FRAUD FIGHTER™

UVeritech Guide to Synthetic Identity Fraud & Theft.

What it is, Who it impacts, How to defeat it.

What is Synthetic Identity Fraud (SIF)?

Synthetic identity fraud / theft is a type of fraud in which a criminal combines real identity attributes (eg. Social Security Numbers (SSN) acquired via hacking / phishing) with fake personally identifiable information (PII).

For example, a synthetic identity may be comprised of a real SSN with a fake name, fake address, etc and that resultant combination of SSN+name+address+date of birth does not align with a real person.

Synthetic ID fraud differs from traditional or “true name” Identity Theft fraud, in that the latter links to and impacts a real person, with a fraudster acquiring key information that enables them to conduct unauthorized transactions and acquire illicit gains under the name of the victim.

A real person is likely to notice fraudulent behavior on their profile and take action to correct it, while synthetic identity fraud doesn’t have anyone connected to it to raise an alarm, and so, can run unchecked and/or lie latent for years. Without a paper trail holding a real person to account, the actual victims of synthetic identity fraud are then the financial lenders and providers who are left to absorb the losses.

Just how prevalent is synthetic identity fraud? According to a study by ID Analytics, “true name” identity theft now accounts for a very small portion of all identity fraud. Given its explosive growth over recent years, synthetic identity fraud now accounts for ~85% of all identity fraud cases in the U.S. today.

SIF’s Driving Factors

Somewhat ironically, advancements in technology have led to increased vulnerabilities in government and financial systems, and now facilitate synthetic identity fraud:

Payment Card Security Improvements

The introduction and widespread deployment of Europay, Mastercard, and Visa (EMV) chip technology in debit and credit cards have made it more difficult for thieves to commit in-person fraud. As such, they shifted their focus and tactics to acquiring illicit gains online.

Our Digitized Life

Our entire life cycle - all experiences from birth to death - can essentially be converted and “digitized” to data and numbers. All of our financial transactions, government benefits, and our very identity itself exists today as a collection of data points, scattered amongst a variety of computer servers in your school, work, bank, or local DMV. Our lives produce a near infinite stream of unique data, and yet it takes just a few, put together, to serve as our identity proxy.

Assume at Risk

There should be no remaining doubt that our digitized lives and PII are now no longer private, but have been acquired and collated by thieves via widespread cyber-breaches of the aforementioned servers holding our personal information. At this point it’s of little use to isolate the most damaging incident(s) out the many thousands of data breaches that have exposed hundreds of millions of personal records, credit card numbers, and social security numbers. The reality is that our records are now for sale, quite cheaply, on the Dark Web and so now it becomes a matter of consumers and businesses being prepared to confront fraud that will inevitably darken our door.

How does it work?

Synthetic identity theft is one of the most difficult types of fraud to detect and protect against since synthetic identities can act and look like an average bank customer. When a to-be synthetic identity thief applies for an account, it may appear like a real customer with a limited credit history.

Technology advancements in remote banking have contributed to the explosion in SIF incidence rates. Tools such as online account initiation, electronic money movement, and automated underwriting and approval of loan applications have all thrown fuel on the fire accelerating SIF's growth in the past 10-15 years.

That said, and very interestingly, ID Analytics' research also revealed that just half of synthetic identity fraudsters apply and obtain credit using the digital channel. That indicates that fraudsters are bold and very confident that they can pass "Know Your Customer (KYC)" tests when appearing in-person to apply, open, or execute transactions on accounts.

So how is this even possible?
How can banks just accept a made-up identity?

At its root, our national credit check system has historically too easily been exploited due to lack of a centralized source of truth for consumers' identities.

Here is a common scenario out of a synthetic ID fraudster's playbook:

1. Fraudster illicitely acquires or generates a Social Security number, and combines it with other real or fake information (name, address, phone number) that aligns with the information on a fake ID document obtained on the black market.

2. He applies for credit or a loan and initially fails due to no credit history, but this action now establishes and implants a new profile in the credit system.

3. Time passes, and he applies again, this time succeeding in acquring a small loan with likely unfavorable terms, eg. a high interest rate.

4. The fraudster patiently cultivates this new credit identity, pays his bills on time, gradually building up the credit score. Realistically, fraudsters are cultivating many, maybe hundreds of synthetic identies concurrently.

5. Finally, the fraudster applies for and acquires his strategic goal: a big loan, regardless of payment terms / APR

6. One End game example: Cash out / Bust out. The fraudster takes the money and runs, with no intention to pay it back. He destroys the credit score and reputation of the synthetic identity.

7. There is no consequence to the fraudster, with no real person to pursue or hold accountable. The end victim is the bank itself.

After Step #3, financial institutions usually can’t detect if synthetic identity fraud has even occurred.

People who commit synthetic identity fraud can establish and use multiple identities simultaneously, and may even keep accounts open, lying in wait on the bank’s books for months or even years.

As we all know, a high credit score is a powerful financial tool, allowing for wide qualification of loans and high standing lines of credit. A devious alternative to an immediate bust-out would be a scenario where criminals rack up vast charges on a fradulent credit card account, and then pose as the fraud victim with the intent to clear those charges. If successful, they then restore the credit line, restarting this illicit fraud cycle from scratch, and use the credit to commit further theft.

Finally, there also exists synthetic identity fraudsters who aren’t motivated by theft, but rather by a need to just participate in the financial system. There are numerous cases of undocumented immigrants using synthetic IDs to obtain access to services such as bank accounts or credit cards, enabling them to receive payment for work or to make purchases.

Who Does it Impact?

Synthetic identity fraud impacts a wide array of providers:

Financial Services

Account Opening

Tradeline Acquisitions

Healthcare

Illegal Drug Sales

Healthcare Access

Public Sector

Benefit Payments

Acquisition of Services

Automotive

Vehicle Attainment

KYC Compliance Issues

Financial Services institutions that offer Banking, Credit card, Home loan, and/or Auto loan products and services

Healthcare organizations

- Illegal access to medical services and in-demand drugs such as opiods

Government and Public Sector agencies

- Unemployment benefits fraud
- COVID19 Payment Protection Program

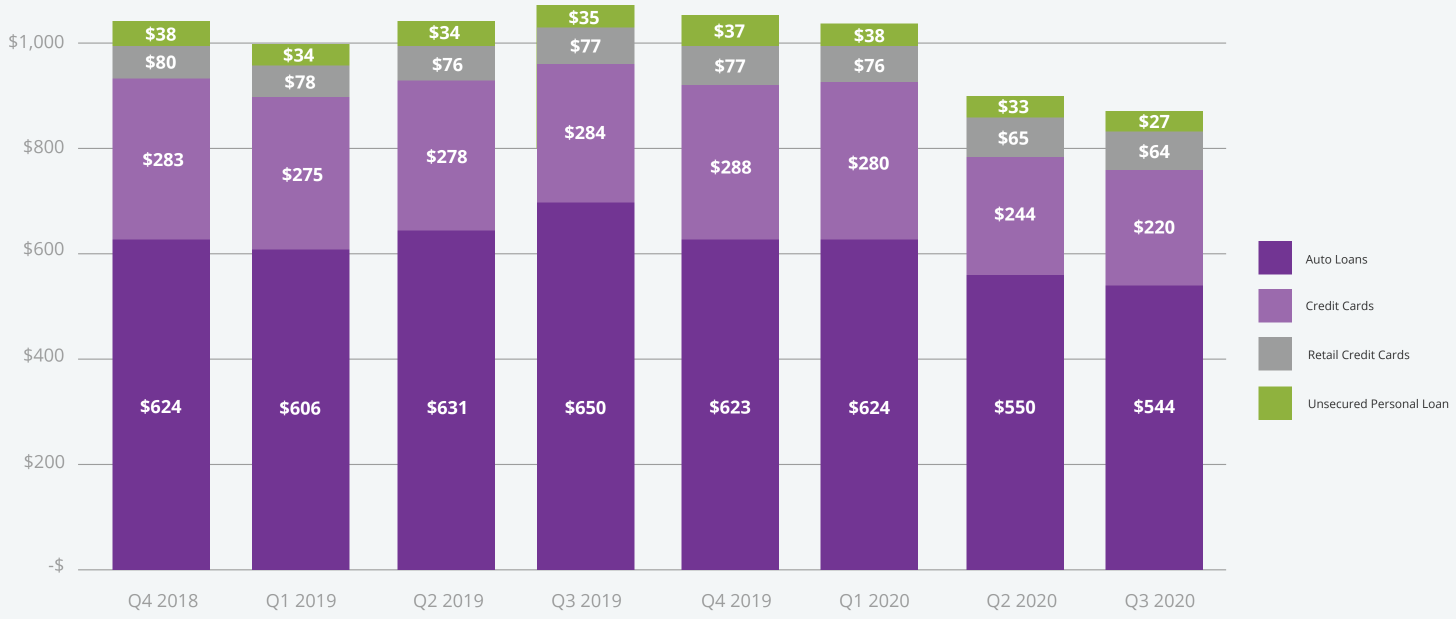
Insurance companies

- Fraudulent claims against personal, medical, or business losses
- Fake injuries brought to complicit medical center, then submitting falsified medical billings attached to fake identities, ultimately submitted as insurance claim
- Complicit auto body shops create false property damage claims

How Big of a Problem Is It?

As of the latest Transunion data available in Q3 2020, combined synthetic fraud balances spanning the Auto Loan, Credit Card, Retail Credit Card, and Personal Loan segments in that period totaled $855 million -- notably down from $1.03 billion in Q4 2018.

Outstanding Balances (in $Millions) for Fraudulent Accounts Opened with Synthetic ID



Source: TransUnion Feb 2021

Looking ahead, the Aite Group (contracted by Transunion) estimates that synthetic identity fraud for unsecured U.S. credit products will total US$1.8 billion in 2020, and it will grow to US$2.42 billion in 2023.

Looking at the synthetic identity fraud problem through another researcher's lens, IDC estimates that up to 20% of consumer loan and credit card charge-offs can be attributed to SIF. Per the Federal Reserve Bank (FRB), as of May 2020 the charge-off rate for consumer debt is about 2.4%.

The FRB data indicates that financial institutions in the United States at the end of May 2020 were holding approximately $2.2 trillion in consumer loan and credit card debt. That indicates that annual SIF charge-offs in the United States alone could be as high as $11 billion.

Given varying methodlogies employed by each respective researcher, the true monetary impact of SIF is difficult to settle on, but regardless of the actual number, the losses to our financial institutions are massive and increasing year over year. The net total costs are even more vast when accounting for the downstream operational costs associated with servicing and investigating fraudulent accounts, as well as any resultant compliance fines.

Solutions: Systemic & Tangible

eCBSV

Better late than never, true source verification of SSN is finally here, albeit for a limited set of “permitted entities”. In June 2020, the Social Security Administration (SSA) rolled out the “Electronic Consent-Based Social Security Number Verification“, or “eCBSV” for short, that provides a source of truth to cross-check an individual’s unique ID combination of SSN+Name+DoB to SSA records.

As mentioned, this service is only extended to “permitted entities”, which includes financial institutions or the service providers, subsidiaries, affiliates, agents, subcontractors, or assignees of the financial institution.

Notable exclusions from that list are companies that create or manage Consumer Services (gambling, social, ecom), Deposit accounts, and Business lending. True understanding of implications and impact of having synthetic identities exist in these ecosystems are TBD.

The eCBSV is expected to have two primary impacts on the multi-billion-dollar synthetic identity fraud landscape:

1. As the eCBSV gains full steam and adoption in the market, the creation of synthetic identities will slow as lenders gain the ability to cross-check customer PII (alongside authentic ID document) in real time. Its full implementation is expected to take some time given cost and inherent operational challenges in adopting new measures.

2. Fraudsters are expected to take advantage of the full rollout delay and ramp back up their synthetic identity fraud activities to create 1) sleeper (early credit establishing / cultivation) accounts now, while they still can and 2) fake goal bust-out accounts that take advantage of pandemic loan forbearance programs.

One key caveat of the eCBSV is that this process does not prove the identity of a prospective customer / borrower. It acts as just one vector of information for a lender to consider, alongside and concurrent with the fundamental process of forensic government issued document authentication.

The eCBSV check result will be a binary “Yes” or “No” that indicates if a provided combination of “SSN+Name+DoB” information matches the SSA records. It does not provide proof that the combination belongs to the person attempting to open or make changes to an account, or withdrawing funds.

Forensic Identity Document Authentication & Analytics

Once an institution has verified via eCBSV that a presented combination of datapoints is actually valid, only then should it link the data to an individual -- done via best available methods of forensic level document interrogation and authentication. The foundation of truth that ties an individual to a set of information is laid bare on a government issued identity document such as a driver's license, real ID, passport, military ID card, etc.

At this point of "identity proving" the consumer, the organization or institution should also capture and leverage this valuable "to-be macro" data. Instead of viewing identity authentications as just an individual act bound to a singular transaction at one point in time, view it as a contributing piece to an ever growing anti-fraud puzzle.

One detection and defeat of a potential fraudulent transaction is a momentary success. Two incidents of fraud detection at a linked location, or to a linked ID or transaction type, etc, is the start of a trend. Successive incidents / datapoints with similar characteristics could ultimately inform predictive and defensive measures.