

Combating the Higher Education Embezzlement Epidemic



By Christopher T. Marquet
April 25, 2011

There is a rash of major embezzlement cases cropping up like a pox at institutions of higher learning all around the country. While employee theft occurs daily at all types of institutions, we have tracked a disproportionate number of significant misappropriations at US colleges and universities. The damage, while significant, is not only financial. Institutional reputation, alumni relations, endowment growth, employee productivity and even possibly enrollment, can all be negatively affected by a major defalcation.

Conventional wisdom suggests that economic factors, such as economic instability, high rates of unemployment, low consumer confidence and other poor economic indicators, may increase the frequency of many white collar frauds, including employee theft. However, this is certainly not the only factor – as many embezzlers’ schemes last for years before they are found out. In fact, they often begin in good economic times, when it is easier to hide their schemes from otherwise more vigilant management.

Consider the following 14 major embezzlement cases that have surfaced at colleges and universities around the US in just the past year totaling nearly \$18 million in direct losses:

Drake University

April 2011; Robert Alex Harlan, former director of student accounts, accused of embezzling at least \$600,000 over a 7 year period. Harlan allegedly “manipulated institutional accounts” which he then converted for his personal use.

Vassar College

April 2011; Arthur H. Fisher, former project manager, accused of embezzling nearly \$2 million over a 5 year period. Arthur Fisher allegedly set up a phony construction company and charged the college for work not performed. As an aside, a veritable arsenal was seized at Fisher’s home after his arrest.

Kansas City University of Medicine & Biosciences

March 2011; Karen L. Peltz, former President, CEO and Trustee, accused of embezzling more than \$1.5 million over a 5 year period. Peltz allegedly engaged in a variety of fraudulent reimbursement schemes, including receiving additional compensation.

University of Montana

March 2011; Christine Rose Bitterman, former residence life employee, accused of embezzling more than \$300,000 over a 7 year period. Bitterman allegedly pocketed cash payments made by students.

University of Vermont

March 2011; Celine Bernier, former administrative assistant at the UVM Extension program in Newport, Vermont, accused of embezzling \$45,800 over a 5 year period. Bernier allegedly deposited checks made out to the institution into personal accounts she and her husband, Tom Bernier, controlled.

New Jersey City University

December 2010; Shaunette P. Ruffin-Moody, former office manager for the university's student government organization, pleaded guilty to embezzling \$502,000 over at least a 3 year period. Ruffin-Moody issued at least 219 unauthorized university checks to herself, her husband, Alexander Moody and three others.

Columbia University

November 2010; George Castro, formerly affiliated with the university in some undisclosed manner, charged with embezzling \$4.5 million over a several month period. Castro manipulated university accounts and caused electronic funds transfers to accounts he controlled under the name of an apparent vendor.

Duke University

November 2010; John William Cotton, former head of the Department of Surgery, charged with embezzling \$267,000. Cotton allegedly used his position to order goods and services for his own personal use paid for by the department.

Iona College

October 2010; Sister Marie E. Thornton, former vice president of finance, charged with and ultimately plead guilty to embezzling \$1.2 million. Thornton, who reportedly had a gambling problem, issued college checks and used college credit card accounts for her own benefit and was also fraudulently reimbursed by the college with phony invoices.

Virginia Commonwealth University

October 2010; Lisa Jones Durham, former coordinator for a university community outreach program, pleaded guilty to embezzling more than \$144,000 over a 3 year period.

Durham obtained checks made out to herself under her former name to pay for personal expenses.

St. John's University

September 2010; Cecelia Chang, former Vice President for International Relations, pleaded guilty to embezzling more than \$1 million from the university. Chang created a non-profit entity which she represented was affiliated with the institution and fraudulently accepted donations which she converted for her own benefit.

La Salle University

May 2010; Stephen C. Greb, former director of food services embezzled about \$5 million over at least a 20 year period. Greb created a phony food vendor and then authorized fraudulent payments which he pocketed.

Naropa University

April 2010; Ronda F. Devers, former accounts payable clerk, accused of embezzling nearly \$600,000 over a 2 year period. Devers allegedly pocketed student refund checks by voiding them and reissuing them to herself and a girlfriend.

How can educational institutions prevent, detect and respond to this phenomenon? Research conducted by Marquet International, Ltd. suggests that most perpetrators hold some type of position with their employer that involves fiduciary duties. Most schemes of this magnitude also span several years – 4½ on average, according to our research. Further, the most common types of embezzlement involve the following basic types of schemes:

- Forging checks payable to cash, oneself and/or to personal vendors
- Pocketing cash receipts meant for deposit into institutional accounts
- Issuing extra paychecks and/or bonus checks through payroll to oneself
- Submitting fraudulent expense reports for reimbursement
- Submitting fraudulent invoices from phony or legitimate vendors
- Abusing institutional credit card accounts for personal use
- Electronic transfers of institutional funds to personal accounts and/or vendors
- Pilfering institutional equipment and/or inventory

Preventing embezzlement involves active policies that discourage employee theft, backed up by proactive auditing procedures to reinforce the policies and to detect irregularities. The reality is that many colleges and universities, simply as a result of their cultural ethos, do not operate as a typical for-profit commercial operation. As such, while they may be large in size,

many practical business controls may not be in place to prevent or detect common defalcations.

Nevertheless, there are some proactive steps we recommend that higher educational institutions can take to minimize and mitigate the risk of embezzlement. These recommendations include, but are not limited to:

- Do not allow a single individual access to all aspects of institutional finances in any given department. Make sure there are divisions of duties in the finance department in particular.
- Regularly rotate responsibilities for bookkeeping personnel.
- Require bookkeeping personnel to take vacation time off. Embezzlers often take little or no vacations to safely perpetrate their schemes.
- Do not allow bookkeepers to take work home.
- Require two signatories on outgoing checks above a certain nominal amount. The signatories should be different individuals from the check preparer.
- Examine cancelled checks regularly. One common method of embezzlement involves the forgery of checks. Another is to have them payable to the embezzler or to personal vendors.
- Maintain unused checks in a lockbox. Be sure all checks, purchase orders and invoices are numbered consecutively and reconcile any of those missing.
- Conduct regular as well as random audits. Educational institution management should take a hands-on approach by physically spending time with the bookkeeping department periodically.
- Audit petty cash regularly.
- Audit credit card charges regularly.
- Audit expense reports regularly.
- Be sure each payment, electronic or otherwise, is backed up with appropriate documentation.
- Backup financial records daily.
- Make and reconcile daily deposits. Use a “for deposit only” stamp for check deposits. The person recording cash receipts should be different from the one making the actual deposits.
- Bank reconciliations should be made by a different person than those that handle cash receipts and cash disbursements.
- Know who your institution’s vendors are. As we can see from the above examples, embezzlers often create phony vendors and submit fraudulent invoices for payment.
- Examine payroll records regularly. Some embezzlers issue themselves extra paychecks and bonuses through the payroll system, as we have also seen.

- Investigate vendor complaints promptly. If vendors are not being paid as expected, it may be a sign that the payment checks are being diverted.
- Conduct pre-employment background checks for all personnel with any fiduciary duties.
- Prosecute perpetrators, creating a permanent record future employers can find.

An institution's response to the revelation of this type of white collar shenanigans is nearly as important as preventing or detecting them in the first place. A swift investigation, overseen by internal and/or external legal counsel must ensue, beginning with a small circle of those who need to know and expanding from there. Such an investigation will involve an analysis of institutional records as well as possibly conducting select interviews and a possible "external" investigation which would focus on lifestyle, conflicts of interest and asset identification.

The most typical records under your control will be financial books and records. And as such, an independent forensic accounting review will almost always be necessary to quantify the loss and to determine how the scheme(s) worked and to where the monies were funneled and from which sources. The accounting analysis will also be necessary for any future claim under a fidelity policy in the form of a "proof of loss" as well as the basis for prosecutorial referral.

Interviews of select individuals, may also be part of the process. Again, use the reverse onion peel strategy, working from the innermost circle outward as needed which helps contain and control the investigation. This process might include an interview of the suspected perpetrator him or herself. If strong enough evidence is gathered quickly, such a confrontational interview may be beneficial and even elicit a confession. In our experience, interviews should be conducted in a "two on one" format, particularly with the suspect in question. This allows for corroborating testimony of what was said, which is often necessary.

As soon as enough evidence is gathered to satisfy institutional authorities, the suspected employee should be immediately suspended or terminated, including all computer, banking, communications and other access rights and privileges. In the event, such a decision should be made within hours or a few days at most, but certainly should not be delayed much longer – in order to minimize further losses as well as to preserve crucial potential evidence.

The internal investigation will necessarily continue after the employee is removed. Our research into the embezzlement phenomenon indicates that many perpetrators use more than one scheme – sometimes several – to steal from their employer. Further, their thefts will have invariably spanned a duration longer than originally thought. A thorough investigation will

therefore look into all aspects of the suspected perpetrator’s employment responsibilities and venture as far back as the time of their hiring.

Any chance at recovery or restitution may also depend upon your “external” investigation. While it is true that many embezzlers spend their ill-gotten gains in such a way as to make restitution difficult – such as gambling, luxury travel, gifts to others and purchases of consumables, many other types of assets can be identified and attached or seized. Homes, luxury vehicles, watercraft, other business interests and luxury items such as art, jewelry and designer clothing may be worth seizing and auctioning off. Third party beneficiaries of the theft – often family members such as spouses, children, parents and others – are also potential sources for recovery. Bank accounts, retirement accounts, investments accounts, such as brokerage and mutual funds, can be identified through subpoena in either a civil or criminal proceeding. In some cases, a judge can be convinced to issue an order freezing assets and giving a forfeiture order.

Finally, as alluded to above, I strongly recommend that all embezzlement cases ultimately be referred to authorities for prosecution. Failure to do so 1) does not adequately punish the perpetrator; 2) provides no discouragement for potential future embezzlers; 3) arguably hurts employee morale and productivity; and 4) puts future employers of the perpetrator at risk for the same type of theft. In general, the better the internal investigation and “packaging” of the evidence, the swifter the prosecutorial response. If federal or state prosecutors are uninterested due to the size of a given employee theft, civil action is always an option and still achieves some of the above stated goals. In either case, expert legal counsel will be required throughout the process. The timing of a criminal referral must also be considered. Once it is made, any civil action will be stayed pending the outcome of the criminal proceedings – which often take time.

While employee theft at America’s colleges and universities is all too common these days, prudent steps, such as those outlined above, can help minimize and mitigate the risk.

* * * * *

Christopher T. Marquet is Chief Executive Officer of Marquet International, Ltd., an investigative and security consulting firm based in Boston, Massachusetts. He can be reached at (617) 733-3304 or chris@marquetinternational.com. Marquet International publishes its annual Marquet Report on Embezzlement which can be found on our website at www.marquetinternational.com.