April 28, 2022

The Honorable Maxine Waters
Chairwoman
2128 Rayburn HOB
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member
4340 O'Neill HOB
Washington, DC 20515

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of SentiLink, I am pleased to submit this statement for the record for your hearing titled “Oversight of the Financial Crimes Enforcement Network." SentiLink is a leader in identity verification technology. With real-time scoring capabilities, our models target synthetic identities – both first-party and third-party – which are often missed in basic Know Your Customer ("KYC") and Customer Identification Program ("CIP") processes, as well as identity theft. Further, our KYC Insights tool helps our partners by uncovering insights about identity risks, empowering financial institutions to make better identity decisions.

The Financial Crimes Enforcement Network ("FinCEN") plays a vital role in crafting the rules intended to combat identity crimes. Those rules, including the risk-based KYC and CIP frameworks, are out-of-date and not meeting the threats posed by the changing fraud landscape. As such, SentiLink encourages the Committee to focus on the need for modernizing the requirements around identity verification in the financial industry. In particular, we offer the following:

- CIP rules should provide greater clarity and specificity with regards to what constitutes a "reasonable belief" of identity verification, and should focus on the changing nature of the actual criminal threats financial institutions face, agnostic to the specific product or service for which a consumer is applying.
- Checks for synthetic identity fraud should be a core feature of CIP rules, FAQs and guidance.
- CIP rules should reflect the reality of the changing nature of identity fraud, and require the collection and additional verification of address, phone or e-mail, depending on the means by which an institution contacts their customers.

Existing Risk-Based KYC Rules Fuel Identity Theft and Miss Synthetic Identities

<u>Identity theft, Checking Accounts and the Pandemic</u>
The foundation of the CIP rules rests on the basic but critical premise that a financial institution must "form a reasonable belief that it knows the true identity of each

customer."[1] These rules have been deliberately drafted to require risk-based procedures. For example, current rules make clear that an application for a "resident consumer account" (i.e., a basic checking account) requires less identity diligence -- compared to, for example, a high net worth private banking application -- because it is a lower-risk product.[2] However, identity fraud has evolved in such a way as to make this assumption unreliable as the challenge of identifying what constitutes risk for a financial institution is no longer as obvious.

This was brought into focus during the pandemic, where fraudsters would use stolen identities to open "low-risk" checking accounts with ease in order to apply for government relief funds. When the funds were received into these checking accounts, they could be laundered through a myriad of other financial accounts. *Overall, from September, 2020, to June, 2021, the percentage of applications for demand deposit accounts identified by SentiLink as using stolen identities increased 187%.*

Missing Synthetics

Synthetic identity fraud occurs when a criminal engineers a fake person. Often this involves a true name and date-of-birth but a not-yet-issued Social Security number ("SSN"), or one issued to a minor. Another method involves a fictitious name and date-of-birth, but paired with a valid SSN.

As a typology, synthetic identity fraud has been designed to circumvent basic KYC/CIP processes. As such, it is no coincidence that basic identity verification processes fail to detect it with such regularity. 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 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. In fact, we've found up to 10% of a credit card issuer's chargeoffs are actually due to synthetic fraud.

The Means of Communication Matters More for Identity Verification

In general, to comply with existing CIP regulations, a financial institution must obtain information on a potential customer's name, date of birth, identification number and address prior to opening an account.[3] However, reliance on a consumer's address has

[1] 31 CFR 1020.220(a)(2)
[2] See "Appendix K" in the FFIEC's BSA/AML Manual for Examiners.
[3] 31 CFR 1020.220(a)(2)(i)(A)

created a regulatory gap: Modern identity thieves regularly leverage this well-known CIP compliance formula of a legitimate person's name + date of birth + identifier + address PII combination -- but paired with a means of electronic communication controlled by the fraudster -- to successfully obtain credit. An application with a street address that ties to the applicant is no longer a reliable signal that the applicant is legitimate. Given the high rate of data breaches, simply knowing a name, date of birth, identifier and address is not sufficient to determine a person's identity.

To support this conclusion, we examined just over 92,000 checking account applications over the last year that our models indicated as likely based on stolen identities. Of those:

- Nearly 55% had a consistent address history of at least two years. Of those:
    - 68% provided known risky VoIP numbers, and 82% of the phone numbers provided had an area code with no connection to the applicant.
    - 77% included a brand-new e-mail address or one that had been created less than two months before the application date.

Conclusion

Thank you for the opportunity to provide these comments. Technological change has revolutionized the way consumers and businesses access the banking system. In many cases, these innovations have fully digitized and automated the account origination process. While this has many advantages -- such as reducing costs, increasing efficiencies, and reaching new and underserved consumers -- it has dramatically heightened the importance of strong customer identity verification procedures. We look forward to engaging with you and your colleagues to advance policy solutions that protect American consumers and businesses from identity crimes.

Sincerely,

/s/

Jason Kratovil
Head of Public Policy