CHAPTER 7

CRIMINAL FRAUD IS MUCH BIGGER THAN YOU THINK

Most of us think of fraud in health care as the domain of a few bad doctors, similar to what exists in virtually any human enterprise. In reality, it adds up to a staggering $300 billion annually, roughly 10 percent of all spending.[80] It is also remarkably straightforward to stop, but only if claims administrators—those actually able to stop it—do so. Yet most lack the financial incentives to do so, only making basic attempts after-the-fact that are like trying to stop fraud with a musket in an era of unmanned drones.

More alarming is that significant fraudulent gains may go to foreign actors. The world's cybercrime hotspots are all outside the United States, according to *Time*.[81] *Infoworld*[82] explained why hackers want your health care data. Among other reasons, it has a much longer shelf-life than other targets like credit cards, which become useless once a consumer gets a new card. However, medical and insurance information has value for years.

If fraud weren't bad enough, the fact that it is leaving the U.S. economy makes it even more of an economic drain. Stopping fraud would be like providing the American economy with an annual recurring $300 Billion economic stimulus. Over two-plus years, that stimulus would be equivalent to the massive stimulus at the beginning of the 2008 financial crisis.

Health Insurance Carriers Are Acting Rationally

There are two key drivers of insurance carrier economics that are relevant to understanding criminal fraud. (These issues were covered more thoroughly in Chapter 3).

1. Anything that drives health care spending upward, even paying fraudulent claims, economically benefits insurance carriers and claims administrators.
2. The ACA's Medical Loss Ratio cap requires that 80 to 85 percent of premium dollars go to care, not marketing and overhead. Because fraud prevention isn't considered care, this reduces economic incentives to invest in it. Technology and other solutions that prevent fraud are just another expense that eats into this government-mandated margin cap.

Even if an employer is self-insured, there is a spillover effect as insurance carriers are generally motivated to invest in technologies and services that fuel revenue increases rather than reduce spending. In other words, there isn't a strong enough motivation to root out waste and fraud.

It's important to highlight how only-in-health-care dynamics open the door to large-scale fraud in the first place. Pay and chase programs (covered in Chapter 3) are like paying a napping guard extra money to chase a criminal who just cleaned out the bank vault. According to private conversations with industry insiders, claims administrators are doing little to stop fraudulent claims. Instead, after allowing fraudulent claims to be paid, they chase after the thieves, receiving 30 to 40 percent of what they recover.

The Data Problem

More fraud creates more upward premium pressure that economically benefits insurance carriers, but takes from everyone else. The root of this is the U.S. health care system's current

claims methodology that is fraught with disconnection and a lack of transparency and control between employers, patients, providers, and insurers. In contrast, the financial industry has been using preventive methodologies for decades, giving the consumers both security assurances and control over their credit, resulting in much lower credit card fraud rates—just 0.07 percent of total volume.[83] This means the cost of health care fraud is 14,285 percent higher than credit card fraud.

The comparably large and equally complex health care industry has generally avoided adopting similar prevention methodologies, erroneously citing a billing and payment system that is too complex for it to work. As a result, employers have resorted to taking a reactive and largely ineffective approach to recovering money after claims have been paid. This "pay and chase" method delivers a dismal average return rate of only 2 to 4 percent—enough to say something is being done, but a drop in the bucket compared to the full magnitude of the problem.[84]

When it comes to auditing claims to identify fraud, insurance carriers have historically relied on sampling methodologies to determine whether or not the claims process is sufficiently secure. Health care claims reviews are done independently on a per-visit basis and are largely a paper-driven process. This allows fraud and waste to fall through the cracks because there is so much disparate data and no standard format for how it is analyzed and processed.

Separately, the industry has pushed to auto-adjudicating claims as quickly as possible, a good thing if not for the lack of correspondingly robust implementation of fraud (and waste and abuse) detection and prevention technologies and processes. "The current claims process is predicated on rapid processing of health care transactions with little real emphasis on the legitimacy and accuracy of the claims themselves," states Scott Haas, Senior Vice President of Wells Fargo Insurance Services USA, Inc. "The Department of Labor claim processing regulations emphasize the time frame in which claim payers must either pay or deny claims. The regulations assume payers are

actually diligent in assessing whether or not the claims require any form of audit or scrutiny."

Such antiquated processes, disparate data, and unintended regulatory consequences creates a macro-situation ripe with subjective interpretation of claims and claims data, often making the eventual reconciliation of plan coverage and payment too late. Often, this also leads to legitimate claims being denied erroneously, further adding to the frustration of everyone involved in the claims paying process. It's a costly failure for everyone.

Connecting the Data Points

Fraud only becomes visible when you connect all of the care participants and events. Here are two real-life examples I've seen.

- A woman undergoing multiple hysterectomies
- A man getting multiple circumcisions from different providers in a single week

Technically, these cases each meet all of the basic claims review and adjudication criteria (e.g., all of the fields are filled out and don't have dates where numbers should be or numbers where text should be). Therefore, they pass the sufficiency test and the claims are paid. However, it's obvious that both are fraud.

The problems from not connecting the dots can be less obvious than multiple instances of one-in-a-lifetime procedures. One example is a case where four doctors provided the same service to the same patient during the same procedure. When each provider's claim is viewed independently, the claim meets sufficiency criteria and thus passes the paid claims review test. But the total amount they're charging far exceeds the total allowable amount for the contract.

Big data and technologies similar to those used for services like Visa Fraud Protection make it possible to identify, predict, and minimize fraud through advanced analytics for detecting fraud and validating claim accuracy and consistency.

Payment integrity technology is available that can analyze disparate claims data at the employer, patient, provider, and insurance carrier levels, simultaneously across all health care systems. Such technology-based systems can connect a patient's behavior with the relevant physician behavior. For example, a patient who has had a hysterectomy in the past and suddenly has pregnancy-related claims should be flagged. By contrast, the financial services industry has used similar behavior patterns both at the retailer and consumer levels to identify purchases that do not fit the consumer's normal behavior since the earliest days of credit cards.

Payment integrity solutions break the reactive "pay and chase" approach with innovative solutions that could nearly eliminate fraud, making it unnecessary for employers to chase after already spent money. These types of solutions will play a critical role in reducing the exorbitant amounts of money lost to fraud and waste in the health care system every year.