IBIA International **Biometrics+Identity** Association

Synthetic Identity Fraud:
Only Biometrics Can Stem Billions in Bank Losses

by **David Gerulski**

Overview

Most are familiar with "traditional" consumer identity theft; criminals acquire personal financial information to gain access to the victim's bank and/or credit accounts to steal money. Thieves also often steal Social Security numbers and other information which they use to open new bank or credit card accounts. Victims can incur significant financial losses and h ve their life's credit history destroyed. Annual losses from this type of crime are estimated at $2 billion per year in the US alone.

> **"Synthetic identity fraud is not a problem that any one organization or industry can tackle independently, given its far-reaching effects on the U.S. financial system, private industries – such as healthcare, automotive and insurance – government entities and consumers."**
>
> US Federal Reserve

Synthetic identity fraud is different. It can be thought of as a hybrid form of identity crime whereby perpetrators leverage stolen elements of real identities to manufacture entirely new, "virtual" identities for the purpose of opening accounts with financial institution .

In its July 2020 report, "Mitigating Synthetic Identity Fraud in the US Payment System," the US Federal Reserve explained SIF in this way: "Synthetic identity fraud occurs when perpetrators combine fictitious and sometimes, real information, such as names and Social Security numbers (SSNs), to create new identities…to defraud financial institutions, government agencies or individuals." Report

McKinsey & Company explains that most synthetic identities are created: "…by applying for credit using a combination of real and fake, or sometimes entirely fake, information. The application is typically rejected because the credit bureau cannot match the name in its records. However, the act of applying for credit automatically creates a credit file at the bureau in the name of the synthetic ID, so the fraudster can now set up accounts in this name and begin to build credit. The fact that the credit file looks ide tical to those of many real people who are just starting to build their credit record—that is, there is limited or no credit history—makes the scam nearly impossible to detect."

While measuring the full impact of this type of fraud is complex, the Auriemma Group has estimated that synthetic identity fraud accounted for a full 20 percent of lender credit losses in the US in 2016.

What sets SIF apart from traditional consumer identity theft is the fact that virtual identities do not trigger alarms. Virtual holders are "synthetic" – not based on or connected to a real

David Gerulski is Executive Vice President for Integrated Biometrics (IB) and a chamption for the use of IB's patented light emitting sensor (LES) technology in securing the rights of identity for citizens of developing nations. David speaks regularly at biometric industry gatherings and on topics ranging from border security and national ID programs to biometrics in healthcare.

human. Since the accounts customarily exhibit "normal" behaviors, they don't trigger even the most advanced analytics software, making it possible for criminals to operate for months or even years before fraud is detected. In addition, criminals typically use these fake accounts responsibly for a time to build up the account's credit score, as higher credit scores lead to greater opportunities for the account operator down the road:

> **"According to Jacobs (CEO, DAL Global), a system that joins biometric identity with an online identity is absolutely vital in preventing SIF: "Only such a system can firmly and undeniably link a unique, real-world human being to their digital record, nullifying current and preventing any future synthetic identities."**

"According to a study by ID Analytics, fraud models built to predict traditional identity fraud did not flag 85% to 95% of potential synthetic identity fraud applicants." - US Federal Reserve System, ibid.

Often, the tactics used to cultivate synthetic identities differ from those used to perpetrate traditional identity fraud. For instance, synthetic identity fraud takes place over a longer period, as fraudsters open multiple accounts to build a positive credit history for the synthetic identities in order to maximize their eventual payoff.

Yet SIF is not always committed with the purpose of stealing money from financial institution . There have been cases involving undocumented immigrants who use invented or stolen SSNs to obtain traditional financial se vices. While still committing a form of fraud, these perpetrators did not set out to steal from financial institution , but rather to get access to banking and credit services for the purposes of making and receiving payments.

Biometrics: The Best Way to Fight Synthetic Identity Fraud

Biometric identific tion technologies offer the only solution for eliminating SIF. While government regulators have called for advances in technologies to address this growing problem, they acknowledge that "most traditional identity fraud tools are ineffective at detecting synthetic identity behaviors and characteristics" because they cannot quickly and accurately determine whether an identity is real or synthetic.

The growing risk of this type of criminal activity leaves most of the US banking system playing a dangerous game of "catch up," risking losses as well as fine .

This creates enormous opportunity for the biometrics industry.

A report from Javelin Strategy concluded that the priority for banks is to "…authenticate the consumer from beginning to end," noting the importance of establishing "the true identity of the consumer."

Biometric identification and verification technologies are recognized around the world as the fastest, most accurate and secure method for proving an individual is who they say they are. Whether used to confirm the right to access banks, air travel, borders, sensitive facilities, government benefits or voting privileges, the world has an increasing level of comfort with and confidence in biometric identification.

"The rising tide of Synthetic Identity Fraud has placed financial institutions in a very difficult position," said Dawid Jacobs, a leading expert on identification verification and CEO of Maryland-based DAL Global. "Current technologies can't spot synthetics, yet regulators demand banks report on and address money laundering and related fraud. If they report these crimes, it may signal regulators they're not in full compliance. If they fail to report, they may be ignoring potentially massive losses and liability due to Synthetic Identity Fraud."