SYNTHETIC IDENTITY FRAUD

The Next Frontier in the Fight Against Financial Crime

SentiLink

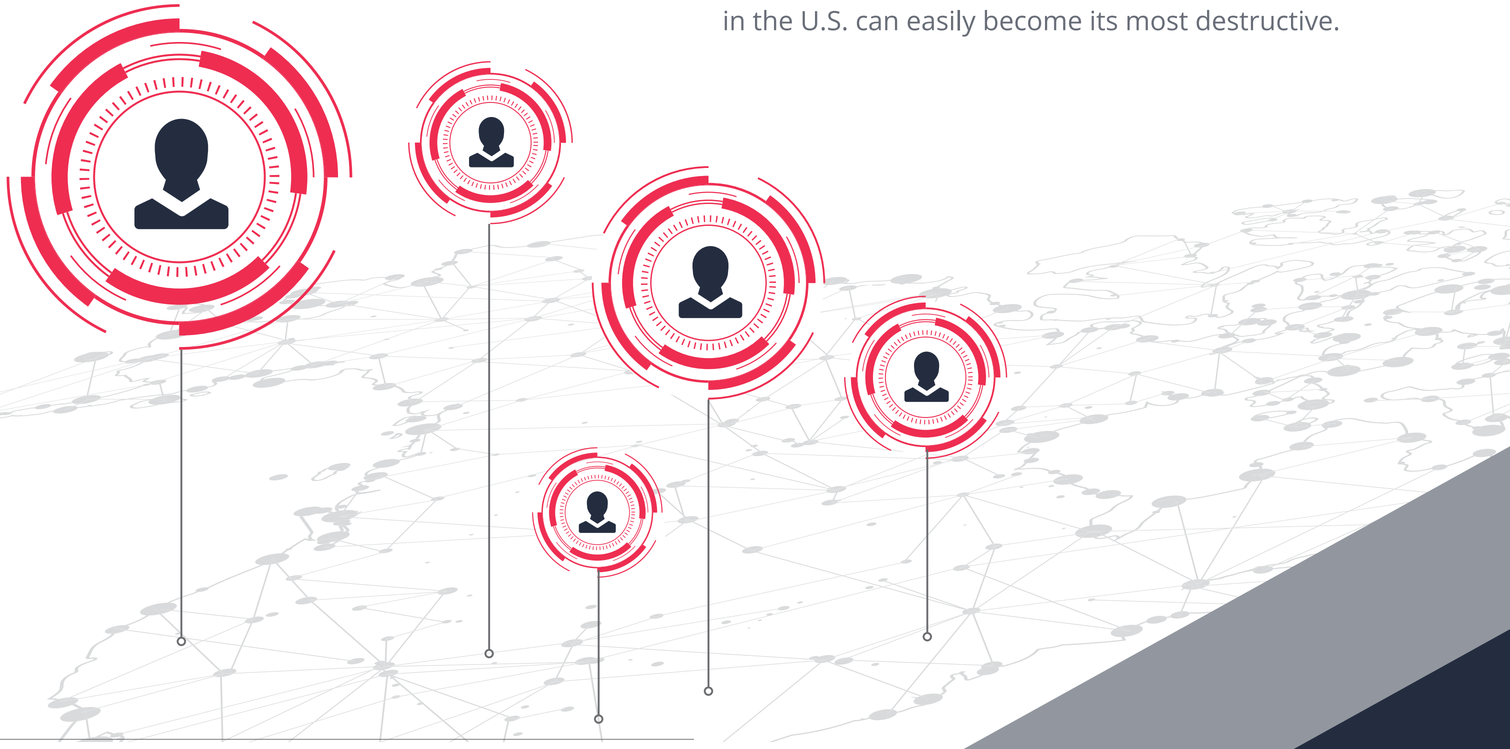
IDENTITY VERIFICATION UNDER SIEGE

> **Bottom line:** Criminals and fraudsters have figured out how to game the U.S. credit system and sidestep KYC requirements to create synthetic identities, and are now able to commit financial crimes with impunity.

The U.S. financial system is officially under siege from a new and growing form of criminal activity known as synthetic identity fraud. The Federal Reserve[1] estimated losses from synthetic identity fraud at $6 billion in 2016 alone. By January 2019, McKinsey & Co[2] called synthetic identity fraud the fastest growing financial crime in the U.S., accounting for 10 to 15 percent of charge-offs in a typical unsecured lending portfolio.

Community banks and credit unions are prime targets for large scale fraud, but the risk extends to include criminal and national security implications that could empower and exacerbate money laundering, terrorist financing, espionage, and human trafficking.

Without an urgent, coordinated response from financial institutions and regulators alike, what is already the fastest-growing form of financial crime in the U.S. can easily become its most destructive.



[1] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

[2] https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

In this whitepaper, we will address:

- ✓ The definition of synthetic fraud and how it differs from traditional identity fraud
- ✓ The extent of the risk and the current trajectory of potential loss
- ✓ Contributing factors allowing synthetic ID fraud to take hold
- ✓ How financial institutions and regulators can respond

In looking at this issue, it's important to understand that, unlike traditional identity fraud where a criminal steals and exploits the identity information of an entirely real individual, synthetic identity fraud is far more sophisticated and difficult to detect. Perpetrated through a combination of manipulated and fabricated identity details, criminals create new identities that can be impossible to trace.

With a synthetic identity in hand, fraudsters can masquerade as trusted consumers, avoiding all identity controls under the guise of the manipulated or fabricated identity. And because it's so difficult to detect, a single fraudster can repeat the routine over a dozen or more identities, wreaking havoc on our financial system.

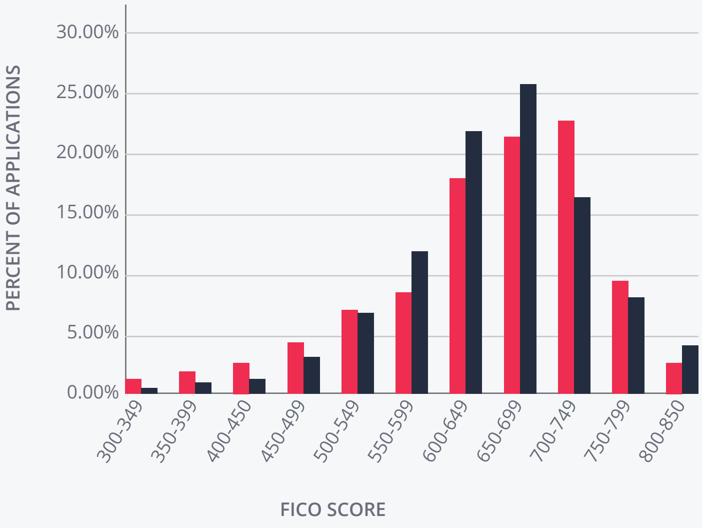
The impacts of synthetic fraud are only beginning to be felt, and are likely vastly understated due to reporting challenges, difficulties in prosecution, and the lack of an economic incentive for the majority of institutions involved in the first-line of defense.

Absent proactive action from both financial institutions and regulators, the potential impact of synthetic identity fraud is great, if not catastrophic. Together, legislative action, technology solutions, and industry engagement can substantially reduce or even eliminate synthetic fraud.

But we must act now.

> **"1 in 5**
> **third party synthetic identities scores has a FICO score above 750. There is a strong disincentive, as a lender, to filter out these fabricated identities."**
>
> SENTILINK DATA, APRIL 2020

SentiLink Data: FICO Scores of Synthetics Versus Other Applicants



SYNTHETIC IDENTITY FRAUD:
What it is and How it Works

Definitions

Synthetic identity:

An identity where the combination of name, date of birth, and SSN do not correspond to a single real person.

First party synthetic identity (manipulated identity):

Typically includes the name and date of birth of the applicant, with a fake SSN. It can include other combinations of real and fake identifiers.

Third party synthetic identity (fabricated identity):

The consumer's name, date of birth, and SSN are all completely fake.

What is a synthetic identity?

A synthetic identity is one where the name, date of birth, and social security number (SSN) combination does not correspond with any real person. Whether manipulated or completely fabricated, the criminal objective of synthetic identity fraud is to misrepresent an identity or give false information with the intent of defrauding financial institutions, government agencies, or individuals in some manner.

How is a synthetic identity used to commit crimes?

Criminals use synthetic identities to open consumer and business financial accounts, establish artificial credit histories, make fraudulent purchases, and even enroll in government benefits. Synthetic identities are also used in money laundering, terrorist financing, and other global crime ring schemes.

Synthetic identity fraud is the fastest-growing type of financial crime.

McKinsey & Company's[1] finding that synthetic ID fraud is the fastest-growing type of financial crime in the United States is not surprising given its scalability. A single fraudster can create and incubate a stable of identities, constrained only by the process of creating the synthetic identities and using them to open accounts. Historically, it was time consuming to cultivate a synthetic identity as the newly-devised identity must be put through a routine of establishing credit, building trust among financial institutions, and staying under the radar of established fraud detection methods. However, with the advent of automated bots used to create identities, a vibrant marketplace for authorized user cards, and the ability to purchase aged synthetic identities 'off the shelf', the lead time is no longer a material constraint for determined bad actors.

Notably, the risk of synthetic identity fraud to the U.S. financial system has drawn the attention of the Federal Reserve, which is publishing a series of whitepapers[2] on the phenomenon. And because synthetic identities mature over time, it's likely we've only seen the tip of the iceberg.

3 critical footholds for synthetic identity fraud:

How is synthetic fraud growing so quickly and why aren't established identity verification programs catching these types of fake IDs?

Part of the problem is that synthetic identity fraud has never been seriously contemplated by applicable laws and regulations, most of which is focused on preventing ID theft. We contend that synthetic ID fraud has found its foothold within today's financial system by exploiting three critical vulnerabilities:

1. **Liberal identification requirements under the Bank Secrecy Act.**
2. **Limited access to the definitive list of identities maintained by the SSA.**
3. **The circular reliance of CRAs and financial institutions.**

Let's explore each of these.

[1] https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

[2] https://fedpaymentsimprovement.org/news/press-releases/federal-reserve-system-white-paper-examines-the-effects-of-synthetic-identity-payments-fraud/

FOOTHOLD #1

The Bank Secrecy Act

The Bank Secrecy Act (BSA) is a robust set of requirements around customer identification and verification to thwart money laundering and other financial crimes. The BSA has served financial institutions and the greater financial system well, however, it is not without its shortcomings. The BSA simply was not written with synthetic identity fraud in mind. Under the BSA, financial institutions can verify identities by reference to name, address, DOB, and SSN alone. These are the very identifiers that comprise a convincing, well-cultivated synthetic identity.

Know that, while gradual and subtle, a synthetic identity used for theft will perform like a perfect consumer for the majority of its lifecycle, until it finally exhibits a 'bust out' behavioral pattern in which it builds credit worthiness in one way or another before maxing out available credit lines and disappearing. Where a third-party synthetic identity is used, it can be almost impossible to trace the ID back to a specific individual. And before realizing what has happened, the criminals can double the payout on credit lines by claiming identity fraud or using bogus checks to pay off balances before maxing out the credit again and then defaulting.

For organizations who only encounter synthetic identities during the 'perform' phase, there is no economic incentive to detect and eliminate synthetic identities. After all, in this phase, the synthetic identity is performing as a good customer and making money for the institution. BSA requirements aren't helping matters since the IDs easily pass traditional KYC tests and institutions can assert 'plausible deniability' by relying on traditional KYC approaches that have no capability to detect synthetic identities. Deposit account business units (as opposed to lending business units), cryptocurrency exchanges, online gambling and peer-to-peer transfer businesses have even less economic incentive to identify and eliminate synthetic identities, as they have no material risk of loss.

As a result, these institutions are providing the synthetic identities a low-risk environment to incubate — only serving to further legitimize the identity, and resulting in the synthetic identity opening more accounts with ever increasing financial autonomy.

Without increased regulatory scrutiny, this pattern will continue.

Busting Out:
Applying for and Maxing Out Credit

- Fraudster uses fake info to apply for credit
- No credit profile exists, application is declined but CRA establishes a credit file
- Fraudster applies for small credit line for borrowers with no history
- CRA affirms profile exists, application approved
- Fraudster established good payment history, applies for more credit and loans
- ❗ **Fraudster “busts out” by maxing out credit lines**

Busting Out:
Assigning Authorized Users to Accelerate Creditworthiness

- Fraudster recruits legit cardholders to add an authorized user to their account
- the authorized user piggybacks on holder’s credit history
- with an artificially inflated credit score, authorized user applies for credit cards and loans, and is accepted
- ❗ **Fraudster “busts out”**

FOOTHOLD #2

The Social Security Administration

It may be surprising to hear that a full 85 to 95 percent[1] of synthetic identities are not flagged as high risk by financial institutions. They are increasingly difficult to detect, in part, due to the Social Security Administration's move in 2011 to a randomized SSN assignment schema in order to obfuscate the geographic origin of SSNs – a problem which is only going to get worse as the proportion of random SSNs increases.

Adding to this, access to the Social Security Administration's records is limited to the CBSV process, requiring written consent from the individual and exact matching, and therefore making it difficult for financial institutions to definitively validate a specific combination of PII. (We discuss the impact of the eCBSV process below.)

This double whammy effect has created a strong second foothold for synthetic identity fraud and has limited the ability of legacy fraud detection technologies to determine the veracity of a given SSN.

[1] https://www.idanalytics.com/wp-content/uploads/2018/11/Synthetic-Identity_Slipping-through-the-cracks_Executive-Summary.pdf

FOOTHOLD #3

Circular Reliance of CRAs and Financial Institutions

A key point to understand is that any credit request submitted to a Consumer Reporting Agency (CRA), such as Equifax, TransUnion, or Experian, will create a credit profile if none existed before.

The initial application made under a synthetic identity is usually rejected because the CRA cannot match the name to a record. The mere act of applying for credit, however, creates a new credit record, or so called "proof of existence," in the name of the synthetic ID account holder. This new file looks just like that of any real person starting to build a credit record, and it lays the foundation for perpetrating future fraud. The more legitimate they appear, the more financial damage they can ultimately inflict.

This would be less of a problem if the CRAs didn't rely on the financial institution's KYC processes when creating a file. In essence, the CRA assumes the financial institution knows who they are dealing with, while the financial institution relies on the CRA data to determine whether that person exists. Reliance on the availability of a credit profile as an indicator of legitimacy will perpetuate this issue, unless and until a specific test for synthetic identities is added to traditional KYC processes.

> **"88% of synthetic identities passed a financial institution's KYC/KYB process and had a file started by the credit bureaus."**
>
> SENTILINK DATA, APRIL 2020

A Synopsis of the Current Approach to **CUSTOMER IDENTIFICATION IN THE U.S. FINANCIAL SYSTEM**

Governed by the Bank Secrecy Act

In the United States, Know Your Customer (KYC) and Anti-Money Laundering (AML) is governed by the Currency and Foreign Transactions Reporting Act, commonly referred to as the Bank Secrecy Act (BSA), which has been supplemented by the 2001 USA PATRIOT Act and various other laws.

Requires a Formalized Customer Identification Program

Under BSA, organizations are required to take steps to know — with a reasonable belief — the true identity of each customer. In particular, Section 326 of the USA PATRIOT Act requires any financial institution engaged in financial activities to establish a written, board-approved customer identification program (CIP) to collect and verify identifying information about each prospective customer.

Reasonable and Practical Assurance

Under BSA, the CIP must include risk-based procedures to verify the identity of each prospective customer to a reasonable and practicable extent. In other words, the information must be sufficient to enable the institution to form a reasonable belief that it knows the true identity of each customer. While not stated explicitly, there is no doubt that a ‘reasonable belief’ under the BSA must include diligence as to whether the identity is real or synthetic now that the prevalence of synthetic identities is known and the deficiencies in traditional KYC processes are understood.

Taking into Account AML Risk

To reach a reasonable and practical level of assurance related to identity, financial institutions are required to perform customer due diligence commensurate with the level of AML risk posed by the customer.

All Customers are Subject to the CIP

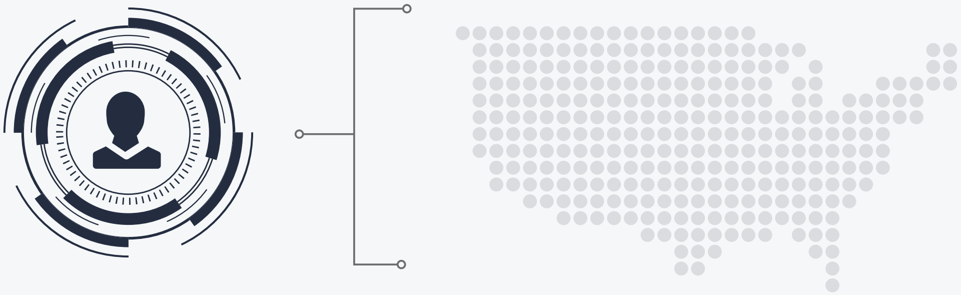
All customers must be subject to the Customer Information Program (CIP), with certain limited exceptions that are defined by regulation. The level of Customer Due Diligence (CDD), and whether or not Enhanced Due Diligence (EDD) is required, will depend on the customer's AML risk rating.

Minimum CIP Information Required

CIP information must include: Name, date of birth (DOB), residential or business address, and identification number (typically a social security number).

Enforced by FinCEN

Authority to assess penalties for violations of U.S. AML rules and regulations rests with the Secretary of the Treasury Financial Crimes Enforcement Network (FinCEN).



WHY CARE
About Synthetic Identity Fraud?

In 2013, the Department of Justice charged 18 people as co-conspirators in a complex credit card fraud scheme that spanned 10 years, 28 states and eight countries. The international crime ring[1] developed more than 7,000 synthetic identities to fraudulently obtain more than 25,000 credit cards, stealing somewhere between $200 million to $1 billion. This case shows just how much damage can be caused.

In 2016, Auriemma Group estimated that the average charge-off balance per instance of synthetic identity fraud averaged more than $15,000 per attack, accounting for up to 20 percent of all credit losses.

Just three years later, in 2019, the Federal Trade Commission estimated synthetic identity fraud was costing American businesses $50 billion[2] each year.

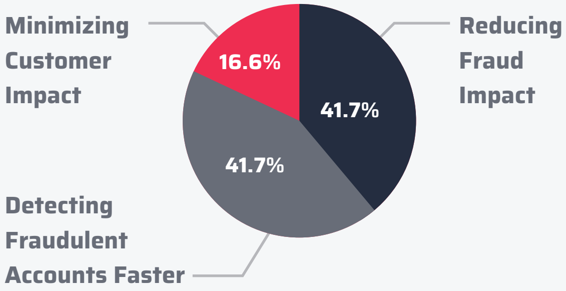
Although there are many reported instances of prosecution[3], it is highly likely that the extent of the problem is far greater than reported due to difficulties in attributing fraud losses to a specific cause — was it fraud or credit abuse? — or to a real person capable of prosecution.

As more and more synthetic identities bust out, the stakes get higher.

The Financial Impact

Synthetic ID fraud accounts for 80 percent of all credit card fraud losses and nearly 20 percent of credit card charge offs, according to a Rippleshot[4] Card Fraud Benchmark Report. The study also revealed that every dollar of fraud costs banks and credit unions roughly $2.92. Since there is no actual person to trace the fraud back to, they end up absorbing the costs. Not surprisingly, 41.7 percent of financial institutions in the study said one of their top goals was faster fraud detection.

Rippleshot's Card Fraud Benchmark Report collects key data points from across the payment card industry. This data is intended to help fraud management teams determine where gaps exist, and how their goals align with others in the industry. Below are the Top 3 fraud goals listed by FIs.



ABA.COM

[1] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

[2] https://www.globalbankingandfinance.com/the-fastest-growing-form-of-fraud-thats-also-hardest-to-detect-synthetic-identity-fraud/

[3] https://www.justice.gov/usao-ndga/pr/identity-thief-sentenced-using-new-form-fraud-synthetic-identities

[4] https://www.aba.com/-/media/archives/endorsed/rippleshot-state-of-card-fraud.pdf

Another Casualty: Children

Children's SSNs are a prime target for synthetic identity thieves because they are inactive for up to 18 years and don't normally have any public information associated with them. The fraud typically isn't discovered unless the child's parents are tipped off by a bill collector or the child begins receiving credit card offers. The real damage comes later when the minor is denied a driver's license or college loan, or has problems getting a job when negative information appears on their employee background screening.

Broader Implications: Money Laundering, Terrorist Financing, Human Trafficking

Less understood, is the use of synthetic identities as a law enforcement and national security issue. FinCEN Director Kenneth Blanco[1] noted that *"[i] dentity is a critical part of how FinCEN keeps Americans and the U.S. financial sector safe"* from money laundering, terror financing and human trafficking, and, regrettably, *"weaknesses in identity verification and authentication systems" enable these crimes"*.

As mentioned above, synthetic identities can avoid all identity controls that currently exist in our financial system.

According to the Financial Action Task Force[2] (an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction) *"the use of synthetic identities pose the greatest risk in the identity proofing and enrolment stage of digital ID systems in the US."*

There are serious consequences when criminals use synthetic identities to steal funds, escape detection, or facilitate drug and human trafficking. When used for money laundering or terrorist financing, synthetic identities are capable of evading even the strictest identity controls, as they are often supported by fake artifacts of identity such as drivers licenses or passports, which are freely available on the dark web, and they are enabled by *"shell companies, that [do] little or no legitimate business"*[3] with equally synthetic directors and beneficial owners.

```
connect to address 192.168.1.1

username: **********
password: ************

Access granted...

---------------------------------------
exited after 0.006146 seconds with return value
any key to continue . . .
```

[1] https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid

[2] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

[3] https://www.justice.gov/usao-edny/pr/11-defendants-charged-credit-card-bust-out-scheme

While we are seeing increasing examples of money laundering using synthetic identities[1], there is inadequate focus on the use of synthetic identities to facilitate this type of criminal activity.

How synthetic identities are used in money laundering:

- **Placement (movement of cash from its source):** Placement of illegal funds into an account opened in the name of a synthetic identity.
- **Layering (disguising the funds):** Transferring funds to other synthetic identity bank accounts (in small amounts to fall below the CTR reporting limit) or used to purchase assets in the name of a synthetic identity which can then be sold for cash.
- **Integration (creating an apparently legal basis):** Opening business or securities accounts to make loans or transfer liquid assets.

How synthetic identities are used for terrorist financing:

- Evading no fly lists[2]
- Renting properties to use as 'safe houses'
- Purchasing trucks and other heavy vehicles
- Purchase of chemicals, industrial and other restricted products
- Open deposit accounts to easily send and receive money
- Purchase cell phones

Despite being an ideal cover for serious crime, there have been few instances of public prosecution of synthetic identities for this purpose, in part because of the challenges of apprehending the perpetrators, but also because regulatory scrutiny hasn't yet forced financing institutions benefiting from such financial transactions to establish processes designed to identify synthetic identities.

[1] https://www.justice.gov/usao-edny/press-release/file/1177966/download

[2] https://www.cbc.ca/news/canada/suspected-terrorist-links-to-synthetic-id-fraud-are-being-ignored-1.2557677

Preventing Synthetic Identity Fraud: Actions Organizations Can Take

Strategies for preventing and mitigating synthetic identity fraud require action on multiple fronts. In 2018, the Economic Growth, Regulatory Relief, and Consumer Protection Act was signed into law. The Act directed the Social Security Administration (SSA) to modify or develop a database for accepting and comparing fraud protection data provided electronically by permitted entities. In response, the SSA established the Electronic Consent Based Social Security Number Verification (eCBSV) program, a fee-based SSN verification service.[1]

The program allows certain financial institutions to directly access the SSA's records in order to validate the existence of a specific name, DOB, and SSN combination for new applicants to financial institutions. While the eCBSV program is a useful step for on boarding new customers, implementation of it will create some challenges for financial institutions, including high-friction customer consent requirements and zero tolerance for inexact matches. And the eCBSV program does nothing to prevent existing synthetic identities currently in our financial system.

As noted by the Fed[2], additional solutions are required to create a comprehensive shield against synthetic identities.

Machine Learning and Data Sets to Instantly Detect Synthetic Identities at Account Onboarding

According to McKinsey & Company[3], ideal solutions will leverage machine learning and data assets to instantaneously detect synthetic identities at the time of application, in order to minimize any negative impact on commerce. This recommendation is consistent with the Joint Statement from FinCEN and Federal Banking Regulators[4] regarding the desirability of using "[N]ew technology, such as artificial intelligence and machine learning … to better manage money-laundering and terrorist-financing risks, while reducing the cost of compliance."

These models can be trained to identify and compare expected customer behavior patterns and detect anomalies that may indicate fraud. For example, since most legitimate identities have a digital footprint well beyond merely an SSN and credit score, institutions can evaluate other third-party data such as cell phone records, previous addresses, and even social media accounts to find attributes that tie the identity to an actual person. A risk-based approach like this can utilize powerful algorithms along with robust data mining capabilities to provide companies with detailed analyses of the relationships and characteristics of identity data that far exceed the simple matching of data against public records.

Such solutions operate in the background of the onboarding process, via digital data transfers, providing no customer friction whatsoever.
In addition, the machine learning models are infinitely scalable and therefore inexpensive. There is no reason that solutions such as these should not be implemented by every financial institution, providing a high level of due diligence that can serve to satisfy regulators, provide a substantial mitigation of fraud losses for financial institutions, and result in an overall improvement of safety and soundness across the financial sector.

[1] https://www.ssa.gov/dataexchange/eCBSV/

[2] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-october-2019.pdf

[3] https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

[4] https://www.fdic.gov/news/news/press/2018/pr18091.html

PREVENTING SYNTHETIC IDENTITY FRAUD

What Regulators Can Do

The unfortunate reality is that in a highly competitive marketplace fueled by FinTech growth, in the absence of an economic incentive, financial institutions do not feel compelled to take action to detect and prevent the use of synthetic identities to open accounts. Only through specific policy statements and directives will financial services regulators be able to proactively drive adoption across the sector.

The Federal Reserve has been leading the way with its whitepapers, and other regulatory bodies have referred to the issue more obliquely. Regulators can underscore the significance of synthetic identity fraud through specific statements and actions, including the following.

✓ Direct oversight and enforcement apparatus to proactively review the compliance activities of regulated entities. Specifically, regulators should be asking all regulated entities what steps they are taking to eliminate synthetic fraud as part of their annual examination process.

✓ Focus attention on organizations that do not have a strong financial incentive to address the issue of synthetic identity fraud, such as depository institutions and organizations that focus on very small-ticket or entry level credit products.

✓ Work with Congress (e.g., the House Financial Services Committee) and the private sector to move away from SSNs as a basis for identification.

✓ Engage the fintech sector in developing solutions that can aid compliance.

✓ Continue to emphasize the consistency and reliability of reporting in order to accurately track the extent of the problem.

SENTILINK'S ROLE

The time has come to address the underlying systemic vulnerabilities that enable synthetic identity fraud to flourish. SentiLink believes that synthetic identity fraud can be substantially eliminated through a combination of tactical and strategic legislative and regulatory action, and we are poised to help guide these efforts.

As leaders in fraud detection in the payments industry, we will work with Congress, the Executive Branch and the private sector to develop efficient and effective solutions that will strengthen the competitiveness and security of our financial system and fortify the integrity of our national security.

SentiLink

sentilink.com