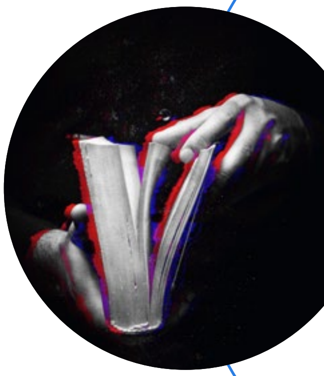
What can Aristotle teach you about your anti-fraud strategy?



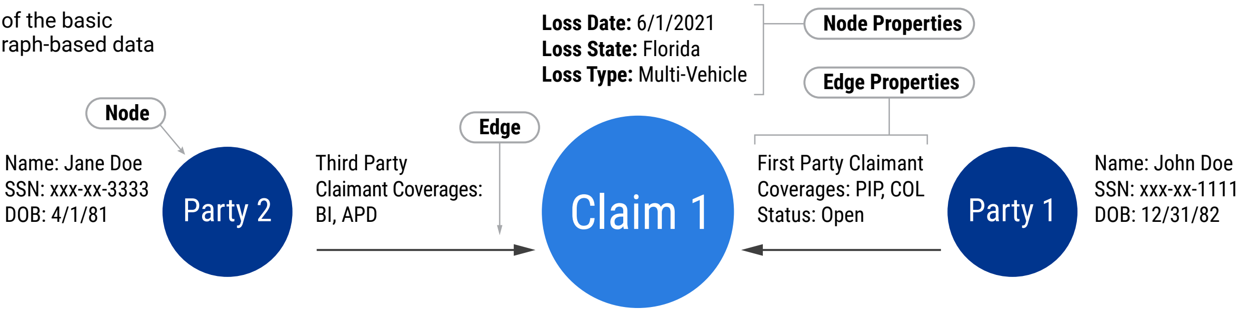
The Greek philosopher Aristotle once wrote: “The totality is not, as it were, a mere heap, but the whole is something besides the parts; there is a cause.”[1] There are unique properties and purposes of organizational structures that are not always present intrinsically within its individual members. For example, a group of musicians (the parts) are not the same thing as an orchestra (the whole). As H.E. Luccock said, “No one can whistle a symphony. It takes a whole orchestra to play it.”[2] There’s a common theme between this Aristotelian perspective and symphony orchestras – and it’s an idea we can apply to catching insurance fraud through social network analysis (SNA).

What is SNA?

The roots of SNA can be traced to a handful of social scientists in the early nineteenth century.[3] Since then, the use of SNA has spread rapidly to a wide array of academic and business applications. The defining feature of social network analysis is its focus on the structure and patterns of relationships.[4]

In practice, SNA uses networks and graph theory to understand social structures.[5] Nodes refer to the entities in the network and edges refer to the relationships and interactions between them. Node and edge properties provide additional data points about entities and relationships respectively. Figure 1 illustrates those basic building blocks of graph-based data that is the foundation of SNA techniques.

Figure 1. Examples of the basic building blocks of graph-based data



What is distinct about SNA in fraud detection?

SNA is uniquely positioned to fill a gap that other analytic methods are simply not designed to accomplish. Unlike many other analytic techniques that assume independence of observations being analyzed, SNA is specifically designed to analyze and derive insights from the interconnections of subjects within data.

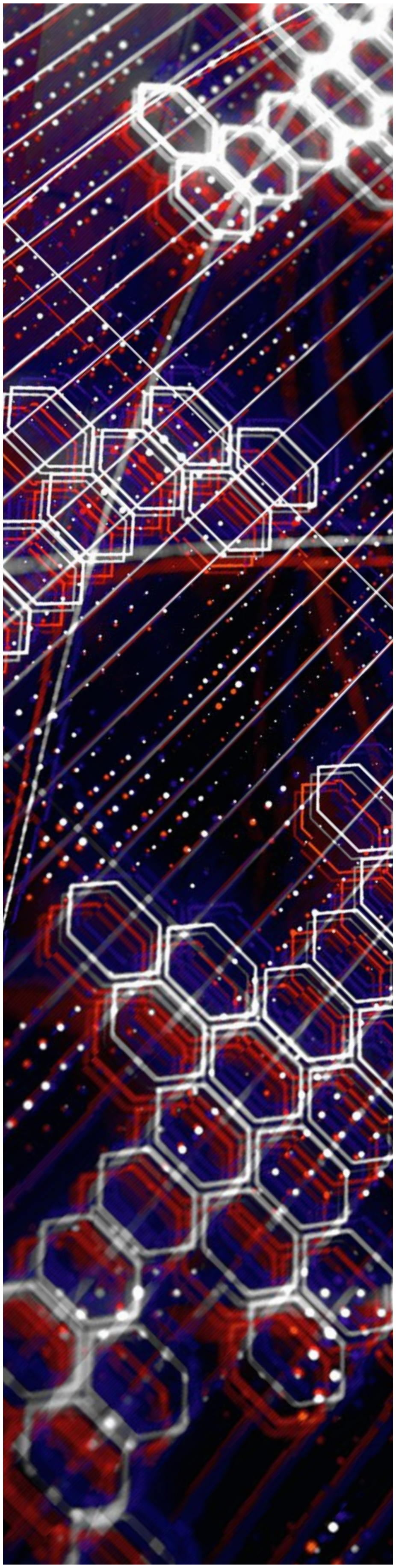
When it comes to insurance fraud, a major objective of an organized crime ring is to fly under the radar to avoid detection. Individual claims that stem from organized fraud structures tend to blend in with meritorious claims. Yet if the connections between those siloed claims could be uncovered, it would be much easier to see the organized structure that's orchestrating it all.

And that's important for insurers to consider when constructing an anti-fraud approach. For example, a claim-level Machine Learning model or scoring routine might help prioritize potential fraud risk at a singular event level. However, carriers would need SNA in place to proactively identify and prioritize potential fraud risk of network structures—and to expose emerging, complex, and organized risks within connected data. Given that these techniques offer different strengths, using both to leverage their unique advantages results in a more robust anti-fraud perimeter defense.

What data do we need for SNA?

Any analytical method requires the right data as the fuel to deliver useful insights—and SNA is no exception. Given that SNA is underpinned by nodes and their relationships, it is extremely helpful to have as complete a view as possible of network structures to derive the most value from them. Since insurance customers are distributed over many carriers and tend to move between carriers over time, cross-carrier data is essential to combat fraud proactively using SNA methodologies.

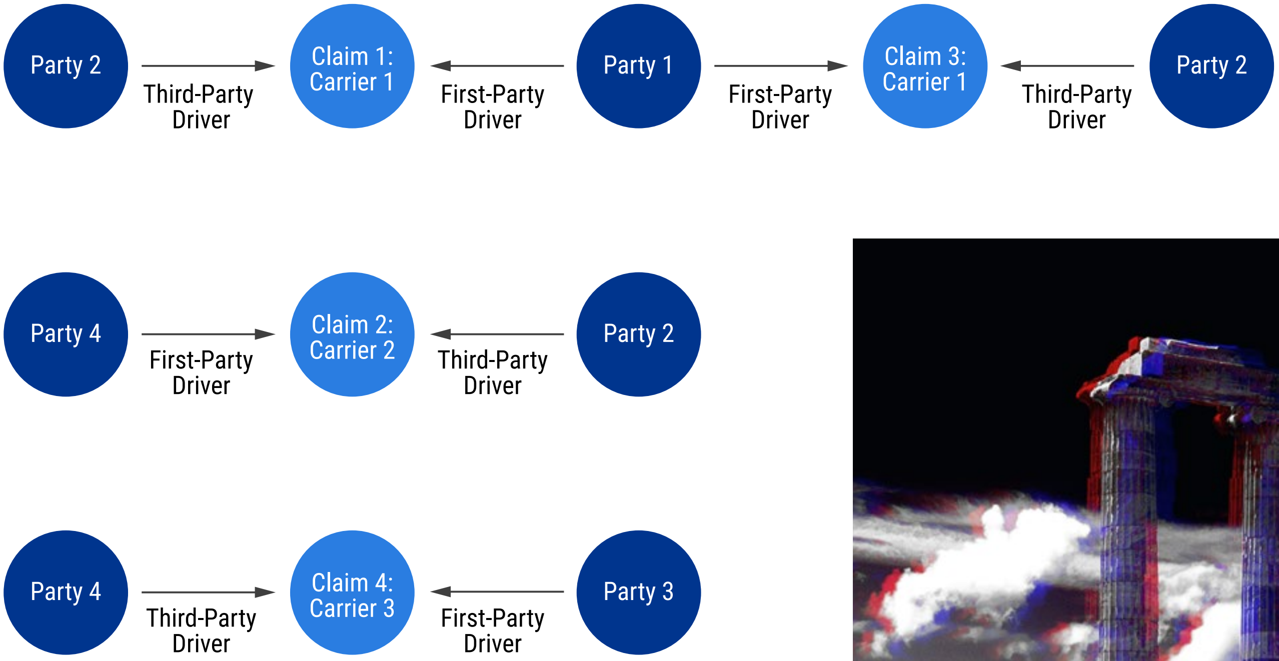
While it's a cliché, the "garbage in, garbage out" principle is the idea that the quality of output is heavily impacted by the quality of input. However, a given analytical pursuit could have the cleanest data available but still may not have the right data to reach valuable conclusions. Whereas "garbage in, garbage out" is akin to putting bad fuel in your car, not having the right data is like trying to run your car on empty.

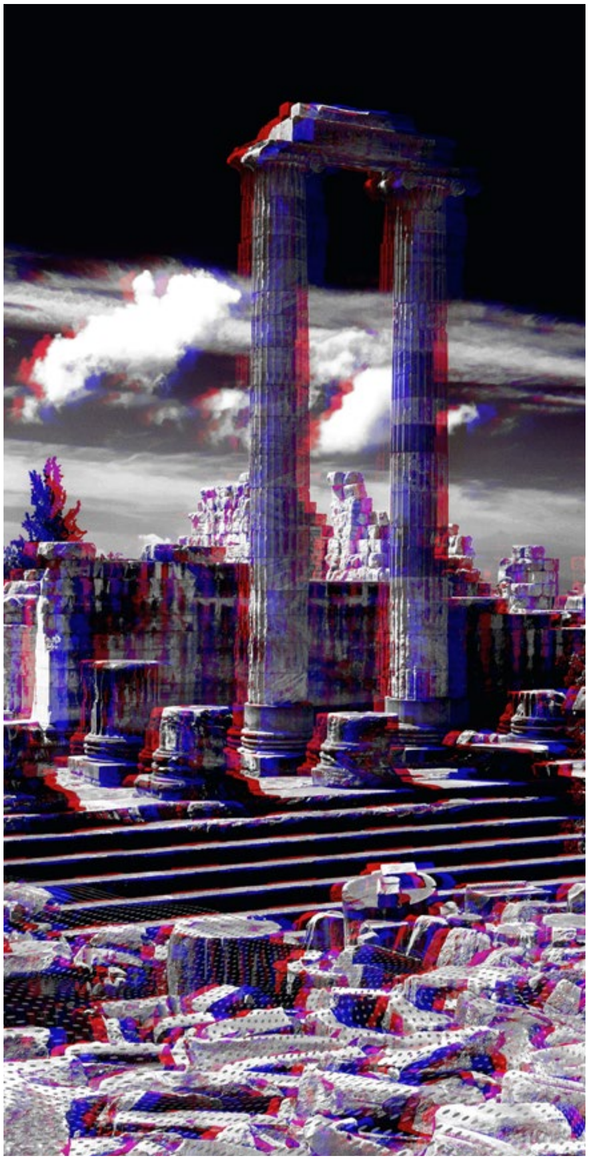


Missing relationships miss fraud

Consider the following example. Figure 2 shows three individual carrier views of network structures that link involved parties to associated claims. To each of the three carriers, these individual views represent benign network structures from a fraud perspective, since—individually—they represent common claim dynamics.

Figure 2. Individual carrier-based views of involved parties linked to associated claims

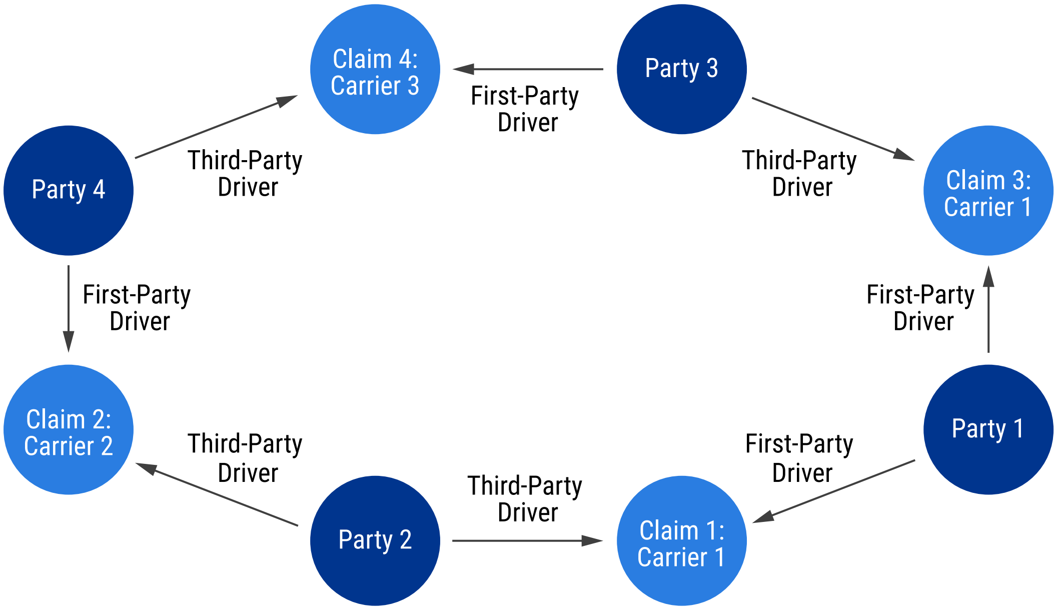




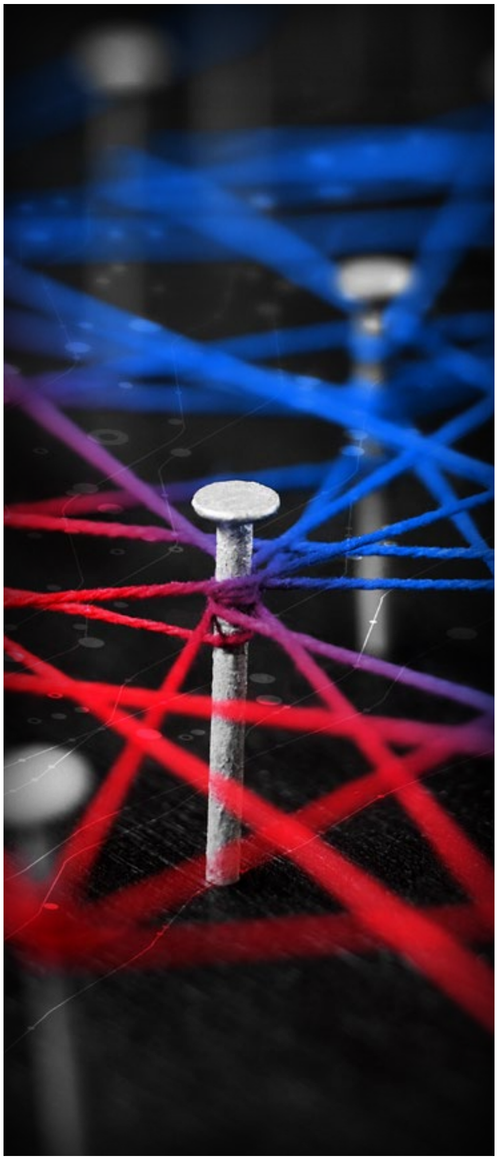
However, a very different picture emerges when analyzing this same exact data in an aggregated, holistic view. Instead of three discrete networks, we observe a single network cluster as displayed in Figure 3. Additionally, in this example, a circular path emerges that reveals implicit relationships within this ring of entities and provides analytical insight that each individual view completely misses in their respective siloed perspective.

However, a very different picture emerges when analyzing this same exact data in an aggregated, holistic view. Instead of three discrete networks, we observe a single network cluster as displayed in Figure 3. Additionally, in this example, a circular path emerges that reveals implicit relationships within this ring of entities and provides analytical insight that each individual view completely misses in their respective siloed perspective.

Figure 3. Industry level, holistic view of involved parties linked to associated claims



This is where we come back to Aristotle and his view that the whole is something besides the parts. It is only with a complete view of this claims network that we can be alerted to the possibility for potential collusion (the cause) among this collective group (the whole) of entities (the parts). This analytical insight fundamentally hinges on the available breadth and wholeness of data going into the analysis—data that breaks past the constraints of carrier-specific silos.



Connecting the data with SNA

It's clear that SNA is one key component in a well-rounded anti-fraud strategy. It's a powerful analytical technique that can be used in combination with other analytic methods to detect potentially fraudulent claims—and, at the same time, clear the way to efficiently respond to meritorious claims.

But for SNA methodologies to reach their full potential in fraud fighting, they must draw upon broad, industry-wide data sets. Only cross-carrier information could provide the fuel to generate the insight in the example above—and in your own book of business. While there are certainly many other factors to consider for successfully leveraging SNA methodologies, completeness of data is extremely foundational because gaps in data wholeness prevent certain types of insights from ever being discovered.

Using broad, industry-wide data is a critical starting point for SNA to push beyond individual, limited views of claims and to mine the hidden properties of the whole. Verisk's ClaimSearch database is unique—the country's most comprehensive database of property/casualty claims with more than 1.6 billion records and participation from over 90 percent of the industry. Verisk also manages the Aggregated Medical Database (AMD), which collects industry-wide medical billing records from claims. The AMD is leveraged by Verisk's MedSentry solution to uncover medical provider fraud, waste, and abuse. To find out how Verisk solutions can help insurers leverage SNA techniques, please reach out to Scott Newkirk.

Endnotes

1. http://classics.mit.edu/Aristotle/metaphysics.8.viii.html#:~:text=In%20the%20case%20of%20all,or%20some
2. https://libquotes.com/halford-e-luccock/quote/lbu4a0e
3. https://reflexus.org/wp-content/uploads/Network_Analysis_History_of.pdf
4. https://link.springer.com/chapter/10.1007/978-981-10-0983-9_9#Fn5_source
5. https://www.sciencedirect.com/topics/social-sciences/social-network-analysis

Verisk™

Learn more about Verisk's Anti-Fraud solutions

Scott Newkirk | Director of Network Analytics, Anti-Fraud Solutions Group, Claim Solutions

Scott.Newkirk@Verisk.com / **+1.984.202.1088**