IDOLOGY
a GBG company

WHITE PAPER

Leveling the Playing Field: Using Tech to **Balance Fraud Prevention** with Frictionless Digital Experiences

What financial institutions can do to improve customer growth while fighting synthetic identity fraud.

Contents

Introduction

Few things are more important to businesses today than **transacting with trust**

As the threat of synthetic identity fraud (SIF) continues to grow, a robust multi-layered digital identity varication program is key to optimizing the balancing act between fraud and friction. Few things are more important to businesses today than transacting with trust, and to stay competitive, FIs must also be relentless in their pursuit of technology solutions to deliver a smooth, seamless, and secure digital experience. Using the wrong approach can prove costly, allowing fraud losses to grow and degrading the customer experience.

Trust is a critical component of every digital interaction. Losing a customer's trust when the security or experience of a digital interaction fails to meet their expectations can have significant and long-lasting implications, especially if competitors can deliver a better experience.

The right identity verification solution can both make it more difficult for fraudsters to profit and improve customer experience. For example, identity verification, which includes the ability to scan and verify physical documents, can thwart a fraudster's efforts while also onboarding customers faster and without friction.

Simply put, fraud prevention no longer has to come at the expense of customer experience. SIF is a threat that financial institutions need to protect against, but introducing unnessary friction will result in a poor customer experience. Solutions exist that allow businesses to deliver a flawless digital experience while preventing fraud.

Synthetic Identity Fraud, A Growing Problem.

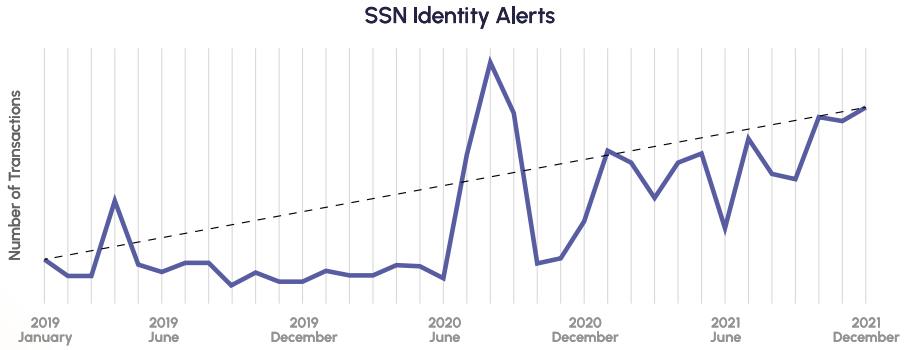
Only 22% of Americans claim to know what Synthetic Identity Fraud is.

4th Annual Consumer Digital Identity Study, IDology, 2021

So how big of a problem is SIF, and what can financial institutions do to gain the upper hand?

As with most forms of fraud, estimates vary regarding the magnitude of the losses. Aite Group estimates that synthetic identity fraud will continue to grow over the next couple of years, with losses projected to reach more than $4.1 billion by 2023. IDology's Eighth Annual Fraud Report noted that 43% of fraud executives across multiple industries reported increases in synthetic fraud in 2020, up from 40% in 2019, 36% in 2018, and 31% in 2017. Additional research shows that only 22% of Americans claim to know what SIF is.

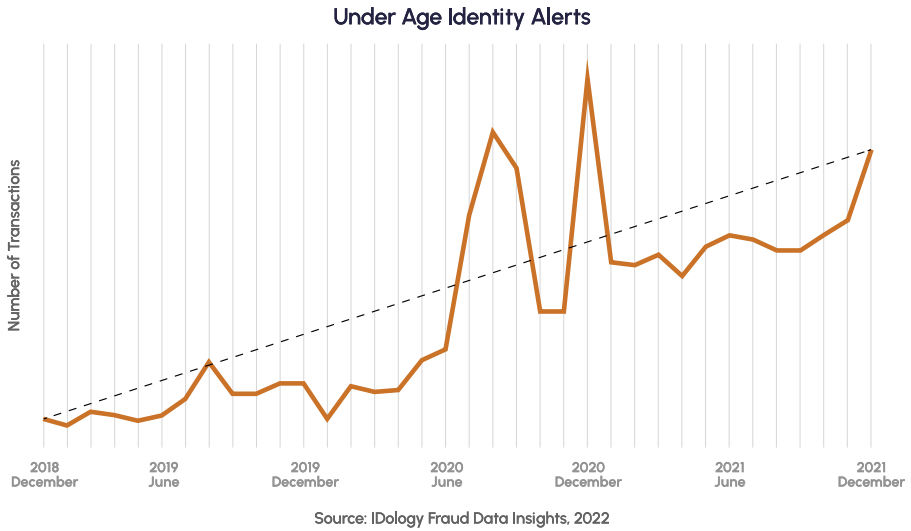
IDology's transparent identity platform, ExpectID®, uniquely enables clear data capture of SIF indicators by business to better understand synthetic identity fraud. The data collected points to SIF's targets and recent surge at a macro level. Furthermore, the data trends demonstrate the power of multiple layers of SIF detection and deterrence. When user-inputted social security numbers (SSNs) don't match record data, there is a strong likelihood of fraud, and this trend appears to be growing. The graphs below show that the rate of mismatched SSNs has steadily increased since 2020.



Source: IDology Fraud Data Insights, 2022

Unfortunately, those who often suffer the most from SIF are vulnerable populations, including young, elderly, and deceased individuals. These demographics are vulnerable for different reasons, but they all have something in common. In addition to being vulnerable to SIF, data from IDology shows that all three groups have seen a progressive increase in SIF rates.

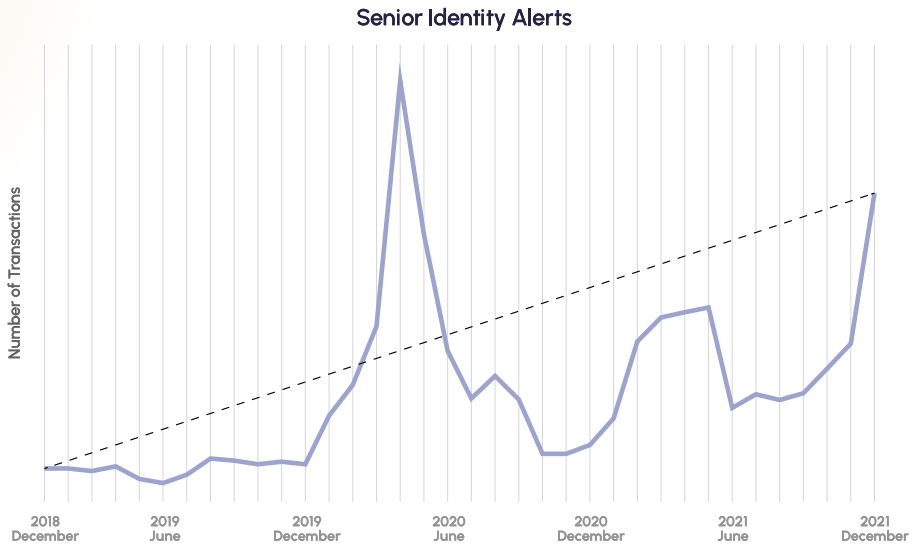
Fraudsters often use the social security numbers of young people to build synthetic identities because they haven't begun transacting yet. Additionally, most parents are not actively monitoring their children's credit reports for fraud. Experiencing identity theft at a young age can result in an inability to receive financial aid for college, buy their first car, or rent an apartment. The graph below illustrates how threats to the identities of young people have increased year over year.



Source: IDology Fraud Data Insights, 2022

Those who often suffer the most from Synthetic Identity Fraud are **vulnerable populations**

IDology transaction data also shows an increase in the number of elderly identity alerts over time. The senior population is target for SIF, since fraudsters are drawn to older people for a variety of reasons. Limitations in mobility or cognition may make some elderly individuals more vulnerable to manipulation. As the chart below shows, identity thieves know older people have greater wealth than other generations and the potential to deliver an increasingly enticing payoff when targeted as part of a SIF scheme.



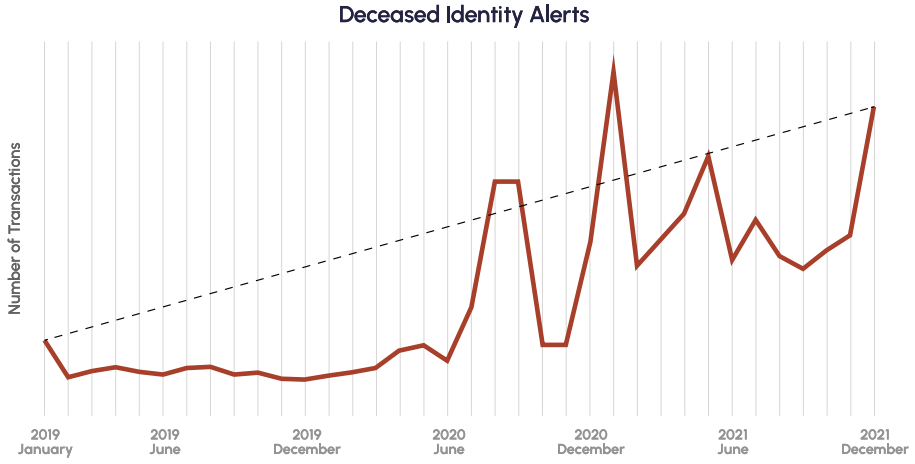
Source: IDology Fraud Data Insights, 2022

More than 2.5 million

identities are stolen from deceased individuals each year.

Source: 2021 Identity theft statistics, Consumer Affairs, 2022

The generation of synthetic identities from deceased individuals is unfortunately not new. According to Consumer Affair's 2021 identity theft statistics, these synthetic identities often remain under the radar, with family members not noticing the theft for months or years more than likey due to COVID seeing a spike. Consumer Affairs estimates that more than 2.5 million identities are stolen from deceased individuals each year. Given the trajectory of this type of fraud is also increasing, banks have even more reason to stay focused on the threat of SIF.



Source: IDology Fraud Data Insights, 2022

Machine Learning, Trust, and the Power of Fraud Intelligence

Tackling SIF requires a comprehensive strategy underpinned by technology to combat the threat without degrading the customer experience. Artificial intelligence (AI) and machine learning (ML) can play a critical role in the process, as they can quickly scrutinize vast volumes of digital data to uncover fraud. Essentially, machine learning serves the role of a high-performing human fraud analyst but scales up the efficiency and speed.

While machine learning can detect established schemes, it needs help learning new attack vectors. With access to fraudulent transactions across multiple industries, a trained fraud analyst accompanied by effective machine-learning technology can catch both new and established fraud trends, including novel threats that AI may miss on its own.

A ML-powered solution that incorporates ID document verification allows an institution to authenticate an ID. It can also help determine if the person presenting the ID is the same individual whose picture appears on the document. Such technology can accelerate customer onboarding and authentication, especially for thin file customers who may otherwise fail varication or be required to present proof of ID in person. It can also remove the need to manually verify an ID and help ensure compliance with regulatory requirements. Machine learning performs what fraud teams can do at scale.

There is an inclusion benefit here, too. ID document verification enables thin-file customers, such as people who are young, new to the country, or have a small digital footprint, to access products and services.

And while difficult to quantify, robust ID document verification with mobile scanning capabilities helps establish and maintain a customer's trust, which is increasingly difficult to accomplish yet remains critical to conducting business in the digital realm. Building trust not only creates a positive first impression, but also contributes to customer lifetime value.

As our research and experience show, when onboarding new consumers, security is paramount. Most individuals want to know that you are protecting their data, and identity verification provides evidence of that commitment. They also want to understand how their data will be used. Therefore, trust is earned through action and transparency.

Since fraud schemes evolve and it takes time for fraudsters to create and perfect their approach, learning how SIF happens elsewhere can help level the playing field. Transaction data shared by related and unrelated companies in a consortium network provides an unparalleled view of fraudulent activity and generates valuable cross-industry insights. Understanding how fraud travels enables FIs to take a proactive approach to combatting emerging fraud schemes.

Artificial intelligence, ID document verification, and cross-industry fraud intelligence, alongside the full suite of tools in a high-performing solution, deliver a multi-layered approach to combatting SIF and other forms of fraud. This provides sufficient hurdles for fraudsters while also making it seamless and straightforward for legitimate customers to prove their identity.

Bridging the Gap Between the Physical and Digital Worlds

IDology transaction data spanning several years shows the increasing growth of SIF. A strong identity verification program means that financial institutions no longer need to accept being two or three steps behind fraudsters. Furthermore, as customer expectations regarding the digital experience change, every financial institution will face unrelenting pressure to make the user experience as safe, secure, and easy as possible.

While combatting fraud is the primary goal, modern identity verification tools can unlock new revenue streams by establishing relationships with individuals with thin credit files or those who have yet to engage in digital transactions. A multi-layered solution with transparent data results is critical in balancing optimal onboarding with deterring synthetic identity fraud.

To compete in today's digital-first environment, financial institutions must cross the chasm between relying on physical branches and delivering every form of banking in a digital environment. Identity verification solutions can help financial institutions make the leap, especially when they provide a multi-layered approach, including physical ID document authentication and verification.