SentiLink

September 17, 2025

Via Federal eRulemaking Portal and comments@fdic.gov

Office of the Comptroller of the Currency
400 7th Street, SW, Suite 3E-218
Washington, DC 20219

Federal Reserve Board of Governors
2001 C Street NW
Washington, DC 20551

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: Request for Information on Potential Actions to Address Payments Fraud; Docket ID OCC-2025-0009; Docket No. OP-1866; RIN 3064-ZA49

To Whom It May Concern:

On behalf of SentiLink, I am pleased to submit the following comments in response to the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the Agencies) Request for Information on Potential Actions to Address Payments Fraud (RFI).[1]

About SentiLink

SentiLink provides identity verification, fraud mitigation and risk management solutions to US-based financial institutions and others. SentiLink's services ensure that applicants are who they claim to be before credit evaluation begins, enabling financial institutions and individuals to transact confidently 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 SentiLink helps over 3,000,000 consumers applying for financial products and services, and in doing so prevents approximately 60,000 cases of identity fraud daily. Underneath the surface of our solutions are statistical models continually trained and

[1] 90 FR 26293 (June 20, 2025).

improved by three primary sources: First, data from external and highly vetted sources; second, 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; and third, data provided by our clients (referred to as "partners”). 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.

SentiLink relies on credit header data and other data sources to build models and enhance the precision of our solutions, which ultimately facilitate consumer access to financial services by reducing fraud in the financial system. The high precision of our scoring models allows our partner financial institutions to expedite approximately 97% of “clear,” non-fraudulent applications through initial identity verification and fraud prevention checks, enabling them to focus on reviewing only those applications that present a high identity fraud risk. We do not collect or rely on demographic data and have a robust process in place for independently auditing our scoring models, including statistical assessments of impacts across demographic groups by a third-party economic analysis firm.

It is from this perspective that we provide feedback to select questions in the RFI.

General Comments

We appreciate the Agencies offering an opportunity for stakeholder feedback on whether additional actions by the Agencies may be warranted to combat payments fraud. We agree that especially due to the complexity and scope of payments fraud, input and engagement from a variety of stakeholders will be helpful to identify and evaluate the range of potential actions to consider. We also concur that as a payments fraud scheme may involve multiple institutions and payment methods that may fall within the remit of different Federal and State agencies, no agency or private-sector entity can address payments fraud on its own.

As a company that is focused on fighting fraud in online and electronic spaces every day, we value that the Agencies are prioritizing the support they can provide to the ongoing battle against payments fraud. Fundamentally, robust anti-fraud solutions must be in place to protect individuals and the financial payments system overall from identity theft and from other types of frauds and scams occurring online and electronically.

Responses to Select Questions Posed by the RFI

Regulation and Supervision

> ***9. What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payments fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?***

We agree the Agencies should consider potential changes to regulations to help address payments fraud and mitigate harms from such fraud causes. In our work to identify and combat identity-related fraud, we have identified clear trends of fraudsters abusing well-intended regulatory protections. We have identified two regulations that should be studied for possible amendment to help better combat payment fraud.

First, the Equal Credit Opportunity Act (ECOA) and Regulation B were designed to ensure equal access to credit, particularly for women who were often denied credit histories independent of their husbands. While this is an important and meaningful goal, the rules as implemented have created a significant first party fraud vulnerability. Under current CFPB official interpretations, if a creditor allows spouses to be added as authorized users, it cannot refuse to accept non-spouses in that same role.[2] As a result, credit bureaus and creditors cannot meaningfully distinguish between spousal authorized user accounts -- which ECOA sought to protect -- and non-spousal “piggybacking” accounts sold in online marketplaces. As explained below, this often results in permitting ill-intentioned strangers to abuse the credit system.

Specifically, this loophole allows individuals with poor credit files to purchase, through online clearnet marketplaces, authorized user status as a means of "credit repair" or "credit boosting" and instantly inherit another person’s long, positive credit history. Empirical studies, including Federal Reserve research,[3] confirm that this practice can boost a credit score by 20 points or more—enough to move a borrower from subprime into near-prime or prime status. For lenders, this means extending credit on terms that do not reflect actual risk. For fraudsters, it creates another tool to manipulate identity information and exploit the system.

[2] 12 C.F.R. §1002.7(a)–2

[3] Robert B. Avery, Kenneth P. Brevoort, and Glenn B. Canner, *Credit Where None Is Due? Authorized User Account Status and “Piggybacking Credit”*, Finance and Economics Discussion Series 2010-23 (Washington, DC: Board of Governors of the Federal Reserve System, March 5, 2010).

To address this issue, regulators should modernize ECOA and Regulation B to allow creditors to validate the existence of a relationship between the account holder and authorized user. This update would preserve the consumer protections that ECOA created, while closing a loophole that enables first party fraud and erodes the reliability of credit scoring models.

Second, there is a growing trend for fraudsters to abuse protections granted under the Fair Credit Reporting Act (FCRA). In a credit washing scheme, a consumer fraudulently disputes a tradeline to have it removed from their credit report by asserting they are the victim of identity theft. If successful, this can result in a bump to the consumer's credit score. The FCRA affords certain rights to victims of identity theft, including the right to dispute a tradeline on their credit report that resulted from identity theft and is negatively impacting their credit. Section 605b of the FCRA empowers identity theft victims to block the reporting of a fraudulent tradeline so that it does not harm the victim's credit score. The filing of the FTC's Identity Theft Report (ITR) initiates a statutorily required investigatory process, and during that investigation, reporting of the tradeline(s) in question must be suppressed. Credit washing involves the abuse of these rights, including the misuse of the ITR process. A consumer, or frequently a credit repair organization (CROs) on behalf of a consumer (and perhaps without the consumer's knowledge), will submit an ITR to either a financial institution or a credit reporting agency claiming one more negative tradeline is the result of identity theft when no such theft occurred. This may occur several times over an extended period of time, prolonging the artificial boost to the consumer's credit score. Credit washing leads to higher losses and increased risk, since subsequent creditors will not see the washed tradelines and potentially misprice the consumer's risk.[4]

We fully recognize and appreciate that many consumers rightfully and appropriately claim identity theft using the Section 605b process and many CROs help consumers navigate this and other credit repair processes. The protections afforded under the FCRA are meaningful and appropriate to victims of identity theft. However, there also are clear signs of abuse. For example, in 2021, the FTC's Office of Inspector General found that an FTC analysis of complaints received during the first 6 months of 2021 "revealed significant patterns that suggest a possible fraudulent use of IdentityTheft.gov."[5] That website is where a consumer files an ITR. We recommend the banking agencies work with the FTC and CFPB to help close the loopholes to ensure that bad actors are not abusing a well-intended system for identity theft victims. Such modifications could include requiring a consumer who files an ITR to also obtain a

[4] *See*: "Understanding Credit Washing: Risks, potential losses and signals associated with this type of first party fraud," SentiLink, 2023.

[5] *See: "*Fiscal year 2021 Report on the Federal Trade Commission's Top management and performance Challenges," FTC OIG, OIG Report No. OIG-21-05.

police report (which was once a requirement). Such a requirement would likely deter many would-be credit washers.

Payments Fraud Data Collection and Information Sharing

> ***16. Broadly, how could payments fraud data collection and information sharing be improved?***

In our experience, a key component to effectively identifying and combatting identity-related fraud is data sharing between the public and private sectors. Federal and state agencies are frequently the sources of truth -- in other words, only these agencies, using the data they protect and maintain, can authoritatively answer whether a key piece of identity information is valid.

For example, SSA's real-time API-based system, eCBSV, allows financial institutions (or their service providers) to verify a name, date of birth, and SSN combination against SSA's records. As the source of truth for which SSNs have been assigned to a given name and date of birth, this system makes it possible for financial institutions to approve more good customers more efficiently, and reduce fraud and risk. The results from eCBSV are not a definitive answer on whether fraud is occurring, but they go a long way in identifying potential wrongdoing. While we continue to work with SSA to expand the capability, efficiency, and effectiveness of eCBSV, it is a strong example of how data sharing between a federal agency and financial institutions can help combat fraud, without risking consumers' privacy.

We encourage the Agencies to explore other ways such partnerships and data sharing can improve fraud detection and prevention. For example, the Internal Revenue Service (IRS) operates the Income Verification Express Service, which permits financial institutions to validate income information directly with the IRS, serving both underwriting and fraud detection purposes. In 2018, Congress directed the IRS to modernize and change the system from a fax-based process to API.[6] Unfortunately, the IRS pursued an implementation of this effort in such a way as to render the system unusable for modern financial services. Correcting this to enable a usability similar to what the SSA achieved with eCBSV would be an important step in mitigating fraud.

General Questions

[6] *Taxpayer First Act*, Pub. L. No. 116-25, § 2201, 133 Stat. 981 (2019).

23. What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud?

Because we closely support a wide range of US financial institutions' identity fraud prevention efforts, SentiLink has a clear window into understanding the evolving face of fraud. Fraudsters are rapidly adapting their methods, exploiting both legacy payment systems and emerging technologies. Check fraud remains a significant vulnerability: images of stolen checks that once numbered in the hundreds per month during 2020 have surged dramatically over the years.[7] These are traded on dark web forums and encrypted messaging channels, underscoring the scale and organization of criminal markets.

At the same time, the use of Credit Profile Numbers (CPNs) and synthetic identities has become a core vector for fraud. Vendors openly market these services—often relying on stolen Social Security numbers from individuals with little or no credit history—to build fake but convincing credit files. Over time, these synthetic identities are used to open accounts, secure loans, and ultimately commit "bust-out" schemes, leaving financial institutions and taxpayers with significant losses.

Criminals are also beginning to weaponize generative AI and deepfake tools in payments fraud. AI-driven voice cloning, fabricated images, and synthetic likenesses are being used to bypass liveness checks and other onboarding controls. Fraud networks exploit shared addresses, legacy email domains, and repeated device or digital fingerprints to scale their operations. The pace of these technological adaptations is now outstripping the ability of financial institutions to update defenses, creating systemic risks.

25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?

The federal government plays an important role in payments fraud identification, prevention, and mitigation. SentiLink encourages the Agencies to think broadly and creatively about how the federal government can most effectively help prevent fraud.

It is imperative that the Agencies, financial institutions, and every player in the payments system "understand the tactics that fraudsters use to bypass...guardrails, like 'synthetic

[7] *See:* Financial Crimes Enforcement Network (FinCEN), Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023, Financial Trend Analysis (Washington, D.C.: FinCEN, August 2024), https://www.fincen.gov/system/files/shared/FTA-Check-Fraud-FINAL508.pdf.

fraud'.... [and] incorporate these patterns and tactics into their technology while also anticipating how these attack vectors might evolve over time."[8]

In our experience, there are solutions available today that can detect identity fraud faster, more accurately, and at lower cost than legacy solutions. These tools can reduce fraud, waste, and improper payments and provide a more precise solution that reduces the need for manual reviews, and create frictionless processes that, for example, utilize standard PII data fields in an application and eliminate the need for additional documents, biometrics, or smartphones or cameras. We encourage the Agencies to explore these tools to better understand them, and to use them in their own systems as well as encouraging use by their regulated entities.

The Agencies can also turn to innovative fraud prevention providers who offer the ability to quantify potential fraud exposure and estimated savings through a free retrostudy – evaluating historic data for fraud at no cost – and who offer trusted and secure products that are specifically built for regulated environments (such as FedRAMP(™) Ready, PCI-compliant, and SOC II-compliant) and backed by deep fraud expertise and continuous innovation in detection techniques. Agencies can seek providers who offer flexible integration options that, for example, (1) provide API integration – real-time submission and response flow into existing agency systems; (2) batch processing – secure SFTP file uploads with results in under 48 hours and no integration needed; (3) dashboards for investigators – manual review tools that highlight deep risk signals for casework; and (4) workflow automation support – fraud prevention providers can embed in end-to-end agency program application and decisioning processes.

Finally, the Agencies could facilitate head-to-head competitive analyses among fraud prevention providers to evaluate the effectiveness of existing or new fraud solutions for agencies. These “bakeoffs” typically have the participating companies receive the same set of data and compete against each other to see whose solution performs the best. By looking at actual head-to-head product performance, government agencies can evaluate solutions based on quantifiable results. SentiLink encourages the Agencies to conduct a bakeoff for existing fraud solutions and potential new fraud solutions. The result of this bakeoff could help inform future supervisory guidance for regulated entities.

[8] "Why We Invested in SentiLink", David Sacks, (Aug. 5, 2021), https://medium.com/craft-ventures/why-we-invested-in-sentilink-a8ef2cddb58f.

We appreciate the opportunity to comment on these important issues and would welcome the opportunity to provide more information about our experience in this area.

Please do not hesitate to contact me at jason@sentilink.com if you require further information.

Sincerely,

/s/

Jason Kratovil
Head of Policy and External Affairs