


# Fraud in Focus: SentiLink Policy Insights

*Vol. 2*

## US Policy Insights

### Treasury Department requests information related to the use of artificial intelligence in the financial sector. How should financial regulators define "AI?"

- The Treasury Department in June published a Request for Information (RFI) entitled “Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector.” Treasury is continuing its effort to stay informed on how technology is transforming financial services. In comments to the RFI filed in August, SentiLink discussed the need for financial policymakers to adopt a tightened definition of "AI" that focuses on technologies posing the greatest risk, while excluding data processing techniques that may be advanced, but don’t truly qualify as "artificial intelligence."
  Citing our own machine learning tools as an example, we urged Treasury to define "AI" based on risk factors such as the degree of generative and predictive capability, its explainability relative to other data processing techniques, level of direct customer impacts, and specific production use cases.

---

### CFPB Director Chopra delivers semi-annual testimony before the House Financial Services Committee. How is Congress pressing the Bureau on fraud and identity?

- During a June hearing, CFPB Director Rohit Chopra faced pointed questions from both Republican and Democrat Members of the House Financial Services Committee about the

CFPB's forthcoming rulemaking related to the Fair Credit Reporting Act (FCRA) and "data brokers."

The discussion underscored concerns that these regulations could hinder financial institutions' ability to use data for consumer protection against identity fraud and to meet the regulatory requirements. Director Chopra repeatedly acknowledged the importance of fraud prevention, stressing that the Bureau is focused on data brokers that misuse consumer data. Read highlights here.

While these remarks were reassuring, uncertainty remains about how the Bureau will address these critical issues in the proposal, especially as more recent statements by Bureau staff relating to fraud appear to be at odds with the Director's public comments.

---

## Evolve Bank & Trust suffers a ransomware attack and data breach. Breaches happen all the time, so why is this one different?

- Evolve, a provider of banking services to a diverse range of fintech and banking clients, suffered a ransomware attack that led to the exposure of a large amount of sensitive data. While data breaches are not uncommon, this incident stands out due to the apparent *combination* of Personally Identifiable Information (PII) and bank account data, which could enable a different type of fraud.

  The leaked data could potentially allow criminals to access and drain victims' bank accounts. SentiLink's research team discusses the wide-ranging potential for risks posed by this breach in depth here.

---

## CFPB publishes a rulemaking that would ban the reporting of medical debt on consumer credit reports. What does this mean for Regulation V or other rules implementing the FCRA, such as one on data brokers that could impact fraud prevention efforts?

- Last Fall, the CFPB released a broad outline of its plan for an FCRA rulemaking to regulate "data brokers" and certain types of data. However, in June, the Bureau split the contemplated rulemaking into two by proposing a rule to ban medical debt from credit reports.

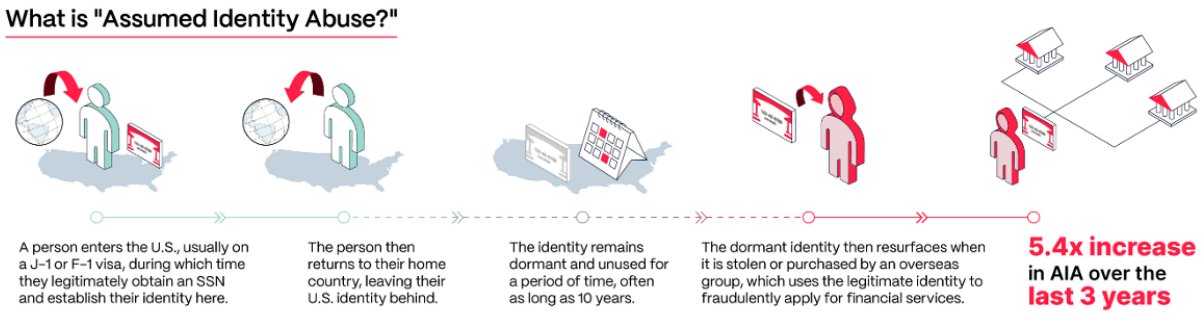
  Arguably, of all the issues the Bureau highlighted regarding the FCRA last year, this is the most straightforward to address, largely because the major credit bureaus have already begun to move in this direction on their own. Politically, preventing medical debt from impacting a consumer's credit is a favorable move, evidenced by the fact that VP Harris was the first to tout this rule.

  Finally, SentiLink and others have provided compelling data-driven arguments to the Bureau

emphasizing that their proposed approach to "data brokers" and banning the sale of credit header data could be detrimental to consumers and increase identity fraud. This feedback may encourage the Bureau to take a more measured and thoughtful approach to the rest of their FCRA agenda.

---

## Fraud Spotlight




*Assumed Identity Abuse ("AIA")* occurs when a fraudster assumes the identity of an individual who came to the US previously, usually on a J-1 or F-1 visa, but has since left the country. These legitimate identities lie dormant for a period of years, during which they are purchased or stolen by fraudsters, including overseas organized crime rings. Once reactivated, the identities are used to apply for credit for which the proceeds go unpaid, leading to significant losses. AIA is hard to detect because the base identity is legitimate and will pass eCBSV, and there is no person in the US to contact and confirm whether ID theft has occurred. **While infrequent in the overall fraud landscape, we've observed a 5.4X increase in this type of fraud over the last few years.**

## In the News

NY Times: "We can't stop writing paper checks. Thieves love that," featuring SentiLink's head of fraud insights, Dr. David Maimon.

American Banker: "A leader in fighting fraud: Naftali Harris, 2024 Innovator of the Year."

SentiLink: "Thoughts on GenAI fraud," by our co-founder and CEO Naftali Harris, in which he addresses some of the fearmongering, shares SentiLink's thinking on the disruption GenAI will have on the fraud landscape, and discusses what we consider the most important open question on its long-term impact.

ICYMI: Webinar -- "Journey of a Stolen Identity: Following the Path of Criminals and Victims," featuring Eva Velazquez, CEO of the Identity Theft Resource Center, Dr. David Maimon, head of fraud insights at SentiLink, and Jason Kratovil, head of policy and public affairs at SentiLink.

*Questions?* Email us at publicpolicy@sentilink.com

Subscribe and view past editions here.

