

Fraud in Focus: SentiLink Policy Insights

Volume 5

US Policy Insights

The Social Security Administration announced a significant change to eCBSV, with more on the way. What will this mean for fraud prevention?

- The SSA announced the first major operational improvement to its Electronic Consent-Based SSN Verification system, or eCBSV. This service has historically returned a binary "Yes/No" response to a name + DOB + SSN combination submitted by a financial institution (or its service provider). A new capability was added over the summer that makes it possible for a financial institution to receive more granular responses in the form of a "Yes/No" for each of the three data fields submitted. While the overall match response has proven helpful in detecting synthetic fraud, this additional data will help institutions better distinguish between harmless typos and more malicious activity, and better prescribe treatment strategies in certain cases. SentiLink was the first company to make this new data available to its partners.
  The Agency has also made clear that additional changes are expected next year. Under consideration is the expansion of the scope of what industries can use the service beyond financial institutions. SSA has also signaled that it plans to eventually sunset the legacy paper-based CBSV service, migrating those users to eCBSV.

The U.S. House Financial Services Committee solicited stakeholder input on privacy legislation. What is the outlook for Congressional action?

- The Committee published a request for feedback on a wide variety of key issues in the ongoing Congressional effort to advance comprehensive federal privacy legislation. As is relevant to this Committee's jurisdiction, many of the questions related to the future of the federal Gramm-Leach-Bliley Act (GLBA), the sector-specific law that forms the basis of modern financial privacy standards.
  SentiLink submitted comments emphasizing that privacy modernization efforts should seek to preserve and strengthen existing GLBA exemptions that allow financial institutions to use sensitive data for identity verification and fraud prevention, warning that eroding these protections could undermine consumer safety. We also recommended that any updated framework establish a single, preemptive federal standard to avoid a patchwork of state rules that complicate compliance and weaken fraud defenses.

  Congress has attempted to pass data privacy and data breach legislation since the mid 2000s — an effort which has consistently been derailed due to the breadth of competing jurisdictional interests and turf, primarily between banking and commerce Congressional committees. While efforts in recent years have had positive momentum, it has yet to be enough to carry any single piece of legislation beyond the committee stage to the floor of either the House or Senate. As such, the odds of enactment remain low.

The OCC, Federal Reserve and FDIC issued a Request for Information on issues related to payments fraud. What are some of the gaps policymakers need to fill?

- In their RFI, the agencies sought stakeholder input for ideas covering check, ACH, wire and instant payments fraud. In particular, the RFI asked how federal regulators and the private sector might strengthen external collaboration, and asked for recommendations on enhancing education, regulation and supervisory tools, and data-sharing practices to better identify, prevent, and mitigate different types of payments fraud.

  In our response, SentiLink urged federal regulators to modernize outdated frameworks and strengthen data-sharing programs to close critical fraud vulnerabilities. Our comments emphasized:
  - **Modernizing consumer protection laws**: Update ECOA/Reg B to verify legitimate relationships between account holders and authorized users, and tighten FCRA identity-theft claim procedures to prevent abuse such as "credit washing."
  - **Expanding federal–private data sharing**: Improve systems like SSA's eCBSV and modernize IRS income verification APIs to enable real-time, privacy-preserving fraud checks.

- **Leveraging modern fraud prevention tools**: Encourage agencies to explore more cutting-edge fraud tools rather than relying on legacy platforms that fall short on protecting taxpayer funds and program integrity.
- **Staying ahead of evolving threats**: Address emerging and expanding fraud trends, including synthetic identity fraud fueled by the misuse of so-called "credit profile numbers" and the growing role of generative AI in payments scams.

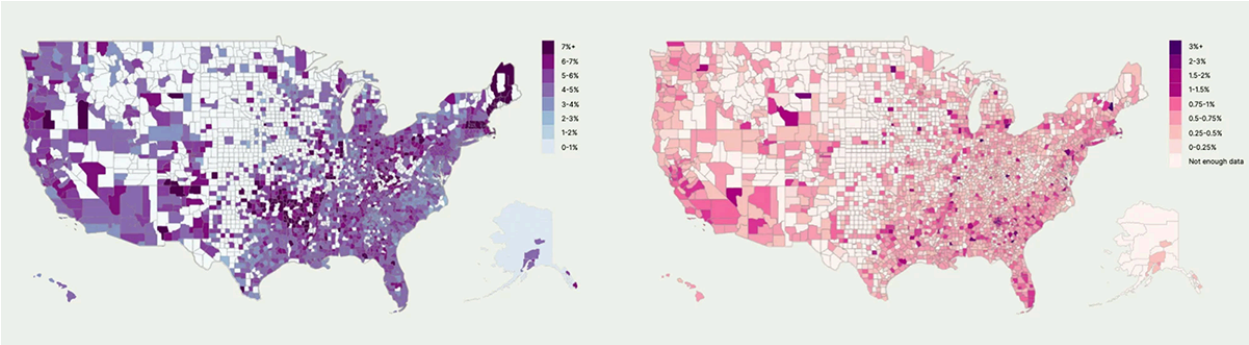
Fraud Spotlight

SentiLink published its second comprehensive fraud trends and benchmarking report, which can be downloaded here. The report — which analyzes data from more than 236 million applications — covers the first half of 2025. Key findings include:

- **Identity theft rates spiked** in both credit card and auto lending sectors late in 1H 2025, driven by coordinated attacks targeting major lenders;
- **Synthetic fraud rates fluctuated** during the first half of 2025, rising to cross the 1% threshold before dropping back to around 70 basis points;
- **Telecom companies experienced significantly higher fraud rates** than other industries, with identity theft averaging 10.15% and synthetic fraud at 2.9%;
- **DDA identity theft rates remained elevated** at nearly 800 basis points, continuing the trend from late 2024;
- **Fraud peaks in early morning hours**, with both identity theft and synthetic fraud rates highest between midnight and dawn;

Phone and email manipulation emerged as the strongest signals of identity theft across all industries.

Visual highlights: **Hotspots for identity theft victims (left, in blue) and synthetic fraudsters (right, in red)**



In the News

NBC: "A ripe target for identity thieves: Prisoners on death row."

Finextra: "The Intersection of Fraud Markets and Compliance Mandates: Why it's Time to Rethink CIP."

SentiLink: White paper — "Probability of Loss: Identity Theft Risk Across Breach Vector."

Payments on Fire: Podcast — "The hard science of fraud investigations" with SentiLink's head of fraud insights, Dr. David Maimon.

Forbes: "Fraud in America 2025: The Consumer Threat Landscape."

Questions? Email us at publicpolicy@sentilink.com

Subscribe and view past editions here.

SentiLink