Socure Unveils New Digital Identity Report on International and Domestic Fraud Rings Targeting Government Programs

NEWS PROVIDED BY
Socure ➞
May 15, 2025, 09:00 ET

Ground-breaking research uncovers novel tactics of organized fraudsters – from China, Russia, and other nations – against U.S. government programs

INCLINE VILLAGE, Nev., May 15, 2025 /PRNewswire/ -- Socure, the leading platform for digital identity verification, compliance and fraud prevention operating in over 190 countries, today released a new report that details common patterns of organized fraud networks from countries including China and Russia targeting U.S. public sector agencies.

According to **reports** from the Government Accountability Office, fraud costs the federal government upwards of $500 billion annually. During the pandemic, government agencies were flooded with fraudulent applications that went undetected by outdated methods and legacy providers. Now, AI-powered technologies are enabling fraudsters to supercharge their efforts, hitting government agencies and commercial entities at once, with relentless speed, and at scale.

"This research confirms what many of us have known – government agencies are under coordinated attack from nation states hellbent on exploiting weaknesses in existing identity infrastructure," said Jordan Burris, Head of Public Sector at Socure. **"This is a matter of national security. We need urgent**

investment in modern, accurate, and intelligence-led identity verification systems to defend against these threats. The time for half measures is over."

The report, entitled "**Fraud in Focus: Exposing Organized Fraud Patterns in Government Programs**," details three suspected fraud rings uncovered by Socure researchers. The rings – two international and one domestic – use a variety of tactics detected by Socure's AI-enabled verification platform. Common techniques included exploiting real Personally Identifiable Information, using fabricated business domains, shifting IP addresses through VPN providers, and submitting suspicious or mismatched phone numbers and emails.

Additional key findings include:

- **U.S. government programs are attacked by international fraud groups originating from China, Russia, Egypt, Poland and several other nations.** In this study, international bad actors were responsible for up to 12% of all incoming applications for government services and/or loans.
- **Fraudsters target multiple government agencies at once**. At least 1 in 4 fraud attempts targeted more than one agency.
- **Fraudsters are more likely to steal real identities rather than create fabricated ones.** Fraudsters were about four times more likely to use stolen identities instead of synthetic identities.
- **Bad actors attack both government and commercial entities with the same identities.** Commercial entities including fintechs and traditional banks, credit unions, auto lenders, telecommunications companies, online gaming and gambling were also targeted.
- **Bad actors evolve tactics to avoid detection**. IP addresses, email addresses and domains linked to an identity were shifted several times within a given day, severely limiting a rules-based or black-list approach to detection.

For the report, Socure conducted two distinct evaluations across government programs, each designed to surface fraud patterns.

The first analysis was conducted over a six-month period (September 1, 2024 – March 1, 2025) and leveraged Socure's Sigma Identity and Sigma Synthetic scores to identify high-risk fraud events, categorizing them as either synthetic identity fraud or identity theft. This dataset was used to support qualitative insights and to illustrate distinct fraud types and behavioral trends observed within government program activity.

The second analysis spanned a longer timeframe (January 2023 – March 2025) and focused on identifying international attack infrastructure. This research incorporated IP address geolocation, time zone analysis, and behavioral analysis to highlight patterns associated with coordinated fraud activity originating outside the United States. This analysis was intended to support broader risk intelligence community efforts.

Together, these analyses provide insight into the evolving threat landscape impacting public sector services and offer actionable steps to strengthen identity verification and fraud prevention strategies.

Socure is currently being used by more than 38 state and federal government agencies to stop fraud without compromising access to critical government benefits and services. Socure for Government (SocureGov) has achieved "Moderate" authorization from the Federal Risk and Authorization Management Program (FedRAMP®) and has been named to the State Risk and Authorization Management (dba GovRAMP) Program's Authorized Product List.

To download the full report, visit the website **here**.

About Socure

Socure is the leading provider of digital identity verification and fraud prevention solutions, trusted by the largest enterprises and government agencies to build trust and mitigate risk. Leveraging AI and machine learning, Socure's industry-leading platform achieves the highest accuracy, automation and capture rates in the industry. With the acquisition of Effectiv, Socure expands its capabilities to offer end-to-end identity fraud and payment risk management, integrating advanced transaction monitoring, credit underwriting and know-your-business (KYB) solutions into its platform.

Serving more than 3,000 customers across financial services, government, gaming, healthcare, telecom, and e-commerce, Socure's customer base includes 18 of the top 20 banks, the largest HR payroll providers, the largest sportsbook operators, 34 state agencies, four federal agencies, and more than 500 fintechs. Leading organizations including Capital One, Citi, Chime, SoFi, Green Dot, Robinhood, Dave, Gusto, Poshmark, DraftKings, PrizePicks, the State of California and many more trust Socure to deliver certainty in identity across onboarding, authentication, payments, account changes, and regulatory compliance.

Learn more at **www.socure.com.**

SOURCE Socure