Procurement predicament

'Veils of trust' hinder detection

January/February 2017

By **Tom Caulfield, CFE; Sheryl Steckler, CIG**

This aerospace case history illustrates how fraudsters are able to easily commit procurement fraud because they can hide behind "veils of trust" they have with organizations' employees and victims. Here's how to thrust back the curtains and let the light shine in on cozy arrangements.

Let's set the procurement predicament stage by introducing you to the employees of an actual California aerospace company, which we'll call GotoAero. They work within the company's building maintenance department and are responsible for ensuring the company's research and development (R&D) buildings are maintained within optimum environmental conditions. Their duties include monitoring building vibration levels, moisture changes, temperature consistencies and dust collection. External vendors, which the aerospace employees select and oversee, perform much of the specialized environmental maintenance work.

GotoAero has pre-negotiated purchasing agreements with five local vendors, and their employees have the option of selecting any one of these vendors for work. The company policy

requires no less than three quotes (no matter the need) from the five vendors, and the aerospace employees are required to select the lowest bidder. The GotoAero policy also allows its employees to make these selections as long as the individual work orders don't exceed the established $35,000 threshold.

For the first year, GotoAero's employees followed the documented process of selecting the lowest bidder from no less than three authorized vendors. However, one by one they began accepting low-dollar gifts such as college basketball tickets and electronic gadgets in exchange for placing work orders solely through one of the five approved vendors, which we'll name BuildNow Pro Construction just for this article. Within six months, one greedy employee formulated a fraud scheme with the vice president of BuildNow to unnecessarily increase BuildNow's cost as much as $20,000 on multiple work orders in exchange for more expensive gifts, which had become (what we call) bribes.

The fraud scheme was working so well that the greedy employee and BuildNow's vice president (with consent of BuildNow's owner) put together a more structured arrangement. The pair devised a scheme in which the employee would receive a cash payment equal to 5 percent of the total amount of any work order the employee placed with BuildNow, and in return BuildNow would inflate its cost an additional 9 percent over what it originally had negotiated with GotoAero — 5 percent for the employee and 4 percent for BuildNow.

The scheme went forward, and within two weeks the employee placed eight separate work orders totaling more than $280,000. In exchange for placing these orders, BuildNow paid the employee $12,800. However, the employee complained that BuildNow owed him $14,000 based upon the agreed rate of 5 percent. The upset employee still continued the arrangement because something was better than nothing. The point to remember is that fraudsters often will cheat each other. (Variation of the platitude, "No honor among thieves.")

Several other GotoAero employees — not to be outdone — also kicked up their requests for more bribes. A government forensic auditor later determined during a criminal investigation that the vendor paid approximately $400,000 in bribes, and in return the GotoAero employees allowed the vendor to inflate federal government contracts by $3.2 million.

Unbeknown to the GotoAero employees, the buildings they were maintaining were exclusively supporting federal government R&D contracts. Therefore, GotoAero passed all costs related to maintaining the buildings to the U.S. government as indirect costs. The employees also didn't realize that because the company passed the costs to the federal government any allegation of fraud related to the building's cost would be within the jurisdiction of federal law enforcement.

Tip off and outcome

As part of the government's conditions for employment to work inside GotoAero R&D buildings, the government required each employee to maintain a security clearance. During a periodic update of one employee's clearance, the government background investigator noted in his report that "a vendor that the employee works with at his aerospace job had remodeled the employee's entire kitchen at no cost."

The background investigator shared his report with the Office of the Inspector General (OIG) of the National Reconnaissance Office (NRO) and the FBI. The OIG's and FBI's joint investigation revealed sufficient evidence to support multiple criminal convictions of acceptance of gratuities, bribes, kickbacks and false claims.

After a nearly two-year investigation, BuildNow Construction's owner, his vice president and seven GotoAero employees were convicted. The courts sentenced BuildNow's owner to 13 months confinement in a federal facility and a $1.3 million fine. BuildNow's vice president and GotoAero employees were fined a total of $800,000. One GotoAero employee was sentenced to six months federal confinement, and others received supervised probations. GotoAero fired all the employees and, of course, the government yanked its security clearances.

The investigation didn't end with just criminal convictions. The U.S. Department of Justice (DOJ) charged GotoAero, under the Civil False Claims Act, with failing to ensure sufficient oversight on payments to the federal government. The company pleaded guilty and agreed to a $2.2 million fine. Independent of the DOJ actions, GotoAero also agreed to submit to OIG investigative oversight of any new allegations of fraud against their employees working on federal contracts.

Hiding behind 'veils of trust'

Undeniably, the universal and most significant threats to achieving or maintaining honest, fair, impartial and legal contracting comes from the 40 plus traditional schemes of procurement fraud and the multitude of ways fraudsters can perform them.

As in our aerospace company case, fraudsters can perpetrate these schemes because they're viewed as "trusted" employees, managers or vendors who are deeply familiar with their companies' procurement processes and can easily manipulate them. Also, these "trusted agents" pull off most of these schemes behind "veils of trust" they have with organizations' victims. The trusted-agent status highlights the peculiar dichotomy of procurement fraud: These crimes can't succeed without trust but neither can organizations' everyday business.

The federal investigation found that GotoAero trusted its employees to follow its internal policy on receiving gifts. The investigation also determined the audit department had trusted the company employees to follow internal policy, which therefore guided the company's decision to not audit the maintenance department. The audit department's failure to audit was a major contributor to the DOJ's decision to charge GotoAero under the Civil False Claims Act.

Experience has shown us that a fraudsters' success is driven by their motivations, abilities to influence decision points within procurements and the effectiveness of entities' procurement integrity controls. (Procurement integrity controls are the processes, procedures and management systems designed to provide reasonable assurance regarding the prevention, detection, prompt reporting and response capability to procurement fraud and abuse.) Stronger procurement integrity controls equal better protection against fraud schemes.

Procurement fraud undermines public confidence

Procurement fraud — often driven by technology — has become increasingly more elaborate over the last decade and saddles the public and private sectors with higher costs to balance sheets and reputations. Fraudsters can now use high-end imaging capabilities to easily create authentic-looking invoices or work orders.

Most distressingly, procurement fraud undermines public confidence in organizational structures and their management. The U.S. federal government in 2014 alone spent more than $447 billion of tax dollars in federal contracts. (See the Annual Review of Government Contracting, 2015 edition, National Contract Management Association and Bloomberg Government.)

According to the 2016 *ACFE Report to the Nations on Occupational Fraud and Abuse*, the median loss for a single fraud in the U.S. and globally was $150,000 with 23.2 percent of the cases causing losses of $1 million or more. (See ACFE.com/RTTN, or page 4 of the report.)

If those losses don't catch your attention, then you can calculate the additional revenue an organization would need to generate to recover the stolen funds from a procurement fraud case. Let's say your organization finds a $150,000 fraud. If you had a 10 percent profit margin over the company's operating cost, you'd have to generate $1.5 million in new revenue to make up the difference.

In the aerospace case, the company would've had to generate an additional $22 million in revenue to offset the $2.2 million fine because they failed to have effective procurement integrity controls. And we're not even including the money the company had to spend to hire and train new employees plus the impact to the company's reputation as the employees' convictions made the local news.

True scope is elusive

One of the key challenges in developing a strategy to combat procurement fraud is obtaining reliable and granular information on how fraudsters deploy each scheme. Yes, we might understand the textbook description of each scheme, but because procurement fraud is an action of deception, the true scope of these schemes is normally elusive. Compounding the problem is that investigative data is rarely consolidated for comparison and analysis due to its minutia and its complexity. However, one source of reliable information comes from the efforts of the former National Procurement Fraud Task Force (NPFTF).

The U.S. Department of Justice Criminal Division began the task force (of which one of this article's authors, Tom Caulfield, was a member) in 2006. In November 2010, NPFTF became part of the Financial Fraud Enforcement Task Force — an interagency task force established to wage an aggressive, coordinated and proactive effort to investigate and prosecute financial crimes.

The NPFTF created a partnership with the U.S. attorneys' offices, the DOJ's Civil Division and more than 20 federal agencies including the FBI, the NRO OIG, the Defense Criminal Investigative Service and the Department of Homeland Security. The task force gathered case data on schemes, industries, perpetrators and damages. An analysis by PricewaterhouseCoppers

(PWC) of NPFTF's efforts reflected the majority of task force prosecutions from 2006 through 2010 involved: bribery (27.3 percent), bid rigging (20.8 percent), embezzlement (21.1 percent), false claims (16.3 percent), money laundering (7.1 percent) and others (7.4 percent). (See Figure 1 below and Cracking down: The facts about risks in the procurement cycle, PricewaterhouseCoopers.)

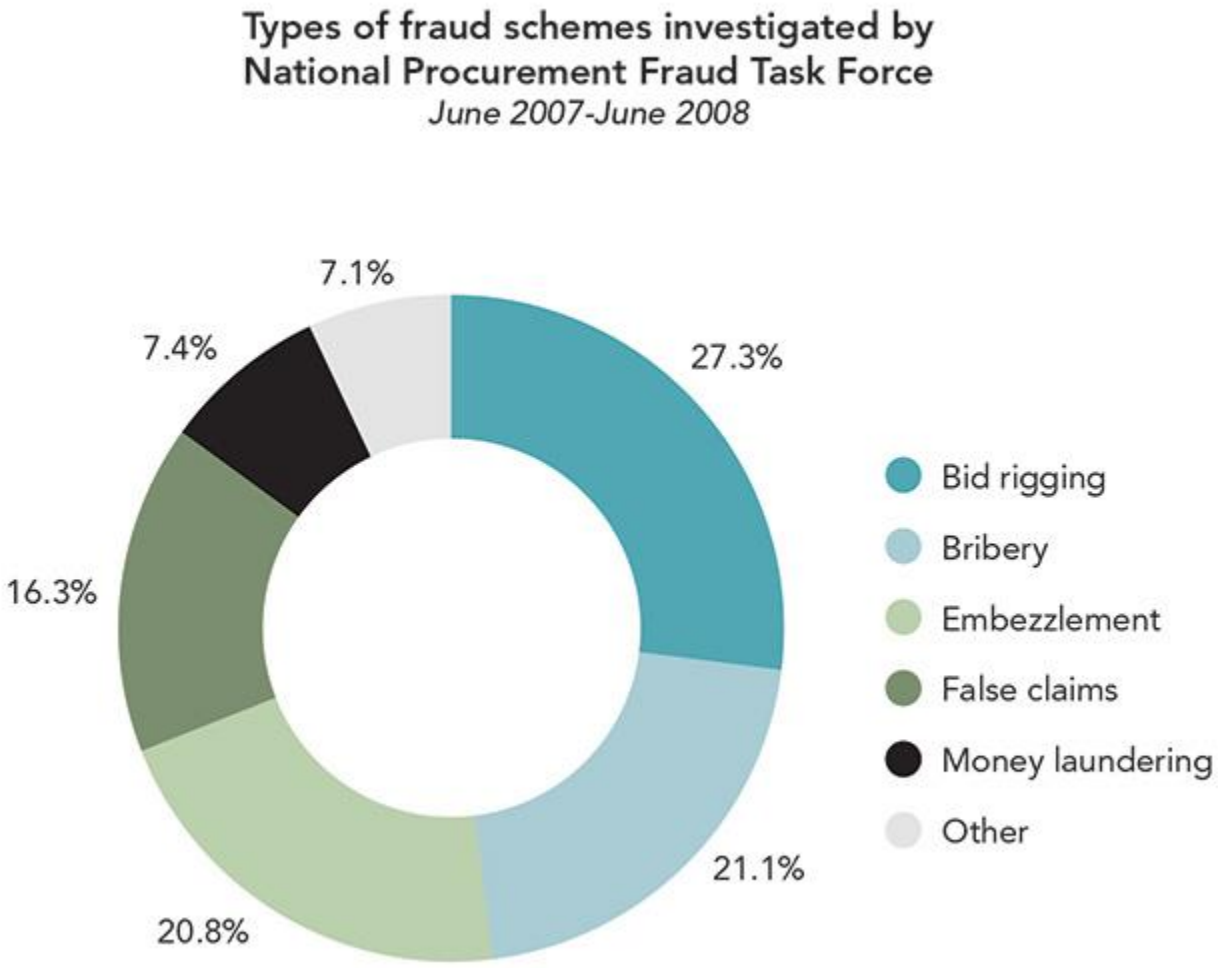

Figure 1: *From Cracking down: The facts about risks in the procurement cycle, PricewaterhouseCoopers.*

The task force prosecuted these types of defendants: vendor companies (35.3 percent), vendor employees (20.2 percent), private companies (4.5 percent), private individuals (8.1 percent), and public servants (31.9 percent). (See Figure 2 below.)

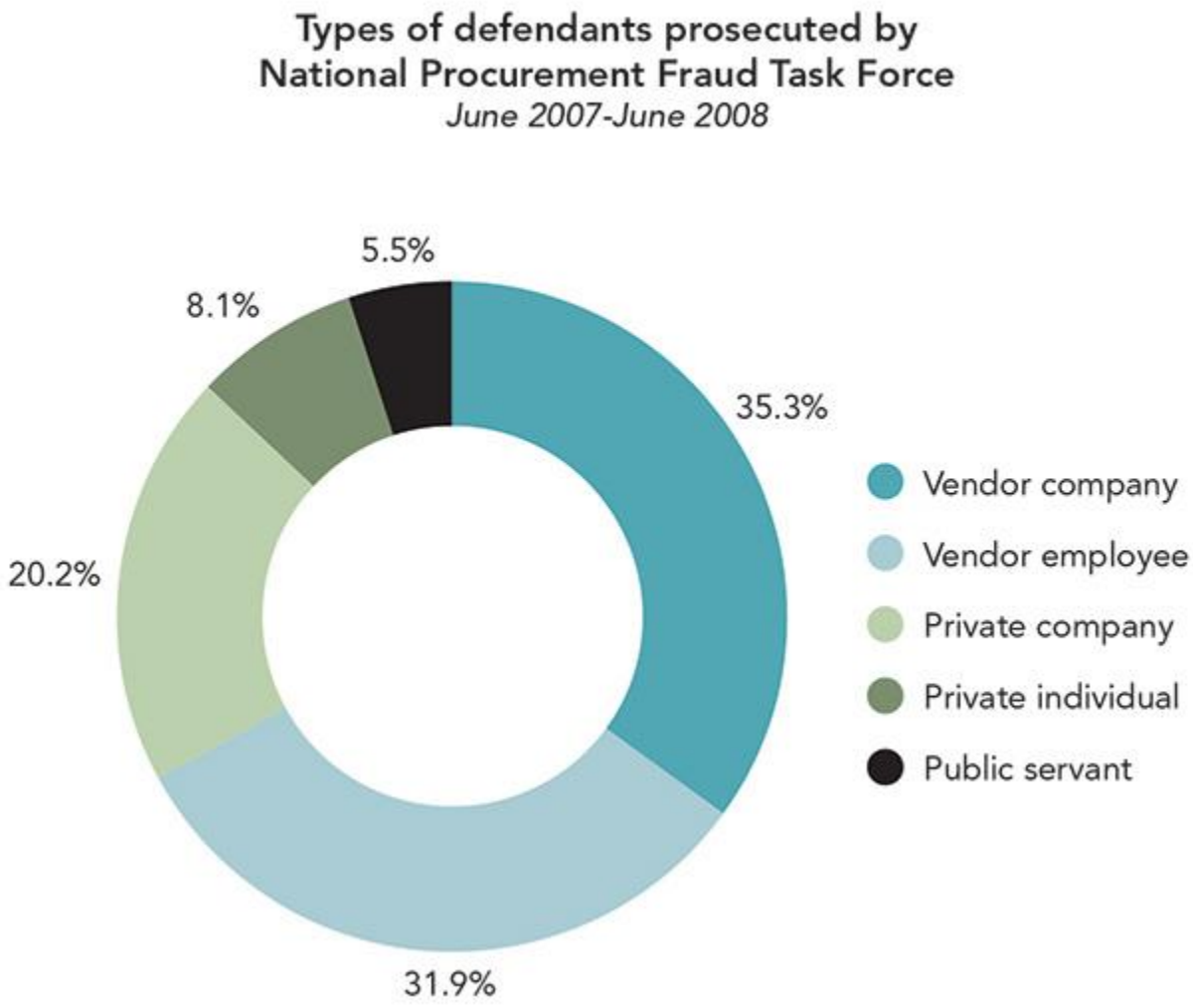

Figure 2: *From [Cracking down: The facts about risks in the procurement cycle](), PricewaterhouseCoopers.*

PWC also reported in "Cracking down" that the following views toward procurement risk are, in fact, misperceptions:

- Procurement risk in the U.S. mainly affects defense contractors.
- Procurement risk is a peripheral issue for corporations with codes of ethics and ethics hotlines.
- Compliance with the internal controls provisions of the U.S. Sarbanes-Oxley Act eliminates procurement risk.
- Procurement risk and corruption are limited to the developing world.

Experience has shown the authors that the search for procurement fraud can be difficult because it first appears to just be on the surface and generally leaves only faint clues and fraud indicators. Employees often dismiss valid fraud indicators as administrative oversights in documentation, or they don't place validity in what they think they overheard. For these reasons, annual training on procurement fraud indicators and what and how to report any concerns are an important part to prevent fraudulent activities.

Also, many program- and division-level managers view any hint of fraud in their sections as either negatively impacting their careers or future funding. Therefore, they continuously minimize any suggestion that fraud might exist. We're not suggesting these managers are deliberately covering up fraud; they're simply rationalizing away what they're observing. Recall the old Edmund Burke quote, "The only thing necessary for the triumph of evil is for good men to do nothing." Or, in our scenario, "The only thing necessary for the triumph of procurement fraud is for good people to report nothing."

Unlike financial statement and accounting fraud, procurement fraud seems to be slightly less likely to be driven by senior management, and it's more likely to be found in companies that are more geographically remote. Organizations are most vulnerable when their divisions, operations and processes are decentralized and lack consistent and ongoing communication of the ethical "tone at the top."

Subtle procurement fraud

Back to our case — early in the investigation, GotoAero was subpoenaed to provide an Excel spreadsheet of all vendor activity in a five-year period designated by the DOJ for the five pre-approved vendors. Within one hour of reviewing the spreadsheet, the investigators identified that nine (41 percent) of the 22 maintenance department employees had selected only the vendor involved in the fraud. (As we wrote earlier, seven were convicted; two retired three years prior to the investigation and subsequently weren't included in the investigation, and one had died before the investigation commenced.)

The DOJ used the ease of this investigative search to demonstrate and eventually convince the company to settle out of court and pay the $2.2 million fine. A review of the subpoenaed records also showed that most likely the employees began committing this fraud before the five-year evidentiary collection period.

Unlike crimes against persons and property that are apparent (assault, murder, vandalism, etc.), procurement fraud schemes are much more subtle. Also, during most crimes against a person or property, the criminal act is clearly understood from the beginning, and the major investigative question is to identify the person who committed the crime. However, in procurement fraud, often the fraud examiner knows the alleged fraudster; the investigative question is whether the fraudster's actions' violate any laws.

It's important to note that often the fraud indicators that precipitated the initiation of a procurement fraud examination lead to totally different fraud schemes. For example, split work orders could be an indicator of a program manager circumventing higher-level review within the

procurement process so he can expedite a contract action from taking too long. However, it could also be that the program manager split the work order to mask his decision to not compete for a contract award after he accepted a bribe.

He devised the scheme to circumvent the organization's requirement for full and open competition by splitting work orders to stay below the contract dollar thresholds. Many companies establish policies that require work orders above a dollar value to be competitively awarded, which would have a greater degree of oversight. Only after an investigation of the fraud indicator would the true motivation for the split work orders be revealed.

Let the light shine in

Organizations must accept material risk of fraud within their procurement processes. Failing to recognize this risk exposes them to the full range and deceptive actions of fraudsters and the consequences, which could include potential debarment, contract termination, financial losses, public mistrust, reputation degradation, and criminal and civil penalties. Dare to thrust open the veils of (mis)trust to let in cleansing sunlight.

***Tom Caulfield, CFE**, is chief operating officer and co-owner of Procurement Integrity Consulting Services, LLC (procurement-integrity.net). He's an instructor for the ACFE's Contract and Procurement Fraud seminar. His email address is: Tom@procurement-integrity.net.*

***Sheryl Steckler, CIG**, is president and co-owner of Procurement Integrity Consulting Services, LLC. Her email address is: Sheryl@procurement-integrity.net.*