industry panel in 2017 with help from the National Academy of Sciences. The result of the gathering was a comprehensive white paper that summarizes market data and subject matter expert input.

The Federal Reserve System launched an ongoing awareness and education campaign in 2019 to combat SIF. An important deliverable from this initiative is a white paper documenting the severity of SIF based on extensive input from industry stakeholders and SMEs. is ongoing.

Federal Agencies Combating Identity Fraud

Federal Agency	Primary Area(s) of Focus and Prosecution
Office of the US Attorneys	White-collar crime (fraud and corruption); healthcare fraud; crime committed online
Federal Bureau of Investigation	Corruption; identity theft; financial fraud and money laundering; organized crime
US Secret Service	Counterfeiting; financial fraud; organized crime
US Postal Inspection Service	Mail fraud; identity theft; crime committed via mail, phone, or internet
Federal Trade Commission	Identity theft

Will the Social Security Administration's Electronic Consent-Based Social Security Number Verification (eCBSV) be a SIF Game Changer?

The Social Security Administration's (SSA) pilot program, launching in mid-2020, will digitize consent for real-time, on-demand SSN verification.

Also known as the Electronic Consent-Based Social Security Number Verification program, or eCBSV, this program (provided that it is launched in a timely fashion and on technically sound and cost-effective grounds) holds a lot of promise. It isn't, however, a panacea for all identity verification problems.

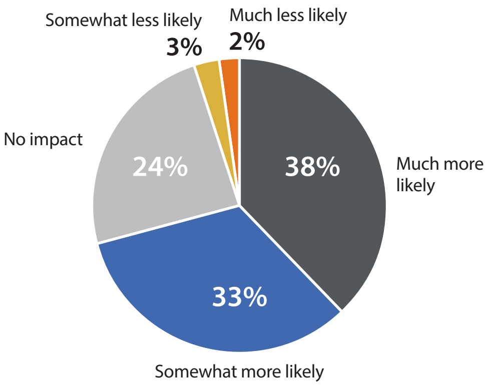
The eCBSV is a fee-based service that allows participating companies to verify that a person's SSN, name, and date of birth match SSA records. The system returns a simple yes or no result. Unlike its analog predecessor, the eCBSV system accepts electronic consent signatures.

The SSA emphasizes that the eCBSV program "does not verify an individual's identity." Because of this, companies still need smart layers of identity verification with diversified data to safely identify consumers and their physical and electronic identity attributes.

> "The missing tool for preventing synthetic fraud is an instant way to verify a Social Security number through an agency process."
>
> – Brian Murphy, senior director of policy at the American Bankers Association

Consumers Express Preferences for Financial Services Providers that Offer Advanced IDV – Could "SSN Verified" Help?

If you knew that a financial provider was using particularly more advanced identity verification methods, how would that affect your decision to choose that company?



Potential Benefits of the eCBSV Program

- Companies with lower risk profiles could streamline their customer onboarding process with a "SSN Verified" option.
- Customers would have a higher sense of security, which would help boost user experience.
- Organizations would have a lower threshold for CIP approval.
- Consent signatures can be electronic instead of physical or "wet."

Realities of the eCBSV Pilot Program

- With a limited pilot going into effect in the summer of 2020, a fully functional program will take over two years to deploy.
- At its core, the SSN was never intended to be a national identifier. The SSA's core competency is not that of a nimble, technically advanced, real-time, always-on identity service.
- These issues could lead to false positives and unforeseen security consequences.

Bottom Line

The SSA's eCBSV program may be headed in the right direction to address SIF, but it will likely require a great deal of time, some trial and error, and significant expense to get it right. And it's not the be-all, end-all. Experts recommend caution and observation. Ultimately, eCBSV will still require a robust identity verification solution that relies on both human and machine intelligence to play a part in helping businesses spot synthetic identities.

There is no silver bullet to stop SIF.

There is no silver bullet to stop SIF. Instead, leading businesses are monitoring several different data types and sources to minimize SIF occurrence and maximize deterrence. The goal of this approach is to employ data diversity with multiple integrated layers of identity intelligence.

Data diversification starts with using fresh identity attribute records outside of the credit bureau data that is used for assessing risk. Given the high amounts of accessible compromised credit data from breaches, SIF can thrive in these corrupted data pools if fresh identity intelligence is not pulled in. Diversifying the attributes collected beyond static KYC /CIP matching to include alerts on newer identity records found, location intel such as geolocation, email and address deliverability, and mobile service and device elements is crucial for a deeper view of a potential synthetic identity.

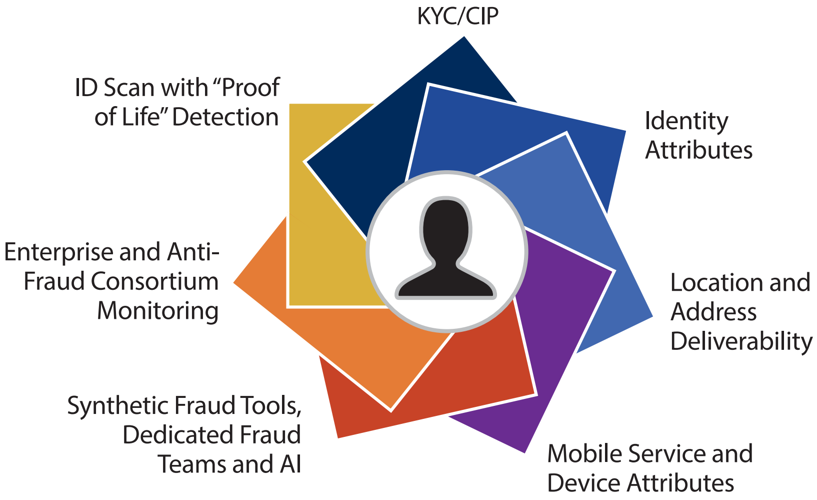
These interconnected layers can be supplemented by system-specific SIF attributes derived from multiple data signals. Diversifying fraud monitoring through both artificial intelligence and human intelligence provides robust, automated antifraud learning and detection at scale with human expertise that can spot unique fraud signals machine learning can overlook.

Broadening company data to include consortium intelligence across a spectrum of companies in a variety of industries has proven effective in spotting the suspicious high-velocity transactions that can be indicative of a synthetic identity.

Finally, suspicious synthetic account onboarding can be dynamically escalated to mobile document identity scan verification. In these instances, the user snaps a picture of the identity document (e.g. driver's license) and takes a selfie with "liveliness detection" to prove legitimacy.

> "By mining the growing number of third-party data sources available, banks can deepen their understanding of their customers. This knowledge can help banks enhance risk controls and stem losses associated with synthetic ID fraud—all without burdening the vast majority of honest customers with ever-more intrusive and time-consuming ID checks."
>
> – McKinsey

Data-Diversified Smart Layers of Identity the Foremost Proven Method to Detect and Deter SIF while Reducing Friction


KYC/CIP
Identity Attributes
Location and Address Deliverability
Mobile Service and Device Attributes
Synthetic Fraud Tools, Dedicated Fraud Teams and AI
Enterprise and Anti-Fraud Consortium Monitoring
ID Scan with "Proof of Life" Detection