PREVENT PROCUREMENT ‘LEAKAGES’ AND SAVE PRECIOUS WORKING CAPITAL

Given the current economic climate and regulatory expectations, monitoring procurement spending for fraud, waste and abuse (aka “leakage”) is even more important. We can proactively monitor procurement data via big data analytics, which will reveal transactions that are fraudulent or diminish working capital.

Chief financial officers (CFO) are always looking for opportunities to optimize working capital and plough it back into their businesses. (Working capital is the money a business uses in its daily operations. It’s calculated as current assets minus current liabilities.)

Let’s say your CFO uses a fraud risk management program to save your organization 1% to 5% of total procurement spending by finding improper expenditures. If your organization invests a fraction of this savings it will increase its bottom line.

So, if your annual procurement spending was $50 million, you could retrieve $500,000 to $2.5 million in recoveries or cost savings with minimal personnel and financial investment. Would you do it? I’m sure your answer is an unequivocal yes.

The timing has never been better to implement monitoring mechanisms to forensically mine procurement data for potential irregularities. Improved compliance and anti-fraud monitoring technologies use advanced data analytics, automation and intelligent risk-scoring techniques. Organizations can now deploy comprehensive spending analytics cheaper and faster than traditional tools or controls.

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
MANAGING DIRECTOR, ALVAREZ & MARSAL’S DISPUTES AND INVESTIGATIONS PRACTICE

THE TIMING HAS NEVER BEEN BETTER TO IMPLEMENT MONITORING MECHANISMS TO FORENSICALLY MINE PROCUREMENT DATA FOR POTENTIAL IRREGULARITIES.

Analytics help break silos and holistically view fraud risks

Organizations must thoroughly understand the interrelated activities within their procurement processes, such as vendor due diligence, contract terms, purchase orders, invoices, receipt of goods and payment activities to effectively combat procurement fraud and coalesce several skill sets to design fraud control processes.

Too often, we see compliance or investigations operating separately and independently from procurement, finance or even internal audit. Departments don’t have insight into what their colleagues are pursuing, which can lead to duplication of efforts and data “silos” of potentially incomplete information.

A chief compliance officer (CCO) needs to amalgamate expertise from manufacturing, procurement, accounting, investigation and legal departments when they design a fraud risk management process. Organizations also must use data science and anti-fraud expertise to combine these skills in designing risk algorithms that help prevent and detect payment irregularities. As anti-fraud professionals, we often can bring these teams together to design preventive solutions.

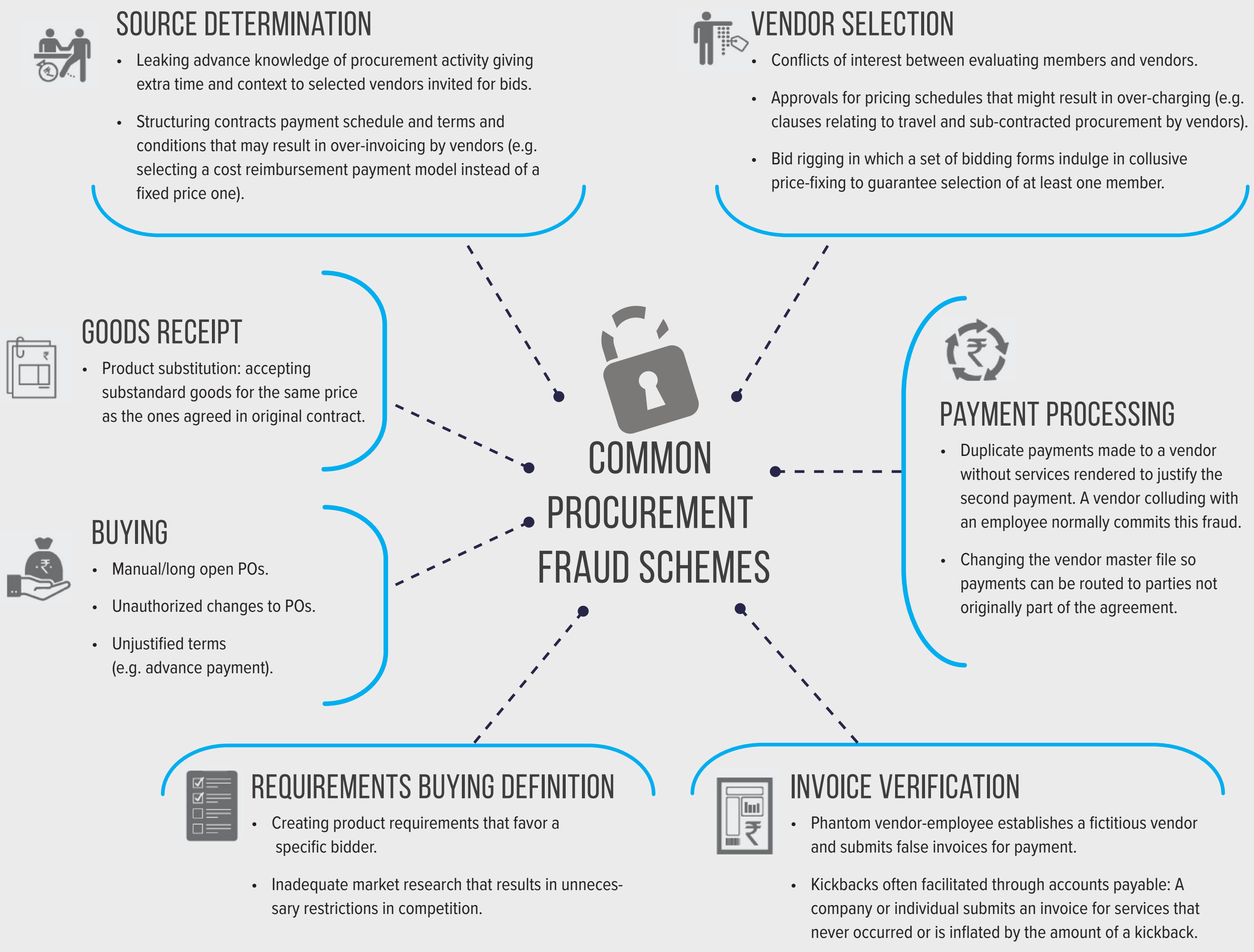
The Institute of Internal Auditors (IIA) recently highlighted dismantling work silos so business functions could better collaborate in its “Three Lines Model,” a July 20 update to its widely accepted “Three Lines of Defense.” (See tinyurl.com/y46z8bkd.)

The IIA model suggests that among all risk management roles of the organization, "The governing body, management, and internal audit have their distinct responsibilities, but all activities need to be aligned with the objectives of the organization. The basis for successful coherence is regular and effective coordination, collaboration, and communication."

In my March/April 2020 column, "Avoiding the DOJ's Red Flags of Collusion," I explored the efforts of the U.S. Department of Justice's recently formed Procurement and Collusion Strike Force. (See tinyurl.com/y6omg5hm.) In this column, I'll focus more on potentially improper payments, which can include conflicts of interests, high-risk or shell companies, bribes and kickbacks, fraudulent payments processing and material pricing frauds, among many others.

Some of my preferred procurement leakage analytics

My friend, David Coderre, wrote one of my favorite reference books, the 2009 "Computer-Aided Fraud Prevention and Detection," that still helps ignite my passion for anti-fraud analytics. In



SOURCE DETERMINATION

- Leaking advance knowledge of procurement activity giving extra time and context to selected vendors invited for bids.
- Structuring contracts payment schedule and terms and conditions that may result in over-invoicing by vendors (e.g. selecting a cost reimbursement payment model instead of a fixed price one).

VENDOR SELECTION

- Conflicts of interest between evaluating members and vendors.
- Approvals for pricing schedules that might result in over-charging (e.g. clauses relating to travel and sub-contracted procurement by vendors).
- Bid rigging in which a set of bidding forms indulge in collusive price-fixing to guarantee selection of at least one member.

GOODS RECEIPT

- Product substitution: accepting substandard goods for the same price as the ones agreed in original contract.

COMMON PROCUREMENT FRAUD SCHEMES

PAYMENT PROCESSING

- Duplicate payments made to a vendor without services rendered to justify the second payment. A vendor colluding with an employee normally commits this fraud.
- Changing the vendor master file so payments can be routed to parties not originally part of the agreement.

BUYING

- Manual/long open POs.
- Unauthorized changes to POs.
- Unjustified terms (e.g. advance payment).

REQUIREMENTS BUYING DEFINITION

- Creating product requirements that favor a specific bidder.
- Inadequate market research that results in unnecessary restrictions in competition.

INVOICE VERIFICATION

- Phantom vendor-employee establishes a fictitious vendor and submits false invoices for payment.
- Kickbacks often facilitated through accounts payable: A company or individual submits an invoice for services that never occurred or is inflated by the amount of a kickback.

Interrelated activities in the procurement-to-pay process and fraud schemes at each stage the appendix, Coderre lists hundreds of rules-based tests that fraud examiners can deploy on procurement spending. In collaboration with the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, the ACFE also maintains an online library of sample analytics, divided by fraud scheme, at ACFE.com/fraudrisktools. I contributed to the development of this library.

Just like enthusiasts collect baseball cards or rare coins, I've been creating a library of anti-fraud tests gathered from my investigative experiences and networking with fellow fraud fighters at ACFE conferences or at client locations. Here are some of my favorite procurement fraud risk tests for discovering various fraud schemes, many of which are in the procurement-to-pay (P2P) cycle. (See the figure on page 13.)

Cash disbursements

- Find duplicative payments as evidenced by exact match in invoice number, invoice date, purchase order/reference, amount — among many other duplicate combinations.
- Analyze weekend and holiday payments.
- Search payment dates prior to invoice or purchase-order dates.
- Find payments approved by the same person who created the payment.
- Look for invoiced vendor information not matching purchase-order information.

Vendor management and fake vendor schemes

- Identify duplicate vendor numbers or names in the master vendor file.
- Ascertain dormant vendors who've had, for example, no activity for more than a year but suddenly receive payments.
- Discover vendors with missing or incomplete information such as tax IDs, website addresses and phone numbers.
- Review vendor due diligence questionnaires for suspicious language, or conduct adverse media or watchlist scans on high-risk vendors.

Conflicts of interest

- Identify database linkages between the employee and vendor master — addresses, phone numbers (including spouse emergency contact numbers) and bank account information, among others.
- Check for unusual preference given to vendors, such as pricing or discounts, and then examine whether any of the employees hold any undisclosed interests in those vendors.

Bribery and kickback schemes

- Compare order quantity to optional reorder quantity.
- Check for any vendor with an irregular share of the business, and then check for any directorship or shareholding by any of the company employees with these vendors.
- Conduct text mining of payments for kickback-related terms such as "facilitation pay," "friend fee" and "help payment."
- Find excessive or frequent payments made to charities, luxury retailers (for expensive gifts) or miscellaneous journal-entry accounts.
- Identify payments made to state-owned entities or organizations with close relations to government entities.

Raw material pricing frauds

- Check for a supplier charging a different price for a similar "stock-keeping unit," or SKU.
- Examine suppliers' pricings at different purchase locations.
- Look for purchase-order prices that are different from contracted prices for the same materials.
- Check for different payment terms for the same suppliers.

Caution: These lists of anti-fraud tests are only representative and intended to spark ideas. It's important that you align your final list of tests with your organization's fraud risk assessment results and customize them to your specific industry, business and prevailing risk dynamics.

Use advanced data science to look for irregularities

Aim to have your analysis experts run all tests on an entire population of data to get maximum results. Don't apply individual tests or rules to procurement data in isolation because they won't provide your desired results or return on investment. Have them combine different tests to see what will be applicable to high-risk transactions.

Run all transactions through your testing algorithms. The analytics will apply each test on all the transactions and assign a risk score to each transaction depending on the number of transaction matches. "Many of these complex linkages and anti-fraud tests are now scripted and automated, with integrated machine learning. A 200- to 300-hour process now takes 20 to 30 hours to run," says Anil Kona, CEO of Spectrum Data Science Corporation.

Now, simply count up the risk scores to lead you to the riskiest transactions that might be potential improper payments.

It's amazing how efficient you can be when you sort tens of thousands of suppliers and you focus on the top five or 10 based on their payment activity.

Naturally, each high-risk payment is also linked to a vendor, which then allows you to also risk-rank your top vendors. It's amazing how efficient you can be when you sort tens of thousands of suppliers and you focus on the top five or 10 based on their payment activity.

Thankfully, advancements in automation and application of data science are helping compliance and anti-fraud teams achieve a five to 10 times return on procurement- spending investment in as little as three to four weeks.

Maximize your savings

A successful data analytics program on procurement spending has several moving parts. All of them need to be perfectly aligned to give the best results. Your chances of finding those cost savings of 1% to 5% on the overall procurement spend population will be maximized when you put these into practice:

- Dismantle functional silos to bring together skills and expertise from diverse sources to design the most optimum solution.
- Select the appropriate tests for procurement fraud risk identification in collaboration with all stakeholders in the P2P process.
- Combine the correct continuous-monitoring data automation, data integration and risk-scoring techniques.

Happy hunting! ■ FM

Vincent M. Walden, CFE, CPA, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice and assists companies with their anti-fraud, investigation and compliance monitoring programs. He welcomes your feedback. Contact Walden at vwalden@alvarezandmarsal.com. Walden thanks his colleague, Varun Mowar, who contributed to this article. Contact Mowar at vmowar@alvarezandmarsal.com.