LexisNexis®
RISK SOLUTIONS

Fraud Alert: Benefits Programs Under Attack

Physical and Digital Intelligence is Key to Stopping Fraud Networks

The LexisNexis® Risk Solutions Special Investigation Unit (SIU) recently detected a network of connected claims across six benefits programs. These claims all leveraged a manipulated email scheme attacking each of the states over a couple of years. Of the 90 uncovered transactions, the only successful fraudulent ones were submitted at an agency that utilized a single physical identity fraud prevention solution. When the agency utilized the combination of real-time authentication tactics leveraging both digital and physical identity intelligence, it empowered them with insightful and actionable decisions to help stop fraud before it occurs.

## Importance of a Digital-centric Approach

Agencies that leverage the power of a digital-centric approach – with the help of the LexisNexis Risk Solutions SIU team and its insights – have been proven to be more successful in detecting fraud networks. Our solutions helped detect and block complex fraud in real-time, and our unique identifier and program participant analyzer capabilities provided a 360-degree view of participants by merging offline and online data to establish true digital identities.

Notably, during SIU's analysis, the one state with only a physical identity layer of protection saw several, but not all, identities make it through the authentication process. SIU conducted analyses of email addresses across program participants to detect cross-agency use of shared data elements. This led to the detection of nine email addresses with similar formats, otherwise known as a manipulated email scheme. These emails were used across six benefits programs and with numerous identities. Additionally, the emails were first used as far back as 2021, with further activity in 2022 and 2023.

Fraud Network

The network in Figure 1 shows claims tied to the nine manipulated emails. Each icon showing a human silhouette represents an attempt at one of the six affected agencies. The colors denote the state in which the identity applied. The only successful transactions were those circled in **red**. These were at an agency that is only utilizing one authentication process without assessing the digital characteristics of the identity. The other agencies shown to the right were using a layered approach with both digital and physical risk assessments.
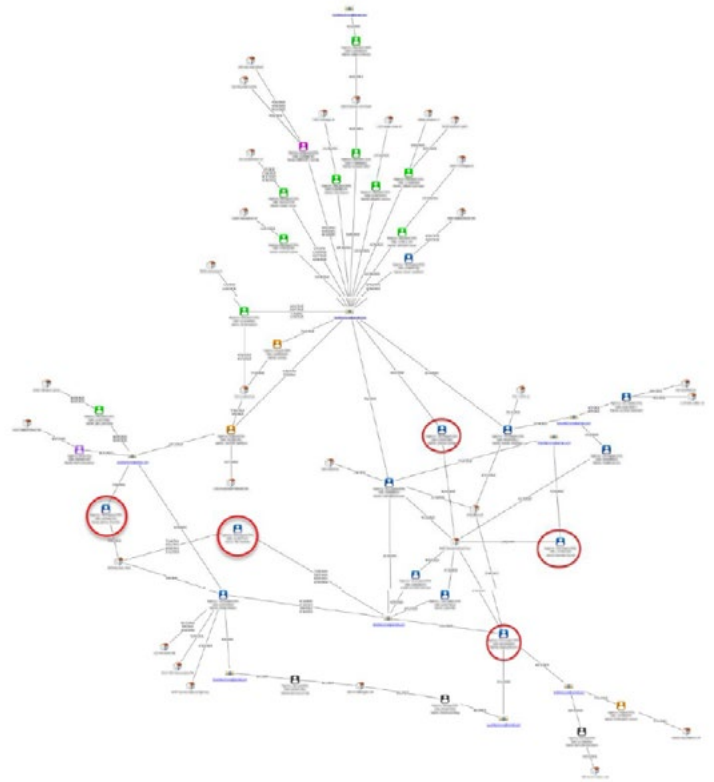
> The tools the criminals used in this fraud network are not hard to access. **Anyone could use or purchase these types of tools at very low prices.** The barrier to entry for fraud is very low: anonymously submitting claims in the benefit space is a low risk and potentially high reward for criminals.

Recommendations and Takeaways

The concept of criminals submitting claims in multiple states is not a new one. However, the above analysis shows the importance of protecting your agency with both digital and physical-based fraud prevention workflows and approaches. Help prevent program vulnerabilities by considering the following takeaways:

- Utilize multiple defenses to block fraud attempts from the network shown in Figure 1.

- Leverage a digital-centric approach are more successful in detecting fraud networks.

- Monitor for criminals who submit multiple claims across state lines and within different benefit programs.

The power of the **LexisNexis® Risk Solutions networks and data intelligence** by the numbers:

- 90 billion records from more than 10,000 different sources.

- HPCC Systems processes 270 million transactions every hour.

- 360-degree view of an individual with over 99.99% precision rates leveraging our LexisNexis® LexID® linking technology.

- LexisNexis® Digital Identity Network® analyzes more than 250 million transactions daily, and over 93 billion transactions annually.

LexisNexis® RISK SOLUTIONS

For questions or to learn more, contact your LexisNexis Risk Solutions SIU Fraud Analyst or email us at SIU@lexisnexisrisk.com

---