Combating Government Vendor Fraud

WHITE PAPER

"The advent of technology has substantially increased the government's ability to detect and combat procurement and vendor fraud."

CARL R. KNUDSON, CFE
Forensic Accountant
Knudson and Associates

Vendor fraud by government contractors has been a significant problem for years, due in large part to the difficulty in identifying troublesome vendors prior to awarding multi-million dollar contracts. Furthermore, the very nature of government auditing programs is not a real-time process, but lags by months or years, which allows fraudsters a significant head start on crafting their schemes.

The Department of Defense's report to Congress on contracting fraud dated January 2011 detailed hundreds of billions of dollars in criminal fines and civil sanctions against our country's defense industry contractors. According to government analysts, government fraud, waste and abuse may be as high as 5% of our nation's GDP.

However, the advent of technology has substantially increased the government's ability to detect and combat procurement and vendor fraud, false claims, and Medicare/Medicaid fraud through Web-based search engines that can query real-time data to ferret out obscure (but important) relationships on targeted information. Web-based search engines are equally important whether you are conducting a due diligence investigation on new vendors, or beginning a full-fledged investigation into possible fraud by a current vendor.

The two pillars of an effective fraud program relate to prevention and detection strategies.

PREVENTATIVE STRATEGIES

As the idiom indicates, "An ounce of prevention is worth a pound of cure."

Situation + Opportunity = Trouble

Chronic criminal predators who have a history of malfeasance are the biggest threat to government-sponsored programs. Fraudsters have perfected the art of staying one step ahead of government scrutiny and are adept at using front companies to shield the identity of the actual operators. Historically, government auditing programs happen after the awarding of a contract, which allows the fraudster a significant head start.

Therefore, one of the most effective preventative strategies is conducting a due diligence investigation of all new government service providers. The simplest and most cost-efficient method for conducting due diligence is by searching historical data such as:

- Person and business data for criminal and civil records
- Non-profit and/or purported minority-owned businesses gaining favorable status with government contracts
- Connections between individuals/vendors and other business entities that have been linked to past fraudulent activity

THOMSON REUTERS™

- Social media and news searches to uncover hits on publicized criminal activity and civil litigation

In addition to searching historical data on business entities or individuals, a preventative strategy should also look to detect:

- Business fronts that pose for companies with conflicts between company executives and government agencies
- Validity of high-risk addresses and business locations. Real-time geographic data can now be used to perform this investigative task right from your desktop. This is especially useful in cutting investigative costs by minimizing costly field trips by management or investigators.

Advanced solutions and public records databases provided by private companies offer these resources and analytic capabilities in powerful Web-based investigation tools. For the first time, you can search across all relevant data sources with the click of a button.

FRAUD PROFILE & RED FLAGS

The key in detecting fraud is knowing what to look for. Staying up to date on the typical profile and schemes of a fraudster is a way to help level the playing field.

The Association of Certified Fraud Examiners profile data on fraud schemes shows that the individual is most commonly:

- Older (30+ years)
- Male (75%)
- Has a stable family situation that adds to the mystique of invulnerability
- Has above-average education – white-collar, not blue-collar
- Less likely to have criminal record
- In good psychological health
- Has attained a position of trust and inapproachability
- Has a knowledge of accounting and reporting systems and their weaknesses, which allows them to cover a paper trail

In addition, there are a number of situational and opportunity red flags for vendors that your employees should be trained to identify and confront.

The first and perhaps most obvious example is business owners or associates who live far beyond their means. The challenging part is proving their correlation to fraudulent behavior. A technique that has proved to be successful to identify individuals with high personal debt is searching for liens that have been filed by debt collectors.

These criminals also use clever means to establish business fronts posing for companies that receive tax break incentives from the government in the form of non-profit, minority, or women-owned businesses. These fronts are used to mask the true identity of their company. This also comes into play among companies that may be on a government debarment list, or possibly have a history of fraudulent behavior.

These instances provide great examples where a small investment on the front end in the form of a public records investigative tool could have easily uncovered these masked identities or past malfeasance, and saved a great deal of money on the back end.

DEFENSIVE STRATEGIES

Defining the battlefield

The first step of every post-fraud investigation should begin with gaining the proper intelligence to define the battlefield. Advances in vendor solutions have made it relatively easy for government agencies to gain access to public records data which provide the backbone or infrastructure of the investigation.

The ideal solution allows you to search public data on both businesses and individuals, and a select few provide the analytic capabilities to make connections between them.

By gaining access to this data, you can search information on the alleged individual and their associates to uncover the following information:

- Addresses, real property, assets, etc.
- Phone numbers
- Criminal and civil records

Searching by full Social Security number is another great way to gain additional insight into an individual and also gain a historical perspective to identify possible tax liens against individuals.

Playing catch-up

The defensive strategy is really playing catch-up after the horse has left the barn. More than ever, criminals are becoming highly elusive. Their ability to rapidly change jurisdictions, and take their schemes from one state to another makes tracking them extremely difficult. But nonetheless, once the fraud has occurred, it's a classic game of cat and mouse to be able to track and locate these individuals. There are, however, some relatively simple investigative strategies that can prove effective for finding cracks in their schemes.

Historical data shows that people who commit fraud continuously change locations, searching for new hunting ground. This usually means replicating their fraud scheme by changing their business name and setting up shop in a new state. This is where cross-jurisdictional searching becomes highly effective. In the past, fraudsters have successfully moved their schemes from state to state and a simple news search could have revealed their past activity or convictions in another jurisdiction.

Connecting a company's family tree is another way to uncover leads when tracking these individuals. In the case where business names are changed or fronts are created, one factor typically remains consistent and that's the individuals behind the operations. Creating a graphical analysis of links between the business owners, their entities and known associates creates a matrix for uncovering leads on these elusive criminals.

Finally, Web analytic capabilities that are now included in some investigative tools have revolutionized Internet searching. Instead of searching individual sites, deep Web crawlers within these tools have the ability to retrieve information on an individual or business in a single search from social media sites, news clippings, blogs, and more. This capability can be a hidden asset in your investigation toolbox to help uncover tracks that fraudsters may be completely unaware they are leaving.

"Web analytic capabilities that are now included in some investigative tools have revolutionized Internet searching."

CARL R. KNUDSON, CFE
Forensic Accountant
Knudson and Associates

CONCLUSION

With the rapidly changing landscape of vendor fraud and the highly elusive nature of these criminals, it is more important than ever for government agencies to adopt effective strategies for combating vendor fraud and saving millions, if not billions, of taxpayer dollars. Staying current on what to watch for and understanding the resources available are foundational building blocks for creating these strategies. Furthermore, advancements in technology and the sophistication of investigative tools have increased the efficiency of government officials to effectively level the playing field.

ABOUT THE AUTHOR

Carl R. Knudson, CFE, PI, Owner/Operator, Knudson and Associates, Thousand Oaks, CA

Mr. Knudson has over 40 years of fraud investigative experience at the highest level of government and the private sector.

Mr. Knudson has been a PI and CFE since 1995. Mr. Knudson worked in the Office of Naval Intelligence and Central Intelligence Agency prior to his 23-year career as an IRS special agent in the Criminal Investigation Division. As an IRS special agent, Mr. Knudson investigated complex white-collar crime cases, including tax evasion, money laundering, drug traffickers, and organized crime syndicates. Some of Mr. Knudson's drug trafficking cases were chronicled in the books *Washed in Gold* and *Dark Alliance*.

Upon retiring from the IRS, Mr. Knudson was hired as a Director in the Dispute Analysis and Investigative practice at Price Waterhouse. As a Director at PW, Mr. Knudson led several international fraud investigations involving overbilling schemes perpetrated against a large computer manufacturing company. Mr. Knudson subsequently was hired as a Director at KPMG where he led several large fraud investigations involving internal embezzlement schemes.

Mr. Knudson started his own business in November of 2000 and has specialized in forensic accounting and fraud investigations for his private and government clients. During this time, Mr. Knudson has testified as a Certified Fraud Examiner expert in more than 50 federal and state court proceedings and trials.