November 3, 2021

The Honorable Ed Perlmutter
Chairman
Subcommittee on Consumer Protection
and Financial Institutions
Committee on Financial Services
U.S. House of Representatives

The Honorable Blaine Luetkemeyer
Ranking Member
Subcommittee on Consumer Protection
and Financial Institutions
Committee on Financial Services
U.S. House of Representatives

Dear Chairman Perlmutter and Ranking Member Luetkemeyer:

On behalf of SentiLink, I am pleased to submit this statement for the record for your hearing titled "Cyber Threats, Consumer Data, and the Financial System." SentiLink provides industry-leading solutions to prevent synthetic fraud, identity theft, and other emerging fraud vectors at the point of account origination.

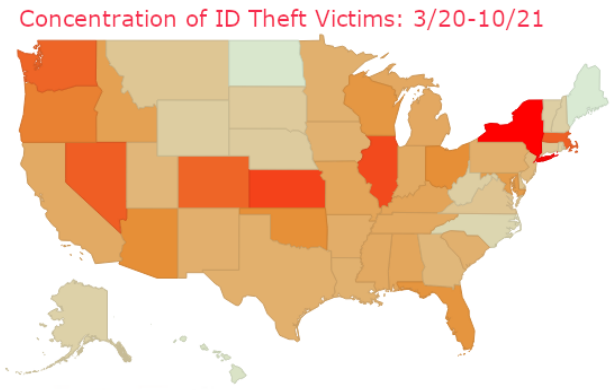
Cyber threats from nation-states and other well-organized actors are unquestionably a serious concern for policymakers and the financial services industry. As the Committee's hearing memo notes, attacks can take many forms -- from those designed to take down a financial institution's network and disrupt critical functions, to attacks targeted at individuals. These more localized, personal attacks all have a common theme: Compromising or manipulating identity data in order to commit fraud.

Of particular importance, I would like to highlight the increasing risk to the financial services industry from synthetic identity fraud (SIF). This type of fraud occurs when a criminal engineers a fake person using a fictitious name, date-of-birth and Social Security number (SSN). When this fake identity is used to apply for a financial product, it leads to the creation of a credit report for the made-up identity. Over time, and after an amount of artificial "credit building," the synthetic identity is used to open new accounts for purposes of commiting bust-out fraud, laundering money, or other financial crimes.

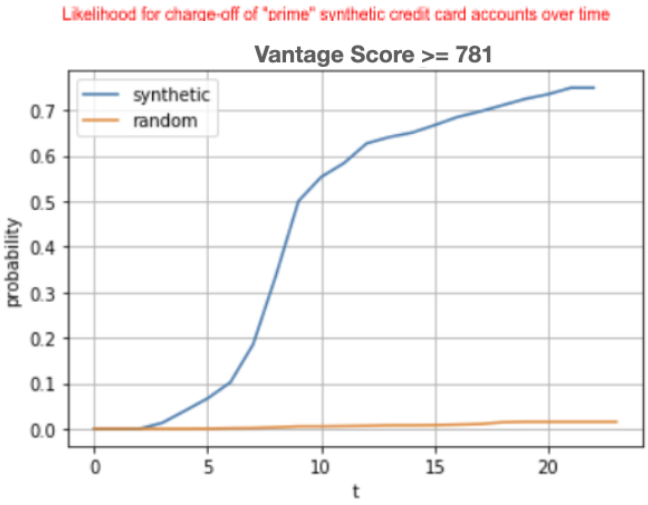
While SIF costs US lenders billions of dollars in losses annually, the financial industry isn't the only target. As the COVID pandemic revealed, governments at all levels can also be impacted by SIF. As we described in a previously submitted statement to the Committee, we have been able to identify synthetic identities, entirely fictitious businesses, and real businesses with fictitious employees that applied for various pandemic relief funds.

More broadly, identity crimes are a widespread problem that impacts the safety and soundness of the banking system, and financial health of US consumers. **We analyzed data from a sample of our financial institution partners and found that during the pandemic, a high concentration of**

identity theft victims whose data was used to apply for accounts were located in New York, Illinois, Kansas, Colorado, Nevada and Washington (as illustrated by the darker colors on the accompanying map). While criminals themselves and their associated fraud rings are still heavily concentrated in "hot spots" like Florida and California, our analysis demonstrates that victims are dispersed throughout the country.



For financial institutions, our analysis of the behavior of synthetic identities over time reveals the potential for increased financial losses. **Looking at the credit card market, for example, our data -- shown in the chart below -- illustrates how synthetic identities that have been built to a "prime"-level credit score tend to charge off 75% of the time within 23 months for an average loss of $13,000, compared to the performance of legitimate consumers who would be expected to charge off at a rate of 1.5% during the same time.** It is also important to recognize the impact on the broader financial system when identity and know-your-customer (KYC) safeguards are undermined by synthetic fraud.



Policymakers must ensure that robust identity verification requirements -- including for identity theft and synthetic identities -- are baked into the fundamentals of KYC rules and regulations. As we've observed, the risk to financial institutions of all sizes and charter types from identity fraud exists across the spectrum of financial products and services, including with basic checking account offerings.

We appreciate the opportunity to provide these comments and look forward to engaging with you and your colleagues to advance policy solutions that protect American consumers and businesses from identity crimes.

Sincerely,

Jason Kratovil
Head of Public Policy