TESTIMONY OF AMY WALRAVEN

Founder and President of Turnkey Risk Solutions

Before the

Task Force on Artificial Intelligence

United States House Committee on Financial Services

Hearing on "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"

September 12, 2019

Chairman Foster, Ranking Member Hill, and members of the task force, thank you for the opportunity to appear before you and provide testimony today to help inform discussions on the future of Identity in the Financial Services sector: threats, challenges, and opportunities.

My name is Amy Walraven. I'm the founder and president of Turnkey Risk Solutions (TRS). TRS is a risk management company specializing in the development and application of highly complex algorithms specifically targeting emerging fraud threats. Prior to starting TRS, I spent over 20 years in the financial services sector at several major financial institutions. I have been a career risk manager primarily focused in the areas of fraud, risk, and compliance. The last 10 years of my banking career were spent at J.P. Morgan Chase. I was responsible for establishing business practices specifically focused on the proactive identification, mitigation, and remediation of various fraud threats including but not limited to credit bust outs, identity manipulation, credit abuse, and synthetic identities.

As we consider how to utilize artificial intelligence and machine learning to navigate big data to identify consumers, it is important that we clarify our target by gaining a more comprehensive understanding of what synthetic identities are. I have been asked to provide the committee a brief overview of the factors that contributed significantly to their emergence in order to better frame the threats and challenges the future of identity is facing in financial services.

For the purposes of my discussion, a synthetic identity is one that is created with a combination of potentially real and/or fake information like a Social Security Number (SSN), name, address, date of birth, etc. to create a new fictitious identity. It is important to note that creating a synthetic identity is materially different than traditional identity theft. In cases of traditional identity theft, the criminal is impersonating a real person by using that person's true identity elements to potentially open accounts and commit fraud in the victim's name or take over existing accounts held by that individual. In cases of synthetic identities, the criminal may be using limited elements of a true person's identity –for example, just their social security number and then leveraging that one piece of information to create an entirely different persona that is completely separate and distinct from the real person.

Once that synthetic identity has been created it can be leveraged just like any conventional identity. For example, it can be used to open bank accounts or apply for loans and other products in the financial

services sector. However, synthetic identities are not limited to just financial services. They can establish a presence on social media, be used to purchase cell phones or insurance policies, rent apartments, obtain utilities, enroll in benefits programs, etc. These identities can be used for whatever purpose suits the creator and/or manager of the synthetic identity.

To better understand the threat of synthetic identities, I believe it's important to understand the current landscape and the factors contributing to this rapidly growing identity fraud issue. There are four major factors contributing to the emergence of synthetic identities. They are as follows:

1) Technology – advances in technology have increased convenience, speed, and provided anonymity for the criminals. In addition, the aged infrastructure makes it difficult to combat today's threats.
2) Consumer awareness – consumers are more informed on the credit infrastructure and different fraud threats. They expect immediate access and decisions and understand the power of social media. Criminals are using those same resources designed to inform consumers to reverse engineer and help formulate their attacks.
3) Regulations and new controls - Consumer protection agencies and legislation are in place to provide consumers who have been a victim of identity theft a wealth of enhanced protections and benefits. Those same regulations and controls have had unintended consequences. We have seen those same protections be exploited, leveraged, and abused by criminals. Adding chips to credit cards to reduce counterfeit activity forced the fraud into other channels like card not present and synthetic identities.
4) Data Breaches – originally were focused on compromising credit/debit card data, those types of breaches are inconvenient for the customer and can be expensive for the issuer but can typically be resolved fairly quickly once detected. Many breaches have shifted to targeting personal identifiable information or PII allowing criminals to create entire profiles on individuals and use them to commit fraud or package them up for sale.

All of these factors have played a major role in the emergence of the use of synthetic identities. This fraud threat was specifically engineered to evade existing controls while exploiting vulnerabilities in the financial system and beyond impacting other industry verticals. Many of the groups committing this type of fraud are: highly organized, extremely sophisticated, and tend to be transnational in nature. These adversaries are focused, committed, well-funded, and have access to the same technological advances as we do. As an industry, we must be proactive in our actions, unified in our defenses, and more effective in our application of evolving technologies including artificial intelligence.

As we seek to deliver unprecedented speed and convenience to increasingly mobile and technology dependent consumers and businesses, we must remain vigilant in understanding the threats to our interests. Synthetic identity fraud in the United States and around the world is widespread and inconceivably pervasive. It is being amplified by increased digitalization of products and processes when coupled with a proliferation of available data; synthetic identity fraud readily operates across all delivery channels, providing the perpetrators with potentially unfettered access to our nation's financial system and federal programs -- making it essential that we act in a unified and collaborative manner to protect the integrity of our infrastructure.

In order to do so, we must recognize the complexity of these next generation fraud types and be fully informed on their severity and scope. Advances in technology alone cannot identify and resolve these

issues. Mitigation efforts from industry and government must be fluid and nimble to ensure we have the ability to effectively address these issues with urgency they deserve. Our control framework needs to be updated to specifically address synthetic identity fraud. It needs to be universally defined, in order for institutions to detect, report, and remediate it.