Stopping The Catheter Fraud Scheme

April 2024

Greg Lyon, Fraud Prevention Advisor

> **“In short, much of the $2B in potential exposure could have been mitigated.“**

Over the course of 2021, 2022, and 2023, malicious actors perpetrated a massive fraud scheme, defrauding Medicare and the United States healthcare system of up to $2 billion through the submission of phantom claims for intermittent urinary catheters.

This article outlines the fraud scheme and explores how it was able to occur with current technology and detection approaches. It also highlights opportunities to deploy integrated artificial intelligence and continuously updated provider data platforms to detect and prevent similar schemes in near real-time.

The Scheme: Ownership Change, Test & Spike

Seven legitimate Durable Medical Equipment companies (DMEs) were purchased by fraudulent individuals. Once the ownership had been transferred, new owners validated their ability to bill Medicare and receive payments. With the ability to bill and get paid confirmed, the fraudsters proceeded to spike large volumes of claims to Medicare for intermittent urinary catheters.

The claim volumes were:

2023
406,000

2022
20,000

2021
21

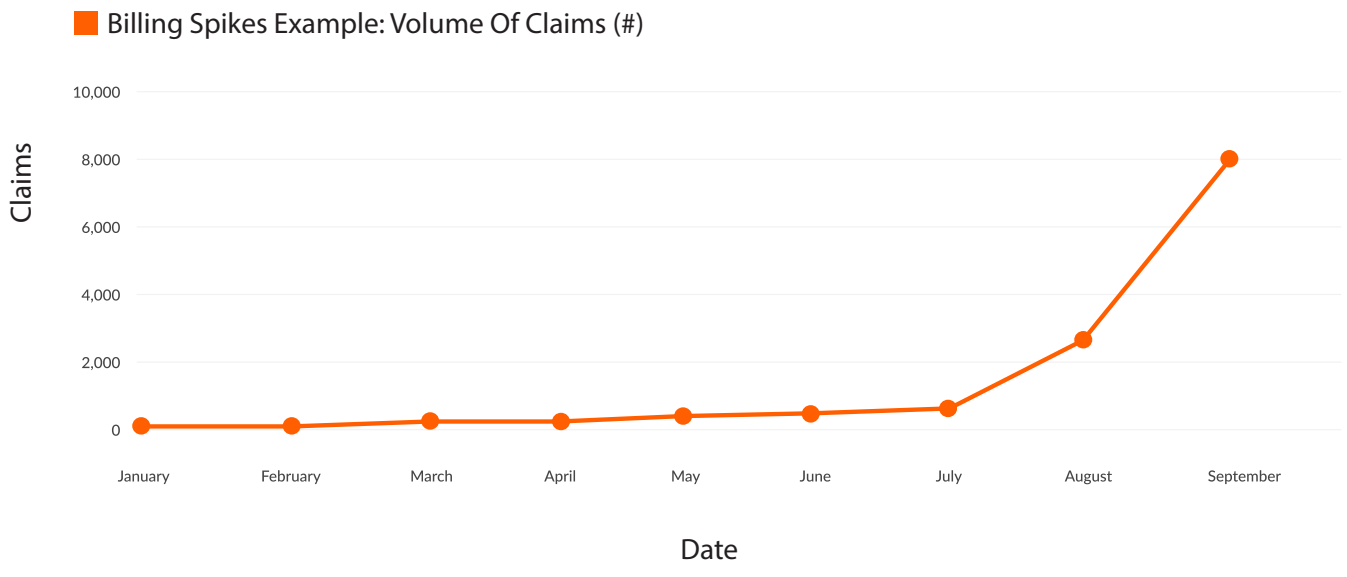
Phantom Billing

“The catheter scheme had red flags that, in retrospect, look obvious.“

The spike from claims submitted by the seven DME companies was so extreme that it caused a noticeable national spike in intermittent urinary catheter claims. This was a ‘phantom’ billing scheme, where the catheters were not medically necessary and were not physically shipped to the Medicare members.

To perpetrate this fraud, the seven DME companies exploited legitimate Medicare member names and IDs to submit the fraudulent claims. It is highly probable that the member data was illicitly obtained, either purchased on the dark web following a data breach or gathered through deceptive cold calls from fraudulent telemarketers preying on unsuspecting Medicare members.

Once this phantom billing fraud scheme was detected, the seven DME owners stopped submitting claims and closed the DME businesses. In at least one known instance, the DME owner fled the United States to evade justice.



PROVIDER SCHEMES *like the catheter scheme, can be prevented with continuous provider-centric contextual claims analysis that detects anomalies such as billing spikes. These spikes are a deviation from normal provider patterns and can be detected pre-payment when monitoring provider behaviors and relationships around claims, patients, and other providers.*

Red Flags

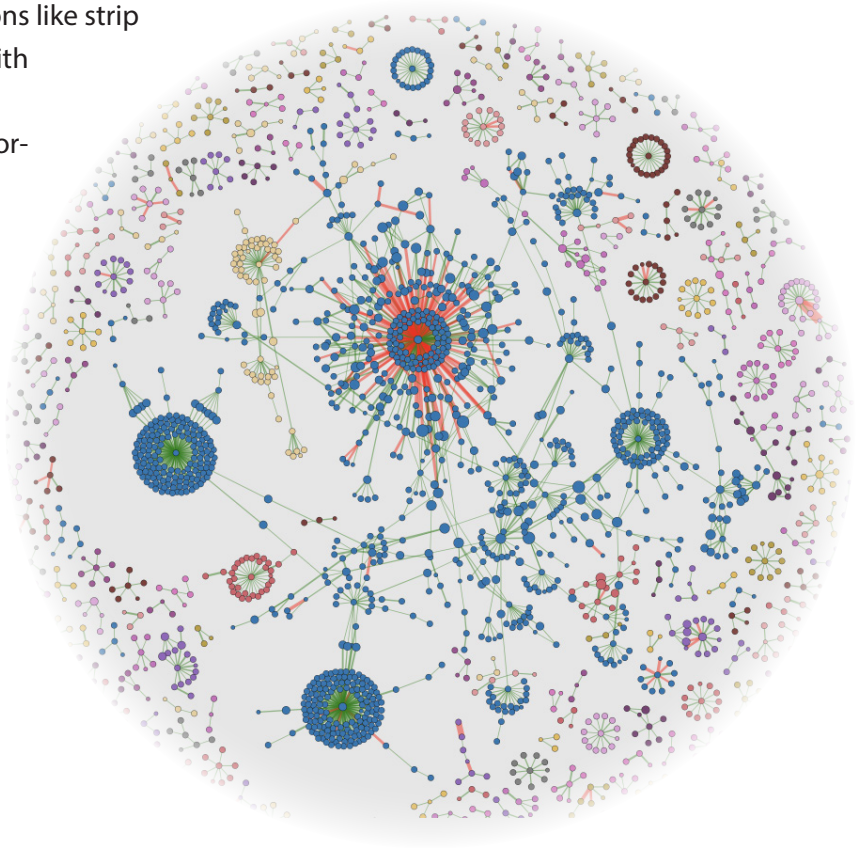
The catheter scheme had red flags that, in retrospect, look obvious. Further, many Special Investigation Units (SIUs) remain challenged with the limitations of claims data-centric, rules-based analytics and periodic (not continuous) provider integrity monitoring. The following red flags could be easily missed when reviewing each claim and each provider in isolation:

- Rapid increases in intermittent urinary catheter claims for seven DME companies (14 to 20,000 to 406,000).
- No history of significant urinary catheter claims for any of the seven DME companies.
- Sudden spikes in claims (or claim type) shortly after an ownership change.
- Suspicious business locations like strip malls, residences, offices with windows covered, etc.
- Common demographic information shared among the seven DME's (matching addresses, officers or ownership).
- Numerous negative social media reviews from Medicare members detailing suspicious behaviors.

Three Technology Tips To Stop The Next Fraud Scheme

Stopping the catheter fraud scheme, or future schemes of a similar nature, requires a fundamental shift in how fraud detection and prevention is accomplished. Healthcare payors can no longer afford to depend solely on claims data-centric analytic models to detect potential fraudulent behaviors and relationships fast enough. We must be able to assess each provider's integrity, relationships with other providers, and claims activity in the context of all historical and near real-time claim behaviors. In short, we need to change our mindset and leverage available technology to solve this problem.

(continued on following page)



CONTEXTUAL MAPPING: *Continuous provider credentialing coupled with contextual claims analysis detects suspicious referral, ownership, multi-party collusions and other behaviors in a way that makes it easy to create near real-time visual maps (see image above) of suspicious claims, provider, and patient behaviors.*

There are three technology and process approaches within reach of any healthcare payor from large health plans to the smallest third-party administrator (TPA). These three approaches include:

1. Know Your Provider

Start with a provider-centric approach.

Take a 'Know Your Provider' (KYP) mindset, just like financial services companies employ a 'Know Your Customer' (KYC) approach to anti-fraud work. To detect fraud early you need to continuously gather and analyze provider data in near real-time to understand their integrity, behaviors and relationships with other providers. Provider-centric data such as licensing, sanctions, address, phone number, social media reviews, bankruptcies, criminal offenses, ownership interests, shared addresses and phone numbers, taxonomy, and other data elements help to continuously flag potential problematic providers. This comprehensive provider data enables payors to have a continuously updated profile of each provider so changes that could be indicative of fraud can be identified and addressed immediately. In addition, this approach allows the network team to continuously 're-credential' providers from an integrity perspective and make informed decisions about whether to do business with out-of-network providers.

2. Comprehensive & Dynamic

Continuously integrate KYP data with historical and real-time claims data to understand context around every claim.

Combining KYP data with historical and current claims data empowers healthcare payors to analyze behaviors in near real-time:

- Every claim submitted against individual provider historical and current-claims submission behavior
- Every provider's claims submission relationships (referring, rendering, billing)
- How an individual provider's historical and current claims submission behavior aligns with all other providers' claims submission behavior (outlier behavior).

This is all doable today with a combination of the right provider data and provider-centric artificial intelligence technology incorporating supervised and unsupervised machine learning.

3. Next-Gen Fraud Fighting

Seek accessible cutting-edge technology.

One mistake many payors make is assuming that cutting-edge AI, ML, neural network, graph, etc. technologies are only for big companies, prohibitively costly, or just for the most tech-savvy individuals. Fortunately, some of these advanced technologies are now available as user-friendly solutions that offer clear returns-on-investment, streamlined deployment, and increased efficiency for fraud and SIU teams.

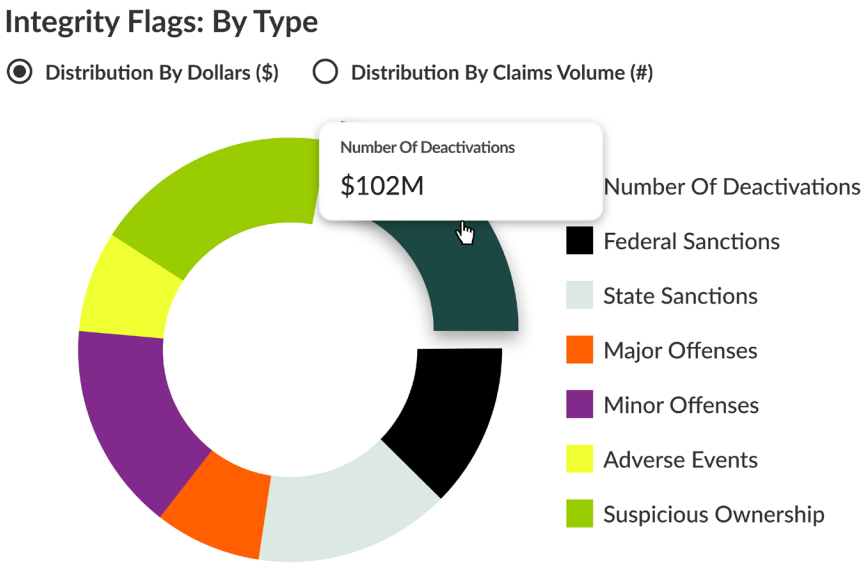
Early Detection

How Technology Tips Would Have Detected The Catheter Scheme

Deploying the technology tips mentioned on the previous page would have had a major impact on the catheter scheme or one with similar characteristics. Let's assume that in 2021, a KYP solution that continuously monitors all 7.9M U.S. NPIs was in place. And let's also assume that an integrated provider-centric artificial intelligence technology that contextually analyzes individual claims, provider behaviors and relationships in the context of all claims and all providers in near real-time was available.

What is likely to have happened?

- Payors would have been alerted to the claim volume spikes in near real-time in early 2022 as the scheme was in it's early stages. The identification would have happened pre-payment – in time to stop suspicious payments and investigate before claims were paid.
- The seven DME's responsible for the catheter claims spike would have been identified.
- SIU investigators would have received comprehensive KYP integrity data on the seven DME's including data showing the lack of catheter claims history, shared ownership, officers and addresses, Google Earth images of office locations, social media reviews and catheter claims data.
- This integrated, contextual data picture would have enabled investigators to rapidly open investigations on each of the seven DMEs and place pre-pay flags in accordance with their organization's policies.
- SIU Investigators could have quickly interviewed members which would have shown that the catheter claims were fraudulent 'phantom' claims.
- SIUs may have had the opportunity to involve law enforcement earlier with clear evidence of fraud.
- In short, much of the $2B in potential exposure could have been mitigated.



PROVIDER INTEGRITY FLAGS: *Continuous provider integrity data elements monitoring would have flagged some of the problematic ownership interests associated with DMEs involved in the catheter scheme. Provider integrity can literally change day-to-day and continuous integrity monitoring can mitigate losses from organized multi-party fraudsters as well as individual providers that resort to FWA schemes due to personal situations.*

About The Author

Greg Lyon is a recognized anti-fraud expert with over 25 years of experience in the Financial Services and Healthcare industries. His guiding principle, "the best way to fight fraud is to prevent it," has been the driving force behind his passion for innovation and dedication to safeguarding members and the fiscal integrity of health plans.

In his time at United Healthcare as Director of Fraud Prevention, Greg provided strategic leadership for the fraud prevention program. He spearheaded the ideation, execution, and enterprise-wide support of industry-leading capabilities designed to identify and mitigate gaps while instilling a prevention mindset into the company's DNA. One of his major accomplishments was conceptualizing and executing an industry-leading capability that leverages robust identity validation and investigation processes to identify and prevent fraudulent providers from submitting claims. Since its inception in 2018, this program has generated significant avoidance savings by stopping scores of fraudulent providers.

Greg also ideated and executed an industry-first predictive fraud analytics model that utilizes open-source data instead of claims data, harnessing innovative technology to generate high true positive rate leads for SIU Investigation. His innovative approach led to a 2023 patent application where he is a named inventor.

Greg has shared his expertise in multiple presentations at the National Health Care Anti-Fraud Association's Annual Training Conference (NHCAA ATC) by creating educational content and courses to help fraud investigators understand and deploy advanced artificial intelligence technologies to prevent healthcare fraud. His commitment to protecting healthcare organizations and their members from fraud's detrimental effects has positioned Greg as a leader in new technology adoption in the healthcare fraud community.

Greg Lyon

Fraud Prevention Advisor
+1 (612) 801-8684 | glyon.lyon@gmail.com
Read Online: News and Publications