February 14, 2022

Mr. Himamauli Das
Acting Director
Financial Crimes Enforcement Network
ATTN: Policy Division
P.O. Box 39
Vienna, Virginia 22183

Re: Review of Bank Secrecy Act Regulations and Guidance - Request for Information, Docket Number FINCEN-2021-0008

Dear Acting Director Das:

On behalf of SentiLink, I am pleased to submit the following comments in response to the Financial Crimes Enforcement Network's ("FinCEN") Request for Information ("the RFI") entitled "Review of Bank Secrecy Act Regulations and Guidance." 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 meet and exceed their regulatory obligations by uncovering insights about identity risks, empowering financial institutions to make better identity decisions. SentiLink was also the first company in history to use the Social Security Administration's Electronic Consent Based SSN Verification service ("eCBSV") to validate account application data.

Our deep expertise allows us to work with our financial institution partners on a daily basis and in real-time to address the challenges they face from the constant and evolving threats from identity crimes. It is from that perspective that we provide the following responses to certain questions contained in the RFI. In general: While our goal as a company is to help minimize the impact of account origination fraud and improve identity verification processes, we believe federal regulators should do more to meet the changing fraud landscape, and that the existing risk-based CIP regulatory regime needs to be modernized.

Answers to Select Questions

Question 9: Are there BSA regulations or guidance that do not promote risk-based safeguards or that no longer fulfill their original purpose? If so, which regulations or guidance, and what changes do you recommend?

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. *However, we believe it is no longer appropriate for regulators to allow these assessments to be overly reliant on less-relevant and antiquated factors such as the physical location of the financial institution,[2] or the perceived risk of the financial product or service being offered,[3] as is standard practice today. For example, identity fraud has evolved in such a way as to make unreliable what should be a reasonable assumption -- that a "resident consumer account" (i.e., a standard checking account) application is low-risk -- as the challenge of identifying what constitutes risk for a financial institution is no longer as obvious. Regulators must instead modernize CIP rules, Frequently Asked Questions ("FAQs") and guidance to 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, and should provide greater clarity and specificity with regards to what constitutes a "reasonable belief."*

Existing Rules are Ill-equipped for the Evolving Financial Industry

In 1994, the first U.S.-based financial institution made online bank account access available to customers.[4] In contrast, last year two-thirds of Americans used online or mobile banking platforms, with nearly one-third reporting the use of online-only banking services.[5] While traditional brick-and-mortar depository institutions have contributed to this growth in digital interactions through their own technological investment over the last 28 years (which, it should be noted, are restrained by the watchful eyes of federal and state regulatory authorities), some institutions have approached the execution of a digital-first or digital-only business model (often with no physical branch footprint) designed to prioritize the benefits of technological innovation over the increases in associated risk, including identity fraud. Thus, from a CIP perspective, a digital

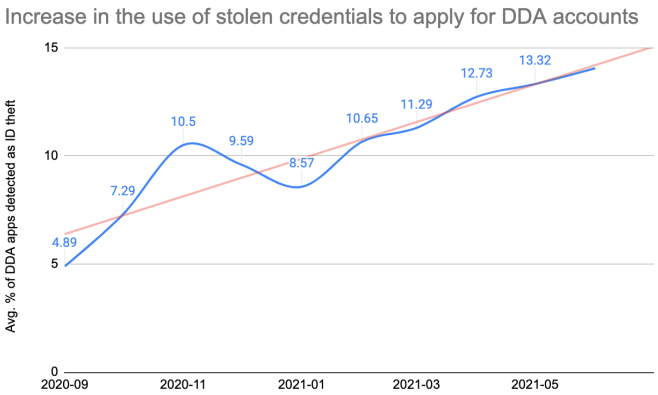
[1] 31 CFR 1020.220(a)(2)
[2] Id.
[3] Id.; See Appendix A.
[4] "The History of Internet Banking," accessed at: https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/
[5] "2021 Fintech Report, The Fintech Effect," Plaid.com, 2021.

customer-acquisition-at-any-cost strategy necessitates a compliance program focused on doing what's minimally required in order to pass a regulatory exam, and does not expand much beyond collecting the specific bits of identity data outlined in the rules.[6]

As we will discuss in greater detail below, there was a time when a product- or bank demographics-focused risk assessment to determine the amount of rigor an institution should employ when validating the identity of a prospective customer was appropriate and sufficient. However, our analysis illustrates why changing technology and ever-smarter fraudsters have rendered that approach insufficient, and how a "do the regulatory minimum" approach to CIP encourages identity theft and the use of synthetic identities to commit fraud. *More directly: A "do the minimum" approach to CIP, which often yields sustained and significant amounts of identity fraud, is indicative of a failure to "form a reasonable belief" that an institution has taken appropriate steps to verify the identity of a customer, and should not be acceptable to regulators.*

Identity Theft: DDAs as facilitators

The lax application of KYC laws and regulations -- particularly for banking services deemed "low-risk" -- materially contributed to the loss of billions of dollars of taxpayer funds to fraudulent unemployment insurance claims and applications for federal Paycheck Protection Program funding over the last few years of the COVID-19 pandemic.[7] Based on our analysis, a significant portion of this fraud found its way into the banking system by way of checking accounts created with stolen identities, relying on compromised name, date of birth, Social Security number and address of the victim for account application.



With a deposit account opened, fraudsters then used the same stolen identity information to apply for government relief funds, to be remitted to the fraudulently

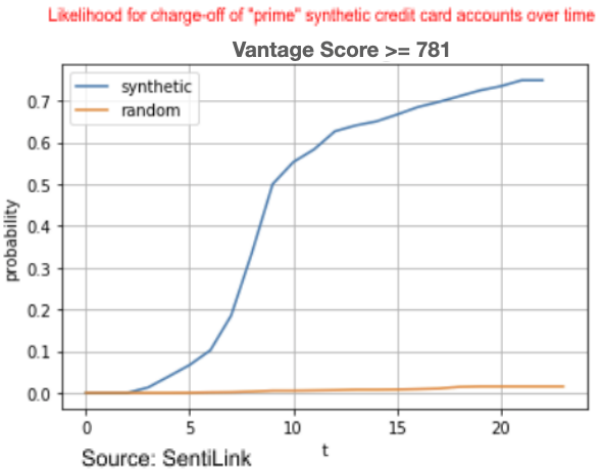
[6] *See* "BSA/AML Manual: Assessing Compliance with BSA Regulatory Requirements: Customer Identification program," FFIEC. Accessed at https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/01

[7] In addition, see for example: "What was fintech's role in PPP loan fraud?" Accessed at: https://www.protocol.com/newsletters/protocol-fintech/fintech-ppp-loan-fraud-report?rebelltitem=1#rebelltitem1

opened "low risk" checking account. When the funds were received, they could be laundered through a myriad of other financial accounts such as other deposit accounts, prepaid cards, peer-to-peer payment services or cryptocurrency platforms. *Overall, from September, 2020, to June, 2021, the percentage of applications for demand deposit accounts identified by SentiLink as using stolen identities increased 187%.*

Basic KYC/CIP Checks Often Miss Synthetic Identities, Leading to Significant Losses

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. In either case, 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 apply for new credit: When the financial institution is presented with an application by a "mature" synthetic identity, a "do the minimum" KYC/CIP check can easily miss the reality of the fraudulent applicant. This leads to bust-out fraud, money laundering, or other financial crimes, which directly undermine existing regulations designed to stop this from happening.



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 depository 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.

We urge FinCEN to directly address synthetic identity fraud and ensure that checks for this type of identity fraud are a core feature of CIP rules, FAQs and guidance.

Question 11: Are there any BSA regulations or guidance that are obsolete because of changes in compliance business practices and/or technological innovation in the financial system or elsewhere? If so, how should FinCEN address this?

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 as the opportunities for some real-time interpersonal interactions diminish or are not present at all in these situations.

The Means of Communication Matters More in Verifying Identity

Historically, signing paperwork and shaking hands with a banker across the table was only the first step to accessing a new financial account. It would not be until some days later, when a box of checks or debit card arrived in the mail, that the account could begin to be fully utilized. Thus, the customer's address was a critical link not only for communication, but identity verification as well.

Existing CIP rules, FAQs and guidance remain focused on the consumer's address as the key means of communication: 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.[8]

The regulatory gap created by an overreliance on a consumer's address in the context of CIP, combined with the prevalence of digital-only consumer onboarding experiences discussed previously, has led to increased amounts of financial crimes and identity fraud. *Control of a physical address is not as valid a signal of a person's true identity as it once was. 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.* Modern identity thieves regularly leverage the well-known CIP compliance formula of a legitimate person's name + date of birth + identifier + address PII combination -- paired with a means of electronic communication controlled by the fraudster -- to successfully obtain credit. *The smarter approach for FinCEN is to ensure sufficient evaluation of key points of data beyond the rote variables currently required; CIP rules should reflect the reality of the*

[8] 31 CFR 1020.220(a)(2)(i)(A)

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.

To support our recommendation that baseline CIP rules, FAQs and guidance be expanded to consider factors beyond just a consumer's physical address, we conducted two analyses of our data:

Analysis 1: Macro Trends

Based on overall trends and insights we observe over time across all our financial institution partners, for every 1,000,000 financial applications, we estimate:

- Approximately 32,000 (or just over 3%) will be applications attempting identity fraud.
    - **Of those fraudulent applications, nearly 13,000 (41%) will have an address with consistent history for at least two years.**
    - Within this population of fraudsters using valid name + DOB + SSN + address on the application, we expect:
        - 41% have a VoIP phone number.
        - 57% present a phone number area code with no known historical ties to the applicant.
        - 20% of application phone numbers are brand new with no history.
        - 12% have multiple distinct identities tied to the application phone number in a short period of time before the application was submitted.
        - 55% apply with either a brand-new e-mail address, or one that has been in existence for a very short period of time.

Thus, for every 1,000,000 financial applications, 1.3% will be fraudulent attempts that present with a valid name + DOB + SSN + address PII combination, and that are likely to pass a minimum CIP evaluation. While to some this may not sound like a large problem, consider that in just the third *quarter* of 2021, there were:

- 19.3 million credit card originations.
- 4.4 million unsecured personal loan originations.
- 8.2 million auto loan originations.[9]

[9] TransUnion Q3 2021 Quarterly Credit Industry Insights Report. https://www.transunion.com/blog/credit-cards-are-surging-thanks-to-gen-z

Applying our analysis, across these three segments,[10] we expect that during Q3 of 2021:

- Over 414,000 applications presented with a valid PII combination but were, in reality, fraudulent.
    - Approximately 170,000 featured a VoIP, which is a very high indicator of fraud on its own.
    - 236,000 applications included a phone area code with no association to the applicant.
    - 83,000 featured a brand-new phone number, and 50,000 used a phone number associated with multiple identities.
    - 228,000 featured a brand-new or recently created e-mail address.

Analysis 2: Checking account applications

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.

Based on this, there can be little doubt that collecting an applicant's address is -- as the sole communication link to a potential customer required to be collected and used for CIP purposes -- an insufficient and often ineffective regulatory standard for verifying the identity of a financial institution's customers. An evaluation of other characteristics, such as the supplied phone and e-mail, must be a required step in CIP rules and guidance.[11]

Further, existing regulations require that after an account is opened, any subsequent verification of identity information deemed necessary by the financial institution is to be completed within a "reasonable" amount of time.[12] However, technological innovations

[10] We recognize this data is based on originations. An analysis based on all applications would yield much higher numbers and amounts of fraud.
[11] Further supporting this argument is data reported in the Consumer Financial Protection Bureau's "2021 Consumer Credit Card Market Report," which notes that in 2020, 88% of all general purpose credit card applications were submitted digitally, with 52% of that submitted via mobile channels.
[12] 31 CFR 1020.220(a)(2)(ii)

have dramatically improved the capability for financial institutions to verify identifying information in real-time. For example, the Social Security Administration's eCBSV allows real-time verification of a name, date of birth and Social Security number combination submitted on a financial application, and is an important treatment strategy against synthetic identity fraud. This and other innovations are valuable tools that financial institutions should be using to stop synthetic identity fraud and identity theft at account origination. We recommend FinCEN consider whether real-time verification of CIP information should be required under certain circumstances.

Question 12: Do FinCEN's regulations and guidance sufficiently allow financial institutions to incorporate innovative and technological approaches to BSA compliance? If not, how can FinCEN facilitate greater use of these tools, while ensuring that appropriate safeguards are in place and highly useful information continues to be reported to government authorities?

As discussed above, while existing regulations and guidance *allow* for the use of innovative and technological approaches to BSA compliance, they do not incentivize regulated firms to do so in all applications where they should be used. Product-focused risk assessments have in many cases fostered a compliance race-to-the-bottom as some institutions adopt a "do the minimum of what's required" approach, creating blind spots for financial crimes and fraud that could be largely avoided if innovative technologies were applied everywhere these risks exist.

In conclusion, FinCEN must modernize its CIP rules, FAQs and guidance to ensure robust identity verification requirements -- including for identity theft and synthetic identities -- become fundamental to BSA and CIP compliance. We encourage FinCEN to foster a "do what's smart" regulatory framework that focuses on the actual threats institutions face, rather than a risk framework focused on increasingly obsolete factors -- such as how "risky" a product is or an institution's physical footprint -- that no longer aligns with the realities of fraud in the marketplace today.[13]

As the empirical evidence makes clear, the risk to financial institutions of all sizes and charter types from identity fraud -- financial, reputational and regulatory -- exists across the spectrum of financial products and services. Further, insufficient identity verification programs can also lead to certain segments of the population -- particularly those with

[13] For additional insights from SentiLink, see "Risk at Fintech Startups: What's required versus what's smart," available at: https://blog.sentilink.com/whats-required-vs-whats-smart

thin or no credit histories, such as new entrants to the workforce or recent immigrants -- having a harder time accessing the financial products they need. As the financial industry moves to more digital-first or digital-only customer experiences, these risks will expand.

Thank you for the opportunity to comment on this RFI. If we can be of further assistance or provide clarification on any of our recommendations, please do not hesitate to contact Jason Kratovil, SentiLink Head of Public Policy (jason@sentilink.com).

Sincerely,

/s/
Naftali Harris
Co-Founder and CEO

Appendix A

The following chart appears as "Appendix K" in the FFIEC's BSA/AML Manual for examiners.