

## Helping to Prevent University Fraud

By Ron Schwartz  
Matthew Larson and  
Mary-Jo Kranacher





For a long time, universities have been viewed as bastions of high ethical standards where the fraudulent schemes common to the workaday world simply would be unthinkable. Increasingly, however, this is proving to be untrue. Instead, universities are as rife with scams as other organizations and as much in need of adopting strong anti-fraud policies and procedures.

The types of fraudulent schemes are legion. The perpetrators come from many levels of the university—from presidents, whose authority makes committing large fraud easy, to maintenance workers who might be tempted, as in a recent case, to switch the new tires on the college van with the old ones from his personal vehicle. Schemes tend to start small and can increase as they succeed.

Reasons for the particular vulnerability of universities to fraud tend to boil down to the late Donald Cressey's Fraud Triangle: the **incentives and pressures** to steal are strong, given relatively moderate salary levels and the reluctance of most universities to prosecute from fear that fundraising will be hurt by negative publicity; the **opportunities** are ample given the usual lack of segregation of duties due to ongoing budget cuts; and **rationalization** is easy in an environment with little comprehensive oversight where there is a perception that everyone

is doing it, especially those at the highest levels of the institution. "Basically anyone who has the incentive and opportunity to commit fraud, and believes they can get away with it, is likely doing it," says CPA and Certified Fraud Examiner, Mary-Jo Kranacher, a professor at York College, CUNY, who participated in a recent panel discussion with members of Deloitte Financial Advisory Services LLP ("Deloitte FAS"): Ron Schwartz, Principal in the Forensic & Dispute Services practice and Matthew Larson, Senior Manager in the Forensic & Dispute Services practice.

Uncovering fraud can be difficult because of the concealment efforts of the perpetrator. Fraud detection engagements are usually prompted by a tip. When investigating an allegation of fraud, a multi-pronged approach including 1) gathering and analyzing physical and electronic records to detect reporting anomalies; 2) interviewing employees—at all levels—who may have information about the fraud; and 3) reviewing e-mails for relevant information could prove to be crucial in helping detect fraud. Building a strong case can potentially help to illicit a confession from the perpetrator. Once a fraud scheme has been identified, stronger policies, procedures and controls should be designed and implemented to minimize the risk of future fraud.

Some of the key issues you may want to consider when putting together a plan to help reduce fraud in colleges and universities include:

1. **Tone at the top.** If the president and other high-level administrators turn a blind eye to fraud, so will everyone else.
2. **Clearly written policies and procedures.** These should be spelled out carefully and in writing so that employees are familiar with the university's code of conduct and the consequences for violating it. In addition, an ethics policy should be implemented and enforced.
3. **Training.** This is an important preventative. Employees are often surprised by what constitutes fraud since there can be grey areas. Round table discussions can help clarify these issues. Online courses can help stretch scarce resources effectively.
4. **Using an external whistleblower hotline.** Encourage employees to report potential problems by implementing a well-advertised hotline that provides anonymity to prevent retaliation by those in charge.
5. **Implement strong anti-fraud controls.** This step is just as essential for universities, as it is for other types of organizations.
6. **Enforcement as deterrent.** In the past, because universities feared the negative impact fraud could have on fundraising, the administrators often refrained from publicizing fraud and the actions taken against the perpetrator(s). However, keeping the problem quiet and allowing the perpetrator(s) to quietly resign did little to discourage future wrongdoing.
7. **Paying attention to small transgressions.** Since fraud generally starts small and can grow over time, addressing even the smallest transgression is instrumental in preventing future scandals.
8. **Prevention first.** Once fraud has been committed and the university's money is spent, it is difficult to recoup the losses. It is far better to keep theft from happening in the first place.

Keeping these factors in mind when confronting fraud at your university can help enhance deterrence and prevent future problems.

How and why is fraud committed at universities and what can be done to prevent it?

## 1. Common Fraud schemes:

Common fraud schemes at universities include misuse of procurement cards (“p-cards”), padding expense accounts, listing fictitious vendors, rigging vendor bids, taking kickbacks and abusing payroll and overtime by fraudulent reporting of work hours.

P-cards particularly lend themselves to abuse since, without tight oversight, employees have carte blanche to charge whatever they want to the university. “We have investigated employees who use the cards to make personal purchases at the hardware store; take trips for personal reasons, but disguise them as business trips; and even one employee who leased a car for personal use when her car broke down for two-to-three months,” says Schwartz, who is a specialist in financial-analysis modeling and internal-control consulting. “Investigations of p-cards can lead to finding more grievous instances of fraud.”

Other schemes can involve paying family members from the university’s payroll account. In one case, a Deloitte FAS team uncovered approximately \$500,000 in fraudulent charges over the time span of a couple of years for transcription services that been paid to a relative of an employee who was approving the invoices.

In another instance, an employee was selling university computer assets on eBay and “pocketing” the proceeds. He was caught when a Deloitte FAS team did a search of employee internet usage patterns looking for frequent visits to work-inappropriate sites.

Collusion between employees can help to perpetrate and conceal a fraud. In a recent Deloitte investigation, in concert with a colleague from accounting, a university employee in human resources set up his relatives, who were not employed by the university, as “ghost employees” on the payroll. This allowed university assets to be misappropriated through payroll money going to people who provided no services to the school and to the insiders who were the architects of the scheme.

Another common fraud scheme is overtime abuse. Employees can manipulate the system and get paid for tens of thousands of hours that were not worked. Testing time systems for anomalies can make this kind of fraud apparent, although sometimes clever fraudsters record their overtime over numerous departments and reporting centers so that the abuse is harder to detect.

## 2. Why fraud occurs:

Specific environmental factors that can contribute to fraud at universities include: silo-ed reporting structures with multiple schools, departments, and programs running independently; budget cuts that affect the segregation of duties for effective internal controls; long tenures contributing to abuse of trust; a liberal control environment and resistance to controls; the lack of written policies and procedures; nepotism; and a lack of financial acumen by the university staff.

Starting at the top, administrators are in a position to override controls. They can authorize payment of a bill that may have been incurred for personal purposes and the people who work below them are reticent to challenge them on paying it without the proper documentation because of fear of retribution or retaliation. “You can have phenomenal controls, but they won’t work if someone overrides them,” says Schwartz.

Often, lax controls enable misuse of funds or concealment of a fraud, as is sometimes the case with grants at research institutions or with operations of college-related entities—such as foundations, auxiliary enterprises (e.g. parking lot, cafeteria) and student associations.

One way this might occur is if an individual with access to the electronic files changes the financial data, after they have committed the fraud, to eliminate the paper trail.

Insufficient staff can also lead to problems when overwhelmed supervisors rubber stamp authorizations or the same person has the power to authorize and execute transactions. Segregation of duties is a basic control in the fight against fraud.

## 3. What to do about fraud:

Discovering fraudulent schemes at universities, as elsewhere, can be like searching for a needle in a haystack. The Deloitte FAS team generally takes the following approach:

- Forensic accountants interview key personnel, irrespective of their level.
- AFT personnel use technology to harvest and analyze the digital evidence.
- After Deloitte FAS has finished its fraud investigation, the next step is to work closely with Enterprise Risk Services (“ERS”) personnel of Deloitte & Touche LLP who can help manage, design, and implement new controls.

## Interviews

It is important to interview people at all levels. This can be especially useful when trying to detect deception at the top. Blunt questions, such as whether an employee has been asked to override controls or book transactions without appropriate supporting documentation, should be asked. Employees should also be asked if they have any concerns about the integrity of management or the relationship of employees with vendors or suppliers or other employees.

Special attention should also be given to the interviewee's reaction to these pointed questions, not just to the verbal responses, but also to the body language. "We have had a lot of success obtaining valuable information by conducting interviews as part of our forensic engagements in helping to identify the perpetrator," says Schwartz.

Kranacher agrees. "It is people who commit fraud, not computers or books. There is usually somebody else who knows about it. Many people are afraid to come forward and volunteer information, but if you go to them and ask them the questions, they may answer honestly," she notes.

## Gathering and analyzing the evidence

Interviewers must work together with those gathering and analyzing the evidence, so that the results from one line of inquiry can be used to fuel the other to build a solid case.

Forensic accountants search the data—whether hard copy or electronic—gathered through emails or computer systems. Often, anomaly testing will reveal red flags that bear further scrutiny. Recurrent patterns can be another tip off.

Technology is an integral tool that assists forensic specialists in looking for fraud. It offers a cost-effective and efficient way to work through thousands, and potentially millions, of records. Since each scheme, from p-cards to overtime abuse, involves its own data sets, forensic professionals can build rules and procedures for a specific scheme to identify anomalies.

"It is an iterative process," says Larson, who has worked on more than 300 computers in the search for fraud. Initially data that is harvested is analyzed and then used in interviews. Then, information obtained from interviews may prompt going back to the computer data and more relevant data may be identified, which then helps interviewers ask more well-honed questions. "So not only

does technology help the forensic professionals get through large volumes of data quickly, but it also helps pinpoint some of the specific areas of fraud,” he says.

Generally, running anomaly detection tools for criteria such as employees sharing the same bank account numbers or addresses, or vendors and employees sharing the same bank account numbers or addresses, can provide important information. Timing of expenditures can also offer clues. E-mails are searched for signs that controls are being circumvented. Deleted files can be another “smoking gun.” Carefully comparing records on back-up files with later records or different versions of emails on various electronic devices, such as PDAs and computers, can really help a forensic engagement.

Running keywords related to the suspected fraud can also help to efficiently detect fraudulent behavior. Keywords can range from simple words to complex expressions and can be tailored to suit the investigation. Boolean operators such as ‘and’, ‘or’ and ‘not’ can help target the resulting population.

## **Designing and implementing controls**

Once fraud is discovered, strong controls should be designed and implemented to prevent it from happening again. “If people know that there is a robust anti-fraud control program at the university, including anomaly detection, they will think twice before perpetrating a fraud,” says Schwartz.

Top administrators can set the tone within the institution by leading by example and establishing a strong culture of compliance. Open lines of communication—among the internal and external auditors and the staff—can also help to reduce fraud.

Implementing training programs at all levels of the organization can help reinforce the message that the university has a zero tolerance policy as it relates to fraud. A combination of in-person and online education is usually effective. As Kranacher notes, often employees do not realize they are doing anything wrong, as was the case recently, when a professor was caught selling review copies of books that he received for free from a publisher, to his students at a “discount” from the retail price.

Whistleblower hotlines that are run by third parties can also help employees to report wrongdoing. Effective hotlines should be anonymous to reduce the risk of retribution. Moreover, there must be both the reality and perception that something will be done about the allegation. The hotline should be open to employees, vendors and suppliers alike.

Periodic analysis of the data to detect anomalies is an easy way to uncover certain frauds, such as employees submitting the same expense twice via p-card and expense account, and can also serve as a deterrent.

## Conclusion

Scarce resources and a culture of lax controls can make any organization, including universities, vulnerable to fraud. Whether overstating overtime or misusing p-cards, fraud schemes to misappropriate university funds abound.

Investigating allegations of fraud, through rigorous data gathering and analysis and by interviewing employees at all levels, is crucial in the fight against fraud. These efforts should be followed up by implementing robust controls and enforcing established penalties for violators.

Universities should not shy away from prosecuting those who commit fraud. If there is no punishment for the crime, it sends a message that it is acceptable to steal from the university, and many employees will continue to take their chances. Our universities, especially those supported by taxpayer dollars, deserve better.

## University Fraud Bios

### Ron Schwartz

Mr. Schwartz is a principal at Deloitte Financial Advisory Services LLP. He has provided forensic and dispute services, including expert witness testimony, for clients in the not-for-profit and higher education sectors as well as manufacturing, healthcare, real estate, food and beverage, retail, service, insurance and telecommunications industries. He specializes in providing forensic investigation, internal control consulting, fraud prevention consulting and arbitration services to his clients. You may contact Mr. Schwartz at [rschwartz@deloitte.com](mailto:rschwartz@deloitte.com).

### Matthew Larson

Mr. Larson is a senior manager in the Analytic & Forensic Technology group of Deloitte Financial Advisory Services LLP. His background includes management of engagements ranging from theft of intellectual property or allegations involving only a single laptop, to multinational government fraud investigations that required the imaging and review of multiple computers and the restoration of e-mail and network files from thousands of backup tapes. Mr. Larson may be contacted at [malarson@deloitte.com](mailto:malarson@deloitte.com).

### Mary-Jo Kranacher

Mary-Jo Kranacher is a certified public accountant (CPA) and a certified fraud examiner. She is the editor-in-chief of *The CPA Journal*, the official publication of the New York State Society of CPAs. She is currently on leave from her tenured position as an accounting professor at York College, The City University of New York (CUNY). Prior to joining the CUNY faculty, she was the University's Director of Trusts and Gifts, where she was responsible for the oversight of a \$140 million investment portfolio which she monitored for fraud and abuse.



**About Deloitte**

As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Member of  
**Deloitte Touche Tohmatsu**