DAI Global Conduct *Quarterly*

Issue 8
December 2018

"If you see something, say something." In every incident of fraud, conflicts of interest or bribery, someone takes the initiative to report their concerns. Taking personal responsibility to report is your duty as a DAI employee.

DAI recently conducted a review of significant incidents of fraud, sexual harassment and kickbacks to identify practices that must be strengthened. Many of the recommendations are reflected in the case study take-aways in this issue. We recognize that saying something when you see something can be difficult. To encourage you to report:

- DAI expects supervisors, COPs, Team Leaders and Home Office Managers to be receptive and respectful in listening to your concerns and the details of the allegation. They must also preserve the confidentiality in which the information is provided and your identity if you are concerned about vulnerability to retaliation outside the DAI workplace. They are also expected to pass allegations of ethical violations to the Team Leader, Chief of Party (their deputies) or directly to the ECO to assure a timely response.

- DAI has a strict non-retaliation policy. We recognize the concern employees have about possible retaliation outside of the workplace. DAI will protect your identity to insulate you from this vulnerability.

- Don't wait thinking that someone else may have reported the issue. Your perspective on the allegation will be important to the timely investigation and resolution of the matter.

- Raising the issue quickly will help prevent the problem from developing into something worse.

If you believe performance has been falsified, please reach out to: **Mike Walsh,** Chief Ethics & Compliance Officer (mike_walsh@dai.com, 301-771-7998) or **Jeremy Finch**, DAI Europe's Director of Internal Audit and Ethics & Compliance Officer (jeremy_finch@dai.com +44-7834-439974).

This document and additional materials can be found at: http://dai-global-conduct.com/integrity/preventing-fraud/

Procurement Fraud

Case Study 1

A review of bank reconciliations found irregularities in electronic payments made by the project. A project associate noticed multiple payments to a single bank account and contacted her supervisor and the Ethics & Compliance Officer. The associate was already suspicious because she recognized that the DCOP was able to approve requests, sign procurements and authorize payments.

Action taken:

A quick investigation revealed that the DCOP inflated the number of consultants needed from two to five with the names of fake individuals. He was also forging the COP's approval and funneling payments for the falsified consultants to his own bank account. A second manager confessed to colluding with the DCOP to inflate the number of consultants. Criminal charges have been lodged. The former employees will be debarred from working on any projects funded by the client.

What would be your concerns regarding inadequate separation of duties on a project? What can be done to limit the risk of procurement fraud under these circumstances?

Take-aways:

- Be alert to fraud indicators (e.g., signatures that appear duplicated by machine or forged and vulnerability to internal control weaknesses).
- Clear separation of duties is essential. Workload is not an excuse to limit controls or take short-cuts. Address internal control issues quickly.
- Quality of the relationships on the project and with the home office must support a comfort level in reporting concerns and allegations as well as enforcement of policies and procedures.
- Understand the consequence of committing fraud are firing, ruined reputation and criminal charges.

Case Study 2

The IT manager provided three quotes for a laptop as requested by the Director of the regional office. The Director found that two of the quotes had the same physical address in the footer. The third quote had no physical address. These irregularities were reported to the Ethics & Compliance Officer.

Action taken:

After a one-year investigation coordinated with the client, DAI found that a single vendor owned the three bidders who submitted the laptop and other fake bids for multiple solicitations on the project. Although there were several suspicious signs, the investigation by Internal Audit found no credible evidence linking the IT manager to this vendor. The vendor was debarred from DAI solicitations. In response to this action, the manager of the vendor visited DAI soon afterwards and alleged that the IT manager demanded "loans" (which he did not repay), cellphones, laptops and a TV in return for awarding non-competitive purchases and favoring the vendor in competitive procurements. The IT Manager resigned before these allegations could be investigated further.

What are the similarities between case study 1 and 2? What are your concerns and what could be done to limit the vulnerability to these concerns?

Take-aways:

- Be alert to fraud indicators (signatures, contact numbers and addresses, etc.).
- Limited competition increases vulnerability to fraud and collusion. Unrealistic delivery requirements (e.g., 10 days proposed but ultimately took 30 days to deliver) and expanded warranty offers (two years rather than one) were used to direct awards to the preferred vendor.
- Solicitations, subcontracts, grants and consulting agreements must include clear language on anti-kickbacks along with local contact information if money or anything of value is requested by a DAI employee.
- Spot-checks are essential, including unannounced visits to bidders and vendors.
- Management must effectively oversee procurements, including asking question about the reasonableness, value and monitoring of technically complex equipment and services.
- Understand the consequence of committing fraud are firing, ruined reputation and criminal charges.

Case Study 3

The Finance Director became suspicious of numerous small purchases of office and conference supplies over the last two years from Heavenly Enterprises, an online store with no website or physical address. A preliminary investigation found that the firm's business registration listed the procurement officer's cellphone number. When asked, the procurement officer offered no explanation.

Action taken:

The investigation also found on social media that the Heavenly owner was in a relationship with the sister of the procurement officer. Colleagues on the project also noted that he often gave the procurement officer a ride to work.

The client was notified immediately of the connection of the procurement officer to the vendor, and he was separated from the project. DAI's internal audit manager also investigated all transactions associated with the procurement officer on the current and previous projects he worked on.

What are the similarities between case study 2 and 3? What are your concerns and what could be done to limit the vulnerability to these concerns? Why didn't we learn of the issue sooner?

Take-aways:

- Be alert to fraud indicators (numerous non-competitive awards to a single vendor, bids with no addresses or phone numbers).
- Assure regular review of conflict of interest policies and disclosure of relationship forms.
- Conduct unannounced spot-checks by different staff, not just procurement, to verify bidders/vendors and their capacity.
- Understand the consequence of committing fraud are firing, ruined reputation and criminal charges.

Case study 4

The Procurement Manager became concerned when she returned from lunch and noticed that an e-mailed bid for IT equipment, addressed to the project's IT specialist and copied to her, had been deleted from her inbox. She later found the e-mail in her trash folder. She recalled that the IT specialist had requested access to her computer before she left for lunch, but she said no as she was on her way out. Then, when she came back from lunch, she found that she had been locked out of her computer. The IT specialist returned and was able to fix her access.

Action taken:

The Procurement Manager informed the COP who passed the information to the Ethics & Compliance Officer. The ECO engaged the Home Office IT office for assistance in investigating the details. Their analysis showed that the password for the Procurement Manager's laptop had been reset by the IT specialist before the Procurement Manager left for lunch. The IT specialist also gave himself access to all project files as a system administrator. DAI determined that the IT specialist colluded with the vendor. In this scheme, the vendor asked the IT specialist to replace their original bid with a second, lower bid. DAI took immediate action to sever the IT specialist's access to DAI systems, confiscated his laptop and separated him from the project.

What are your concerns in this case study? What can be done to address your concerns?

Take-aways:

- Be alert to fraud indicators – irregularities with emails and the handling of bids, proposals and applications.
- Be consistent in requiring all bids, awards and correspondence be sent and received through DAI email accounts.
- Clear and enforced separation of duties and responsibilities protects the integrity of the procurement process and the project's reputation for fairness and professionalism.
- Understand the consequences of committing fraud are firing, ruined reputation and criminal charges.

What happens when you report an allegation?

- The ethics hotline can assure your anonymity in reporting allegations. If you use the webpage at www.dai.ethicspoint.com, you can provide details, and the Ethics & Compliance Officer can follow-up with you through the website without the need to reveal your identity.
- All allegations are directed to the Ethics & Compliance Officer to determine the next steps. Depending on the nature of the allegation, the ECO may engage Home Office HR, Internal Audit, Contracts and/or General Counsel to conduct a preliminary investigation. Often there is a need to follow-up with the individual making the allegation to request more details to enable DAI to conduct a more effective investigation. If only broad allegations are received without details on when, what or even where a violation occurred, we will not be able to investigate.
- The ECO will quickly inform the client if there is concrete evidence of fraud, conflict of interest, bribery/kickback, sexual misconduct, human trafficking or data breach. The ECO will also coordinate next steps with the client.
- If the client wishes DAI to conduct the investigation, Internal Audit and HR are often involved. They are often able to conduct the investigation in a manner that can protect the anonymity of the individual making the allegation. If the client wishes to conduct the investigation, the ECO will coordinate with project and home office staff.
- All allegations received are tracked by the ECO through to closure. Regardless of who investigates the matter, the individual reporting the allegation will be informed of the outcome.