FIVERITY

INSIGHTS FROM THE FIVERITY IDENTITY INTELLIGENCE HUB

2024 Synthetic Identity Fraud Report

Table of Contents

Understanding SIF as a Threat 01

The Federal Trade Commission data shows that consumer-reported fraud reached over

$10 billion in 2023

That marks a new level of losses, and a good portion of this statistic comes from Synthetic Identity Fraud (SIF).

Think of SIF as a merger of identity tags. SIF uses a combination of both legitimate personal identifiable information (PII) such as social security numbers (SSN) and invented designators like addresses and names for financial gain.

For example, using an SSN from a minor with no credit history but attaching a new name, DOB, and address confuses common fraud prevention systems, exploiting security gaps and allowing hackers to gain access to credit cards and bank transactions.

SSNs can be acquired through a variety of methods. From scams, dark web sales, where they only cost **$4 for a complete PII packet** with SSN, to data breaches of major institutions . Over time, these new PII packets are then nurtured through applications to loans and lines of credit to build creditworthiness – leading to larger loans and funding access.

In most cases, this SIF cultivation starts small. Low limits are reasonable starting points until enough history is grown so the fraudster can cultivate a strong financial presence. These fraudulent activities are both long- and short-term endeavors. PIIs are assessed for validity in the short term and grown in the long term for larger financial rewards.

Understanding the motivations behind SIF and the impact it can have on any bank or financial institution is crucial to preventing charge-offs and losses.

Why is SIF a Threat?

Thinking of SIF as a traditional form of identity theft is a mistake. They offer unique advantages to fraudsters due to the nature of the fraud versatility and detection difficulty.

SCALABILITY

Today, in the United States, there are around 0.505% of identities with multiple SSNs (excluding ITINs). That places the estimated number of identities with multiple SSNs in the US to roughly: 300M * 0.505% = **1,515,000**. While not all of these are direct cases of fraud, they highlight the high volume of SIF risk that exists.

With artificial intelligence and digital automation, it has never been easier for fraudsters to create millions of PIIs for testing and hacking using SIF.

EVASION

There is no direct consumer victim of SIF at the point of account opening. Where a traditional crime of identity theft would be noticed by someone getting a random bank charge or credit history claim, SIF has no active monitoring outside of the credit card or bank that issued the loan. Individual victims may be left with the time-consuming process of correcting their credit reports.

Hackers are well aware of the current US payment system and leverage AI-enhanced software and online tools to manufacture profiles that are increasingly difficult to detect.

VIRALITY

A SIF profile is not a single entity. Once a profile is established, up to five additional trade lines will typically follow. Criminals then "piggyback" on these profiles to expand their reach and diversity for more significant financial gain.

The total loss due to SIF can be estimated at $31.8 billion for a mature identity with an average of 7 accounts and an average loss amount of $3,000 per account and $30.3 billion under assumptions of 5 accounts per identity with an average loss of $4,000 per account.

$31.8 billion
7 accounts per identity

$30.3 billion
5 accounts per identity

HARM

With harder-to-track transactions, SIF proliferation can lead to criminal enterprises purchasing weapons, illegal narcotics, and other substances. This quickly becomes a pre-built manufacturing process where SIF is industrialized.

On the dark web, these rings have become FaaS (Fraud as a Service) organizations, often leveraging the sale of SSNs, credit card numbers, and health information to create pre-packaged PIIs in bulk.

How Did SIF Become a Problem? 02

SIF generation is a double-edged sword that highlights our advanced societal technology and the dangers of rapid online proliferation. It is a natural progression of financial fraud that adapts technology and automated tools to circumvent current regulations.

Financial institutions must remember that SSNs were not created to catalog the U.S. population. They were originally intended to document workers for the Social Security program and ensure the accuracy of employee reporting.

Since its inception in 1936, the world has changed drastically. Now, SSNs are used for everything from getting into college to applying for a passport. Such diversity was made harder to track when the SSA introduced number randomization on June 25, 2011. This effectively removed the check between the first three digits and the applicant's state on any credit or loan application.

1936
since its inception

2011
SSA introduced number randomization

The result is that fraudsters can now "make up" the first three digits, increasing their ability to commit SIF over a wide range of financial products.

In July of 2021, stricter standards were applied as the rollout of Consent Based SSN Verification (eCBSV) was introduced. This allowed approved banks and institutions to check the SSN of an applicant against the registered date of birth, address, and other personal details.

Fraudsters now look to move their operations outside the US, where financial institutions cannot conduct this eCBSV through the use of VPNs or physical relocation.

With the NY Federal Reserve Quarterly Report showing 2,305 million new credit card accounts originating between Q4 of 2022 and Q3 of 2023, finding a way to plug that gap in security is crucial to any institution's bottom line.

SIF loss rate

0.5%

~$35 billion

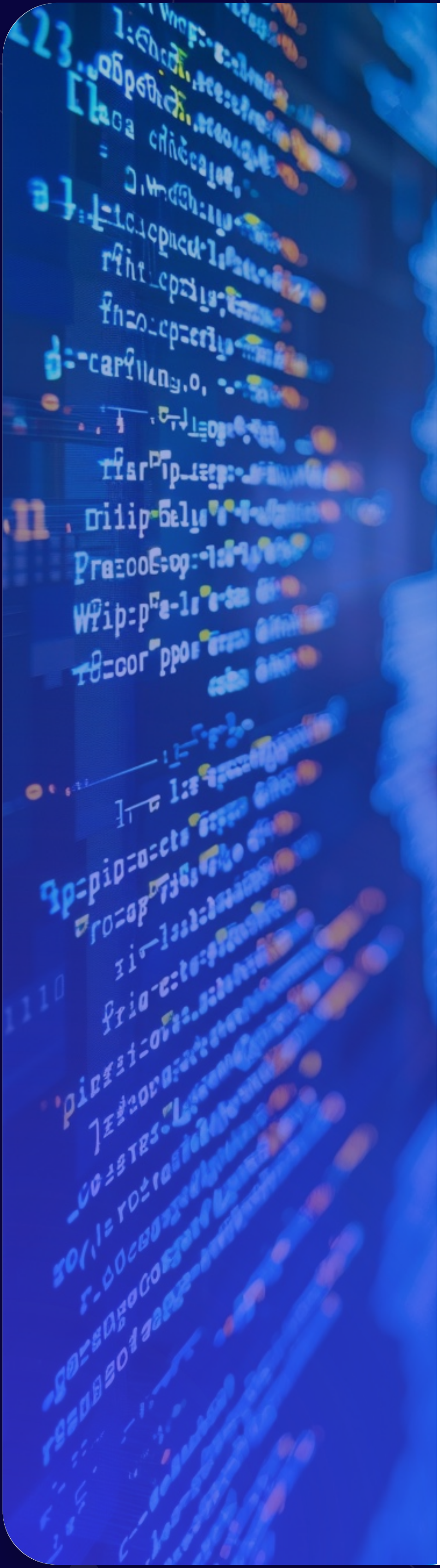
at an average CC loss

$3,000

per account in write-offs

If we only assume a SIF loss rate of 0.5% (half the industry average), we can estimate a total loss rate of ~$35 billion at an average credit card loss amount of $3,000 per account in write-offs.

The more data breaches become frequent and accessibility of real PII expands, SIF will only become easier to cultivate. The cheap cost of acquiring PIIs allows criminals to digitally barrage financial institutions struggling to keep up with the sophistication of this fraudulent activity.



Modern Evolution of SIF

When looking at any form of fraud, it is best to consider the incentive. The goal of securing additional funds from financial institutions and credit card agencies was made much easier during the global pandemic. The advent of online banking and the rush to move all societal operations into the digital space made things easier for fraudsters.

By one indication, the global Phishing and Fraud Report from F5 Labs showed that phishing attacks alone experienced a **220% increase during** the height of the worldwide pandemic. Combine that with the incentive of financial subsidies drawing out more criminal activity, and you have a "perfect storm" for greater demand for SIF attacks.

The problem is that most financial institutions do not have the tools that can maintain the speed and innovation hacking attacks are using. Modern SIF schemes employ everything from advanced algorithms to machine learning. Trying to mirror these innovations is like fighting a many-headed beast.

There is an urgent need to develop equally adaptive and sophisticated responses to SIF through an industry-wide effort. As more financial institutions embrace digital processes and engagement to maintain customer connections, a comprehensive effort must be made to detect, undermine, and resolve SIF attacks while ensuring identity trust.

In the first half of 2023, the U.S. auto lending industry saw one of the highest instances of SIF, with an increase in lost revenues and write-offs totaling **$1.8 billion**. That is only one sector of the many exposed to SIF.

Why is SIF so Hard to Detect?

Addressing Synthetic Identity Fraud (SIF) poses a unique challenge, as it does not always directly affect individual users as traditional identity theft does, often making financial institutions solely responsible for detection.

Given the substantial amount of data processed by the average financial institution, there is a heightened need for fraud detection and ongoing monitoring systems—tools that many organizations have yet to implement.

STEALTH

The very nature of SIF rests in its undetectable profile. As long as these attacks can fly under the radar of detection, they can be expanded and developed by fraudsters. That is why most SIF begins with smaller credit limits and thin loan applications.

Criminals cultivating these profiles will make minimum payments to lend validity to the account before going in for the "financial kill" of a bigger score.

EVOLUTION

Just as our modern society relies on AI and machine learning tools to create new systems and content across all industries, hackers are leveraging those same tools. As quickly as an adaptation to SIF prevention is created, AI backed tools learn to get around such regulations to continue receiving loan approvals and credit line access.

The result is a feedback loop helping inform fraudsters of what needs to be improved more than banks learning how to prevent future SIF.

Potential Loss Due to SIF

If we look at a two-component system for estimated SIF losses to the current economy, we begin to paint a picture of what is at stake.

Component 1

In the first component, we have losses due to new originations of loans and credit accounts. Based on the data of FiVerity's customers, the low threshold estimate of SIF loss rate is **~0.91%** and the high threshold rate is **~1.28%**.

According to the NY Fed Quarterly Report, the total consumer outstanding debt (excl mortgage) is $3202 billion. Then SIF exposure from outstanding debt is around $29.2 billion if we use the low threshold.

$3202 billion
consumer outstanding debt

$29.2 billion
SIF exposure

Component 2

In the second component, we look at losses due to credit charge offs. According to Experian (Javelin White paper), **20%** of credit loss rate is attributed to SIF that is undetected or miscategorized.

The total credit losses in consumer lending (mortgage excl) from Q4 2022 to Q3 2023 are $27.7 billion making the SIF exposure from charged off credit losses at $5.5 billion.

$27.7 billion
credit losses

$5.5 billion
SIF exposure

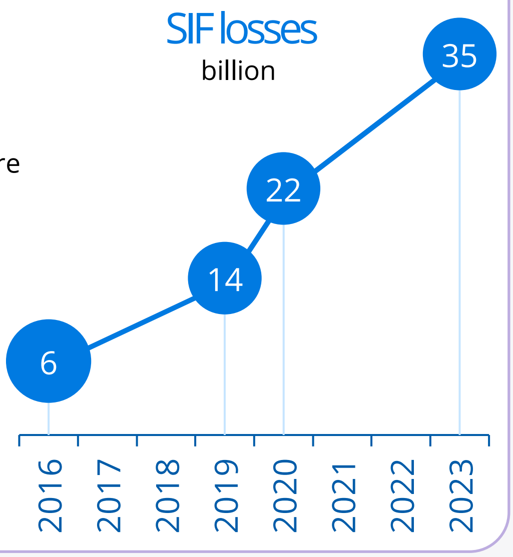
Total Losses

These two components combined place the total SIF exposure of current financial institutions at an estimated $35 billion in losses.

$35 billion
total SIF exposure

From a historical perspective, you can see the increase in SIF losses. SIF has been increasing during the past several years.

If left unchecked, SIF poses a significant threat to the economic stability of financial institutions at a global level.



What Does a SIF Account Look Like? 03

The nature of Synthetic Identity Fraud (SIF) has become increasingly elusive, with fraudsters constantly refining their tactics to circumvent detection. While Financial Institutions (FIs) are quick to close accounts they identify as fraudulent, many sophisticated SIF accounts remain undetected due to their resemblance to legitimate customer profiles. These accounts often go undetected, masquerading as poorly underwritten but genuine accounts.

FiVerity's analysis reveals that the behavior of older SIF accounts—those that have evaded initial screening processes and have been active over time—is particularly challenging to discern. Typically, these accounts exhibit a pattern of rapid credit utilization, swiftly ramping up charges to 25% to 50% above their initial credit limits shortly after account opening. This strategy is a red flag for FIs, signaling potential bust-out fraud, where the fraudster maxes out the available credit with no intention of repayment. On average, the damage per incident can soar to an estimated $90,000.

However, the financial impact is often compounded by additional deception. In a nefarious twist, fraudsters have been known to feign victimhood, falsely claiming that their 'identity'—which is, in fact, synthetic and fabricated—has been stolen. By exploiting the identity theft claims process, they aim to extract double the financial benefit before the account is shut down. This bold strategy not only increases their ill-gotten gains but also complicates the recovery process for FIs, as they must navigate the murky waters of purported identity theft, further illustrating the sophistication and audacity of modern-day fraudsters.

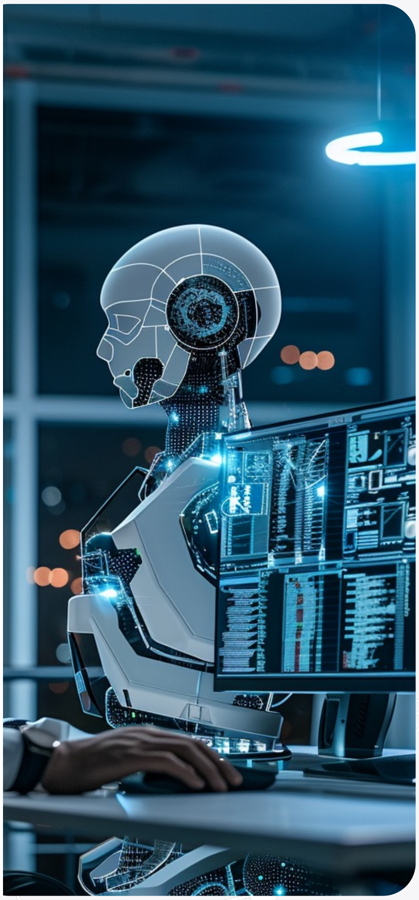
Fighting Back Against SIF

Automation

Hackers achieve all the same benefits of automation as any financial institution. Leveraging tools like machine learning (ML), artificial intelligence (AI), natural language processing (NLP), and automation allows for SIF to adapt and innovate at rapid speeds.

As an industry, we can apply these same technologies in detection and prevention. For example, cutting down on multiple inquiries from the same IP address or preventing high application volume over a short period of time from processing.

The goal is to find the underlying patterns of fraudulent accounts and applications, as well as the positive signals of real, trustworthy customers. Once identified, these can create a “bottom up” approach to detection, allowing profiles that retain certain red flags to be slowed, blocked, or stopped before securing funding through the integration of machine learning.



Industry Collaboration

Effective Synthetic Identity Fraud (SIF) mitigation hinges on the seamless and secure exchange of intelligence between the financial institutions often involved in cultivating SIF profiles—typically five to ten banks or lenders. However, the timely sharing of this data is hampered by concerns over competitiveness, user privacy, and logistical challenges. To overcome these obstacles, passive, secure information sharing mechanisms need to be integrated directly with detection systems. Additionally, dismantling data silos is essential for accessing historical threat intelligence, empowering teams across various institutions to synthesize identifiable data and recognize SIF patterns.

To complement these efforts, education and strategic communication must be prioritized. Establishing 'cyber fusion' centers can be a transformative strategy, combining the expertise of cybersecurity professionals with the historical insight of fraud analysts to foster a more comprehensive understanding of SIF threats within organizations.

Updating the Approach

The simple truth is that SIF is the evolution of legacy attacks. The only way to ensure current FIs can fight fire with fire is to adapt and evolve. Relying on legacy systems that prevent older forms of identity theft is no longer acceptable, given the current state of SIF and other modern attacks.

Leveraging tools like ML, AI, and automation from the institutional side of the equation equips organizations with much-needed preventive and defense capabilities. Once these fraudsters have been exposed, sharing that information with others inside the industry ensures that future attacks using similar identifiers are stopped before they can steal any additional funds.

Measuring Digital Identity Trust to Defend Against SIF 04

The education of SIF inside the industry and development of tools that can combat such attacks in real time is crucial to the stability of today’s economy. Approaching this challenge from a multi-faceted, holistic standpoint allows organizations of all sizes to develop strategies that should slow, if not remove, the damage done by SIF.

FiVerity's strategy elevates the fight against Synthetic Identity Fraud (SIF) by combing cutting-edge technology and industry-wide collaboration. In the face of increasingly complex financial crimes, our platform's combination of shared intelligence, machine learning, and AI is indispensable.

FiVerity's models swiftly adapt to the nuanced tactics of fraudsters, employing sophisticated algorithms that pinpoint and respond to suspicious behavior. By providing easily understandable, actionable insights on digital identities, FiVerity equips every level of a financial institution to take action. This proactive approach not only curbs the spread of fraud but also arms the financial community with the collective understanding and agility essential for preempting the cybersecurity threats of the future.

Getting Started with FiVerity

FiVerity is the leading solution to aiding financial institutions in digital identity trust, risk, and fraud prevention. Stopping criminal enterprises from accessing funding sources is a challenge and FiVerity helps by leveraging machine learning to quickly identify threats as they evolve, boosting an institution's fraud detection rates by over 50%.

Beyond prevention and detection of SIF, FiVerity's real-time information sharing ensures the shared intelligence needed between banks, credit unions, regulators, and law enforcement agencies is assured. This exponentially multiplies every organization's ability to identify and learn from patterns emerging in both SIF, and the identity fraud sector as a whole.

Learn more about FiVerity's Digital Identity Trust Platform by visiting

www.fiverity.com