Deloitte.

To catch a fraudster: Following the digital breadcrumbs

Leveraging social media intelligence and tools in healthcare

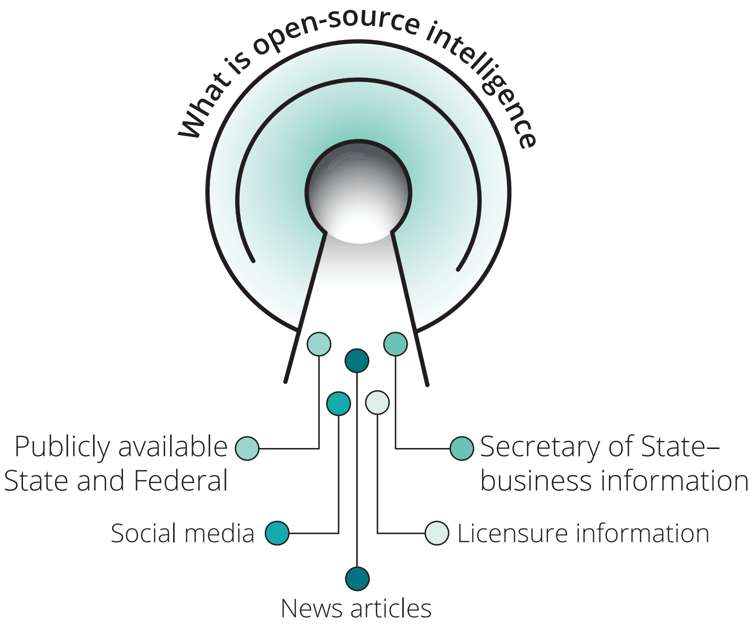
July 2023

MAKING AN IMPACT THAT MATTERS since 1845

Fraudsters utilize social media to their advantage to purchase, sell or acquire personal identifiable information (PII) and/or personal health information (PHI). This results in a personal and financial detriment to individuals and organizations. Social media has made connecting and communicating between fraudsters easier than ever. While the digital realm represents tremendous opportunities for fraudsters, it also provides open-source intelligence data for investigators to pursue "digital breadcrumbs".

Program integrity challenges in healthcare

The healthcare industry is ever changing, and with it, so must the methods and tools used to investigate fraud, waste, and abuse (FWA). As we continue to progress into the digital age, more and more services are provided through electronic means. These services create opportunities for fraudsters to hatch new schemes. Investigative techniques to identify, track, and trace schemes, trends, and connections between suspected providers have also moved into the digital realm with demonstrated success. For example, by using open-source intelligence, we can identify instances where Medicare Beneficiary Identifier (MBI) information was being openly marketed and sold online.

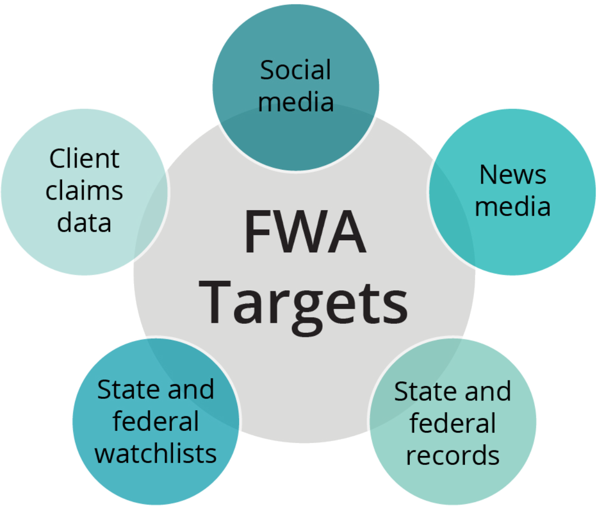

What is open-source intelligence
Publicly available State and Federal
Social media
News articles
Licensure information
Secretary of State– business information

Historically, FWA investigations within the healthcare space have relied heavily on an analysis of claims data, prioritizing quantitative data analysis to detect anomalies and outliers that could indicate FWA. However, this approach often results in investigators playing catch up with fraudsters due to the time lag of data reporting, collection, analysis, and interpretation. Integrating claims-only analyses with open-source intelligence, such as social media, to identify FWA is effective. This approach looks for the nexus of known bad actors to highlight their fraudulent networks and connections. Incorporating social media helps investigators identify suspect providers and their networks. However, it is an underutilized and underdeveloped tactic across the industry.

Advantages of social media in the investigative process

Deloitte proactively utilizes social media to enhance the investigative process to identify and investigate sources, fraud schemes, and leads. Our approach "humanizes" the data to represent the person or persons involved in the scheme. By focusing on the individual's publicly available data and social media, we can get near real-time updates and changes in the fraud landscape, keeping investigators on top of emerging players and schemes. Social media provides four main benefits for investigators:

- **Early scheme identification**
- **Identification of at-risk network connections**
- **Prioritization of at-risk providers**
- **Proactive lead generation approach**



We can help investigators obtain direct knowledge of the individual(s) behind the identified scheme. Using social media, we can tell a more comprehensive story of the scheme and individual. Integrating information like property ownership, criminal history, shared contact information, other business linkages, and complaints into the investigation provides a more holistic understanding of the situation, acting as a method of quality control unmatched by a claims-only approach.

In addition to helping investigators identify providers and schemes faster than traditional methods, the open-source first approach has several other benefits. Using network analysis can drastically increase investigation efficiency by helping to identify and prioritize the riskiest leads. For example, linking suspect providers through practice ownership or shared billing entities allows us to trace fraudulent networks to their source. By identifying compromised PII and PHI on social media, we can identify networks of suspicious actors leveraging compromised patient information that may not be connected in any other way.

This approach enhances investigations and provides greater insight into not only individual providers but the collective of providers working together. Additionally, once these individuals are identified it becomes much easier to select leads for additional development. By prioritizing targets based on their digital red flags, they can be ranked on their level of organizational threat. This process helps drive case selection to prioritize investigations with the highest return on investment (ROI). Deloitte recognizes healthcare payers have limited time and resources available, and this approach can avoid wasting time and money following dead ends and non-actionable leads.

Deloitte offers analytics solutions

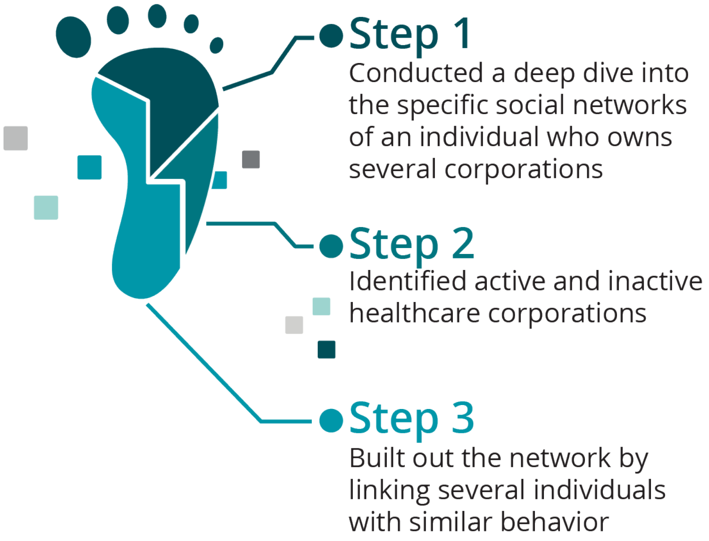
By taking an open-source and human intelligence approach, we remove assumptions early in the process, turning "digital breadcrumbs" into relevant actionable intelligence. The incorporation of social media and third-party analytic techniques in the investigative process plays a significant role in increasing investigators abilities to fight FWA. Deloitte provides services, partners and products, that actively monitor social media. Below, are several tools Deloitte offers:

- AI tools that search deeper and faster for relevant information and learn from investigative counterparts
- Tools that aggregate social media and news alerts based on hashtags and keywords
- Tools that summarize social media and public records for specific targets
- Tools that scrape publicly available data from web sites around the world

Real world use case

Identifying collective groups of risky providers allows for a holistic view of potential FWA. Is the provider part of an emerging FWA trend or is the provider new to healthcare and requires some additional education?

Below is an example on how our approach identifies "digital breadcrumbs" of information and develops them into a more comprehensive investigation involving healthcare providers who turned out to be bad actors. This approach results in high quality lead development and is more likely to be accepted by law enforcement:



Step 1
Conducted a deep dive into the specific social networks of an individual who owns several corporations

Step 2
Identified active and inactive healthcare corporations

Step 3
Built out the network by linking several individuals with similar behavior

How Deloitte can get you started

As new fraud trends emerge and are identified, fraudsters learn how to avoid getting caught, shut down their operations, and pivot to new schemes. The ability to shift quickly is an advantage for the fraudsters. By integrating social media into the investigative process, Deloitte identifies schemes and at-risk networks early and generates prioritized leads creating actionable solutions. Utilizing Deloitte's comprehensive approach and the tools described above will narrow the gap quickly, not only helping to identify those "bad" actors but also by linking them to other schemes. Deloitte can alleviate any concerns clients might encounter when utilizing social media in investigations. Deloitte's experience will quickly assist our clients in identifying problematic actors or service areas and generate investigative successes. Contact Deloitte for additional information.

The benefits of open-source information

- Early scheme identification
- Identification of at-risk network connections
- Prioritization of at-risk providers
- Proactive lead generation approach

Contacts

Kelly Bowman
Principal Program Integrity
Deloitte LLP
Program Integrity
+1 571 814 7098
kelbowman@deloitte.com

Dan Olson
Vice President Product Management
Deloitte LLP
Program Integrity
1 312 486 2805
danolson@deloitte.com

Gary Cantrell
Specialist Leader
Deloitte LLP
Program Integrity
+1 703 509 5824
gacantrell@deloitte.com

Antonio L. Valdes
Manager
Deloitte LLP
Program Integrity
+1 786 512 6113
antvaldes@deloitte.com

More information

For more information, visit
Deloitte's Program Integrity Solution | Deloitte US

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.
As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services, and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. Please see http://www.deloitte.com/us/aboutfor a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Designed by CoRe Creative Services 1442016