SentiLink

October 30, 2023

Via Electronic Mail

Comment Intake
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552
CFPB_consumerreporting_rulemaking@cfpb.gov

Re: Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration

Dear Director Chopra:

On behalf of SentiLink, I am pleased to submit the following comments in response to the Consumer Financial Protection Bureau's ("CFPB") Small Business Regulatory Enforcement Fairness Act of 1996 ("SBREFA") outline of forthcoming proposals ("the proposal") under the Fair Credit Reporting Act ("FCRA") related to data brokers and certain data.

SentiLink provides identity verification, fraud mitigation and risk management solutions to US-based financial institutions. Our tools enable institutions and individuals to transact confidently with one another by preventing identity fraud at the point that a consumer is applying for any type of financial account. 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. Each day we help over 1,000,000 consumers applying for financial products and services, and in doing so prevent approximately 10,000 cases of identity theft daily. We were founded in 2017 and have 85 employees based out of our San Francisco headquarters and satellite offices in Los Angeles, Denver, Chicago, Austin, San Ramon and New York.

Underneath the surface of our solutions are statistical models continually trained and improved by three primary sources: First, our team of expert risk analysts who review and manually investigate cases to stay abreast of the leading edge of fraud tactics and criminal activity, feeding that knowledge into model updates; second, data provided by our clients (referred to as "partners"); and third, data (including credit header data) from

external and highly vetted sources. Our models deliver real-time fraud scores and signals via Application Programming Interface ("API") to our partners to help ensure:

- Good customers, including thin file and those new to credit, get onboarded quickly;
- Consumers are protected from identity crime;
- Fraud in the financial system is reduced; and
- Financial regulatory obligations are satisfied.

It is from this perspective that we provide the following responses to select questions contained in the SBREFA outline.

Consolidated Response to Questions 1-4:

The proposal would subject identity verification and fraud mitigation companies and the data they use to the FCRA. Broadly, SentiLink and other companies in our space who provide these services to the financial industry -- as well as to many government benefit-disbursing agencies -- will be impeded in their ability to operate viably, compromising their ability to protect consumers and keep fraud out of the financial system.

This outcome would directly impact consumers in two ways:

1. Consumers would be exposed to an increased probability of identity theft, with all of the financial, emotional[1] and administrative complexity that entails, as a result of a reduction in the available identity theft prevention solutions.
2. Many consumers with minimal credit history, including young adults and immigrants, would be denied credit products because superficially they would look the same as perpetrators of identity fraud.

By collapsing identity verification into the FCRA framework, companies like SentiLink would need to reconstitute the analytic elements of their fraud prevention tools, and that effort would be hindered by FCRA requirements. Fraudster misuse of FCRA consumer rights, for instance, could enable fraudsters to dispute vital fraud detection-related data. These criminals could also use FCRA disclosure mechanisms to reveal fraud prevention details and could then hone strategies for slipping through identity verification defenses. In short, the proposal would obstruct our ability to provide a vital fraud prevention

[1] See, for example: "The Emotional Toll of Identity Theft," accessed at https://www.nbcboston.com/investigations/consumer/the-emotional-toll-of-identity-theft/3130483/.

function that protects consumers and enables our partners to focus their subsequent credit-worthiness assessments on genuine applicants.

SentiLink is not a consumer reporting agency. We do not provide consumer reports, we do not provide any evaluation of a consumer's credit-worthiness or eligibility for a transaction, and we do not support our partners' credit-worthiness and eligibility determinations. We do not sell consumer data like a marketing company; rather, we use data to verify identities and detect fraud in the financial system, and we provide tools to help our partners do the same. In fact, we stipulate that our solutions may not be used for FCRA purposes and do not constitute an evaluation or indication of a person's credit-worthiness or eligibility -- because they do not.

This is not only legally proper, but also completely logical. Identity determination and eligibility are conceptually and legally discrete and, in fact, sequential: A financial institution cannot determine a consumer's credit-worthiness without first knowing who they are.

To ensure SentiLink is able to continue to provide our technologies that protect consumers from identity crimes and reduce fraud costs in the financial system, we urge CFPB to exempt fraud prevention and identity verification activities and data, including fraud prevention-related use of the credit header file, from FCRA regulatory requirements, and to exempt businesses engaged in fraud prevention or identity verification from the definition of "data broker."

Q5. Other than compliance costs, what costs, burdens, or unintended consequences should the CFPB consider with respect to the proposal under consideration? Please quantify if possible. What alternatives, if any, would mitigate such costs, burdens, or unintended consequences?

If SentiLink was to be regulated as a "data broker" or "consumer reporting agency," and our access to data necessary to protect consumers from fraud was subjected to the FCRA, the costs to SentiLink would be significant and consequential. This would include the costs of redesigning products and undertaking additional legal compliance, and the costs of being forced into a new arms race with fraudsters, where the FCRA would perversely become an offensive weapon to actively undermine anti-fraud defenses. All of these costs ultimately get passed down to consumers.

The heavier cost burden is societal. Compromising identity verification and fraud reduction by subjecting companies like ours to regulatory burdens designed for and targeted at others (i.e., marketers), as well as limiting our ability to use the data necessary to support our models, will make it easier for identity thieves and synthetic fraudsters to victimize consumers and drive up the cost of banking. Those costs will be

borne by consumers in the form of higher direct costs and reduced access of legitimate and deserving consumers to financial products.

While transparency is an important aspect of the FCRA, that sort of transparency in fraud prevention works against efforts to prevent fraudsters from harming consumers. For example: In a theoretical future state where our services were subject to the FCRA, a criminal using a stolen identity would be flagged by our models and declined by the financial institution. An adverse action notice would then be sent to the criminal. As the CFPB has recently stated, the notice must be "specific" and contain information intended to "...accurately describe the factors actually considered or scored by a creditor."[2] When the denial was made due to identity defects signaling a crime, the adverse action notice would provide the fraudster with actionable information about how their fraud was detected and would hand them a troubleshooting roadmap to improve their schemes, causing further harm to present and future victims of identity crimes.

An additional negative consequence relates to potential dispute scenarios. Building off the previous hypothetical, such a regulatory change would make it possible for a criminal who has stolen a person's identity to dispute and potentially change certain valid identity components, such as the means of communication, to something they control, further cementing the fraudster's ownership of the victim's identity. The compounding harm this would cause to a consumer victim would be multifaceted and profound.

To mitigate these negative consequences, the CFPB should exempt providers of identity verification and fraud prevention services, as well as the data -- including credit header data -- required to carry out this critical function, from this rulemaking.

Q6. Are there any statutes or regulations with which your firm must comply that may duplicate, overlap, or conflict with the proposal under consideration? What challenges or costs would your firm anticipate in complying with any such statutes or regulations and the CFPB's proposal under consideration?

The FCRA was never intended to govern fraud mitigation and identity verification activities in the financial industry. The FCRA implicitly assumes that the consumers addressed under the Act are the consumers they purport to be, and is intended to provide consumers with the information they need to, for example, understand their eligibility for credit.

---

[2] *See* U.S. Consumer Financial Protection Bureau, *Consumer Financial Protection Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B*, https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

Specifically: The regulatory requirements and consumer rights mandated by the FCRA become applicable *after* the identity of the consumer has already been established. This is a necessary and logical bright line regulatory distinction between ex-ante identity verification and fraud reduction efforts (subject to the Gramm-Leach-Bliley Act ("GLBA") and various anti-money laundering statutes under the jurisdiction of FinCEN) and the ex-post regulation of credit reporting and evaluation of consumer credit-worthiness (under the FCRA) for a consumer whose identity has been verified.

Critically, as part of a BSA/AML compliance program, financial institutions are required to maintain a "Customer Identification Program."[3] Subjecting fraud mitigation and identity verification providers -- and the data relied upon therein -- to the FCRA would compromise the delivery of these important services. That, in turn, would directly conflict with federal BSA/AML obligations. When banks fail to meet the requirements of these regulations, federal prudential regulators exercise their enforcement authority in earnest.[4]

Additionally, other state and federal laws explicitly exempt activities related to fraud prevention from undue regulatory burden in many cases. For example, the California Consumer Privacy Act and the federal GLBA similarly exempt from certain regulatory obligations activities related to "...[detecting] malicious, deceptive, fraudulent, or illegal actions,"[5] or those "to protect against or prevent actual or potential fraud."[6]

More recently, the CFPB provided an advisory opinion related to Section 1034(c) of the Dodd-Frank Act in which it stated, consistent with the underlying statute, that "information collected for the purpose of preventing fraud or money laundering, or detecting or making any report regarding other unlawful or potentially unlawful conduct" is exempt from the requirements of this provision of law.[7] Similarly, in its proposed rule to implement Section 1033 of the Dodd-Frank Act, the CFPB adhered to statutory direction to exempt "...information collected by the data provider for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct."[8] Taken together, Congress recognized that fraud prevention and related data necessitates a different approach under consumer financial protection law.

---

[3] See, e.g., 12 CFR 208.63(b)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC).
[4] *See, e.g.*, U.S. Federal Reserve Board, *In the Matter of Metropolitan Commercial Bank* (Oct. 16, 2023), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20231019a1.pdf.
[5] California Consumer Privacy Act of 2018, as amended, §§ 1798.140(ac), 1798.105(d)(2).
[6] Gramm-Leach-Bliley Act, U.S.C. § 6801, § 6802(e)(3).
[7] U.S. Consumer Financial Protection Bureau, Consumer Information Requests to Large Banks and Credit Unions, https://files.consumerfinance.gov/f/documents/cfpb-1034c-advisory-opinion-2023_10.pdf.
[8] U.S. Consumer Financial Protection Bureau, Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights, https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf

If the FCRA were intended to apply to fraud prevention, identity verification and related data, then Congress would not have specifically addressed these activities in the GLBA, various sections of the USA Patriot Act, or the Bank Secrecy Act and instead expanded the FCRA beyond its existing purpose and scope. As it currently stands, the potential for direct conflict with existing regulatory requirements and existing federal and state precedent recognizing the importance of preserving identity verification and fraud prevention activities, makes clear that an exemption for these activities, the firms that provide them, and the data necessary to carry them out should be included in the proposed rulemaking.

Consolidated Response to Questions 8-11

Firms engaged in fraud prevention and identity verification activities should not fall within the definition of "consumer reporting agency." The statutory definition of that term hinges in part on whether an entity furnishes "consumer reports."[9] As discussed below in response to Questions 16-18, companies like SentiLink -- which work to verify identities and prevent fraud at the point of application, prior to any evaluations of credit-worthiness -- do not provide consumer reports. SentiLink also clearly establishes with our partners that our products are to be used for identity verification and related fraud prevention purposes only, and not any FCRA purposes for which a consumer reporting agency might furnish a consumer report.

Further, it is imperative that any proposed rulemaking not inhibit companies engaged in identity verification and fraud prevention from accessing the data necessary to carry out those functions. As discussed previously, these functions are critical for consumer protection as well as fulfilling legal obligations under BSA/AML law. These functions are not, however, FCRA-covered purposes.

Subjecting fraud prevention data providers to the FCRA by deeming them to be "consumer reporting agencies" will significantly inhibit our ability to train statistical models on the highest quality inputs, leading to more identity crime and fraud costs to the financial system. Therefore, similar to SentiLink itself and our solutions, data provided to firms like SentiLink should not be deemed "consumer reports" and those data providers should not be deemed "consumer reporting agencies" for purposes related to fraud prevention and identity verification.

Consolidated Response to Questions 14-15

To advance our fraud prevention and identity verification activities, SentiLink assembles and evaluates data from two major sources: Data acquired (such as credit header data) and application information from our partners. However, as discussed in response to

[9] Fair Credit Reporting Act, 15 U.S.C § 1681, § 603(f).

other questions, SentiLink (and companies like SentiLink) obtains data expressly to verify identities and prevent fraud. Neither the data we obtain and use nor the services we provide have any bearing on credit-worthiness determinations, and therefore they are not consumer reports and are not obtained or used for any statutory permissible purpose under the FCRA.

The transmission of consumer data electronically by an intermediary, vendor or other entity to SentiLink and others engaged in fraud prevention and identity verification does not create a risk of harm to a consumer. In fact, data sharing of this type benefits individual consumers by reducing their risk of fraud and benefits society by reducing the number of victims of identity crime, lowering fraud costs, and supporting the integrity of the financial system.

Any proposed rule should clarify that fraud prevention and identity verification activities do not constitute "assembling or evaluating" consumer credit information for purposes of the FCRA.

Consolidated Response to Questions 16-18

Credit header data consists of the basic elements of current and historic identity information associated with credit-active individuals. Credit header data is the foundational reference used by SentiLink and many other firms that work to prevent fraud, verify identities, and protect consumers from being victimized. In order to verify an identity and determine whether it is being used to commit an identity crime, fraud detection and identity verification models must have a starting point from which to conduct validation and analysis. Credit header data is often that starting point.

Section 603(d) of the FCRA defines a "consumer report" as, generally, "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other permissible purpose authorized under FCRA section 604."[10] This definition is not applicable to credit header data when it is used for fraud prevention and identity verification purposes. Under the FCRA, consumer reports are used to make assessments and eligibility determinations *of a person whose valid identity has already been established.* When SentiLink and others use credit header data, it is to determine if the identity information contained in an application for a financial product corresponds to the applicant, a synthetic identity, or an actual person whose identity has been stolen.

[10] Fair Credit Reporting Act, 15 U.S.C § 1681, § 603(d)(1).

When used in this way, credit header data cannot practically be considered a "consumer report" under the FCRA because the identity of the consumer to whom the credit header data *may* relate is unverified.

To illustrate the importance of credit header data in identity verification and fraud mitigation, consider the following two anonymized examples from SentiLink's work:

Case study: Using credit header data to prevent elder identity theft

An online application was received by a mid-size financial institution for a credit card.

- Credit header data showed that the name, DOB of October 1948, and SSN provided on the application are all consistent with an actual consumer named "John Doe."
- Credit header data showed no historical connection with the application address in Geneva, Alabama. "John Doe" has no address history within 100 miles of the address.
- The application address has ties to 20 additional stolen identities across our network, indicating evidence that the address is controlled by a fraudster or fraud ring.
    - In each of these cases, credit header information confirms that these victims similarly have no address history near Geneva, AL.
- Credit header information revealed the application phone number's area code is from a state where the applicant has never lived.
    - The application phone is a high-risk VoIP carrier. Further, based on credit header information and other data sources, "John Doe" has never been associated with the phone number prior to this application.
- The email address is brand new, created on the day of the application.

Conclusion: Based on this analysis, we determined that "John Doe" was a victim of identity theft. The financial institution was able to prevent the fraudulent account from being opened.

Case Study: Using credit header data to enable an immigrant to open a bank account

A financial institution received an application for a checking account that included a common indicator of fraud: a lack of financial activity history for the application's combination of name/DOB/Social Security number.

- Credit header data revealed the application SSN was newly issued. However, our analysis using credit header information also revealed the applicant was previously tied to ITINs dating back to 2013.

- Credit header analysis showed the applicant has seven years of consistent address history that matches with the application.
- Through our network, we were able to see additional applications at other financial institutions using these ITINs and other PII consistent with credit header data over a multi-year span. None of these applications presented signs of fraud.

Conclusion: We determined the application is that of an immigrant who arrived in the US in 2013, at which point he obtained an ITIN. Less than a year prior to this application, he obtained an SSN. Despite surface-level signals that could have led to a rejection, our holistic and deeper analysis of credit header data and his application history in the US made it possible for us to conclude the application was not fraudulent.

SentiLink reviews over 1,000,000 applications each day, including many cases like these. Credit header data is a vital tool to make these decisions possible for the benefit of consumers, and when used for fraud prevention and identity verification purposes, should be excluded from the definition of "consumer report" and the FCRA broadly under any proposed rule.

* * *

Thank you for the opportunity to provide input as you begin this important rulemaking. We appreciate your consideration of our comments and look forward to continued dialogue as this process moves forward.

Sincerely,

/s/

Jason Kratovil
Head of Public Policy and External Affairs