

Fraud in Focus: SentiLink Policy Insights

Volume 4

US Policy Insights

CFPB is undergoing significant changes to its operations, staffing and leadership, which will affect its policy agenda. What could this mean for its data broker rulemaking and identity fraud?

- While several other pending or final rulemakings initiated under the Biden administration have been derailed in some fashion, the CFPB -- after granting a 30-day extension on the comment period for the proposal -- appears to still be progressing with its FCRA data broker rulemaking. During his Senate confirmation hearing, CFPB Director nominee Jonathan McKernan praised former Director Rohit Chopra for his focus on data privacy and data brokers, describing it as a valid policy issue to evaluate.

  In response to the Notice of Proposed Rulemaking, SentiLink filed an extensive set of comments (available here). Key points include:

  - Without an exemption for identity verification and fraud prevention, the Proposal would directly harm consumers by increasing identity theft and denying access to credit—impacting an estimated 5.7 million consumers in SentiLink's data alone, based on our internal model simulations.
  - The Proposal conflicts with existing federal laws such as the Bank Secrecy Act and USA PATRIOT Act, which require effective identity verification as a foundational compliance step, and that imposing FCRA requirements on ex-ante fraud prevention activities would undermine these critical obligations.
  - The CFPB's justifications for restricting access to credit header data are logically flawed and practically unworkable—particularly the reliance on consumer consent or permissible purpose before identity has been established, which could be exploited by fraudsters and erode consumer protections.

- The CFPB should either withdraw the Proposal or, at minimum, include a clear exemption for identity verification and fraud prevention activities to preserve consumer safety, avoid regulatory conflict, and maintain access to essential financial services.

It is not clear how extensively a new CFPB leadership regime will seek to change former Director Chopra's proposal. If the rulemaking does move forward, the timing for release of a final rule is likely still many months away, and there would be an implementation period following the release. Furthermore, the CFPB announced a major RIF at the agency, including most or all of the regulations team (although this remains tangled in the courts). SentiLink will continue to engage with the Bureau and, once confirmed, Director McKernan to emphasize our policy arguments and the potential negative impacts a flawed rule would have on consumers.

Check fraud -- including checks issued by the Treasury Department -- remains a major challenge. How do updates to the Treasury's check verification service impact check fraud detection and prevention?

- The US Treasury Department has long operated the Treasury Check Verification System (TCVS), providing a public-facing website that allows financial institutions to verify the authenticity of a Treasury check, as well as the means for an API integration -- although the later had not been widely adopted. Check fraud is a top challenge for many banks and credit unions: Treasury checks are particularly concerning given their high legitimacy, as well as "next day availability" requirements. Like traditional checks, fraudsters have become adept and stealing and modifying Treasury checks -- through "washing" or "cooking" -- in order to cash them and divert funds into accounts they control.

Last November, Treasury made an important update to their TCVS API to include the ability to verify the payee name -- but did not similarly update their public-facing website functionality. This gap allows fraudsters to simply change the name on a check and still pass the website verification process, rendering the system far less effective.

In February, SentiLink launched an integration with Treasury's updated API, offering the service for free to our partners. This addresses a critical gap in the legacy Treasury check verification system, verifying payee names, and helping our partners stop more check fraud.

Reporting of beneficial ownership information (BOI) to regulatory bodies provides an important mechanism to deter certain types of fraud in lending. What is the status of FinCEN's implementation of the Corporate Transparency Act's BOI reporting requirements?

- The US Treasury Department announced in March that it will not enforce penalties related to the Corporate Transparency Act's (CTA) beneficial ownership information (BOI) reporting requirements for US citizens and domestic entities, exempting US companies going forward.

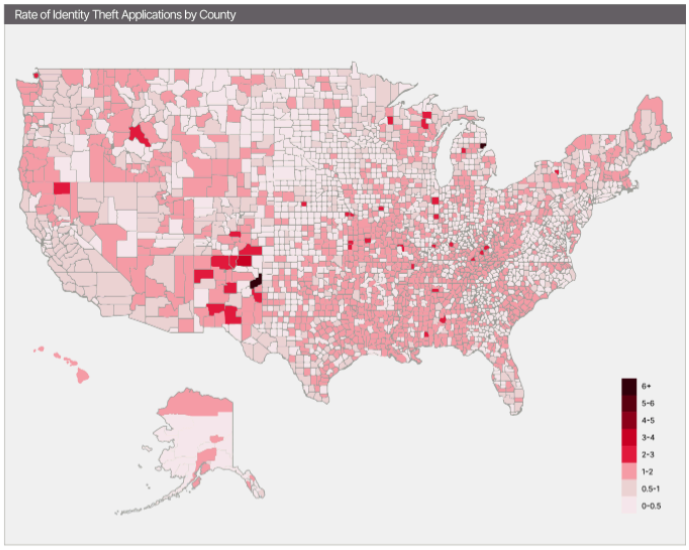
In addition, several lawsuits are proceeding aimed at striking down the underlying statute as unconstitutional. Under FinCEN's Customer Due Diligence rule, financial institutions are required to take steps to verify beneficial ownership information at various points in the customer lifecycle; the BOI database would have served as a centralized repository of such information, replacing the largely inconsistent databases maintained by each state. Comprehensive BOI data is a valuable asset to fight certain types of fraud, such as company impersonation attempts or the use of opaque shell companies and synthetic "owners."

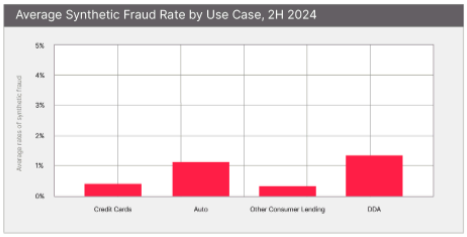
Fraud Spotlight

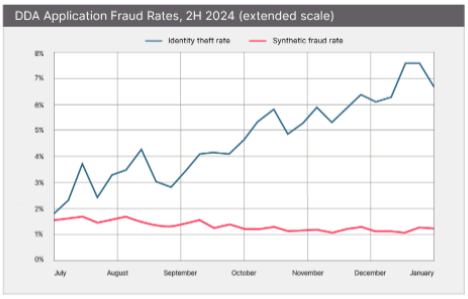
This month, SentiLink published its first comprehensive fraud trends and benchmarking report (download the full report here). The report -- which analyzes data from more than 100 million applications -- covers the second half of 2024, and focuses on trends in **credit cards, auto lending, consumer lending, and checking account (DDA) applications**. Key findings:

- A **decline in synthetic fraud**, dropping from 1% to .75% during 2H 2024;
- The rise of **new tactics**, including legacy phone abuse, residential proxy IP manipulation, and Assumed Identity Abuse (AIA)—a scheme exploiting identities of individuals who have left the U.S.;
- Increased activity from **regionalized fraud rings**, including a high-volume auto loan bust-out scheme in Miami and a serial identity theft ring in Massachusetts;

Visual highlights (click to download):







In the News

SentiLink: "What's going on with SSA's Death Master File?" (part 1 & part 2)

Wired: "Scammers are Creating Fake News Videos to Blackmail Victims," quoting SentiLink's head of fraud insights, Dr. David Maimon.

Payments on Fire (podcast): "Scams, Stings, and Swindles in Payments," with SentiLink's Dr. David Maimon.

Questions? Email us at publicpolicy@sentilink.com

Subscribe and view past editions here.

SentiLink