Another Way to Share Your Financial, Compliance, and Ethical Concerns – the RIT Ethics Hotline

In the complex and fast moving work environments we find ourselves in these days, we may observe situations or activities that just don’t seem right. In the Taking Responsibility document which may be found at [www.rit.edu/fa/iaca/sites/rit.edu.fa.iaca/files/forms/ethicsbrochure.pdf](http://www.rit.edu/fa/iaca/sites/rit.edu.fa.iaca/files/forms/ethicsbrochure.pdf), Dr. Destler states that “The University’s reputation depends on the personal integrity and commitment of every person. Each employee shares in the responsibility to promote a safe and ethical environment, to conduct their business and employment activities in a highly principled fashion, and to report violations of the Institute’s ethical standards.” When we observe these situations or activities and when discussion with a supervisor may be challenging or may make us feel uneasy about bringing the issue forward, RIT employees have another way to alert management that something may be amiss – the RIT Ethics Hotline.

The RIT Ethics Hotline (the Hotline) was established in November 2005. The Hotline is an ideal way for RIT employees to report financial, compliance, and ethical (including conflicts of interest) concerns they have observed while maintaining anonymity. The Hotline is hosted by EthicsPoint, a Navex Global company. It is important to note that the Hotline is NOT intended to supersede existing processes for reporting concerns or emergencies (such as speaking to a supervisor or contacting the Human Resources or the Public Safety Department), but rather to be an option for employees who are uncomfortable reporting a situation in person.

To report a concern, an employee may do so electronically at [www.ethicspoint.com](http://www.ethicspoint.com), by telephone at 866-294-9358, or by TTY at 866-294-9572. The reporter will first be asked to categorize the report into one of five general categories: financial, research, employee benefits, confidentiality, or information security/privacy. The reporter may choose to remain anonymous or to identify themselves. Of the reports received to date, approximately 82% of the reporters have chosen to remain anonymous. There are a number of RIT websites (i.e., Controller’s Office, Global Risk Management Services, and IACA) that have a link to the Hotline to click on which will take you to the RIT EthicsPoint File a Report webpage. Also, Dr. James Watters’ (Senior Vice President for Finance & Administration) webpage [www.rit.edu/fa/svp/](http://www.rit.edu/fa/svp/) (Ethics and Compliance sidebar) has information about the Hotline and a link to make a report.

(continued on p. 2)
After a report is made, a small group of senior RIT managers (report recipients) receive the report and promptly dispatch the report to the appropriate RIT department(s) for investigation (i.e., Human Resources, IACA, Controller’s Office). It is important to note that all investigations are performed in a careful and methodical manner thereby maintaining confidentiality at all points along the way. Soon after the report is received, a general receipt acknowledgement is posted in the system. An investigating department, via the report recipient, may choose to communicate with the reporter and ask additional questions by utilizing the Hotline system. Once a reporter files a report, he/she is provided with a code so that they may log back into their report (or call back) to see if “RIT” has any questions for them. This anonymous back and forth discussion is a useful function of the EthicsPoint system. The reporter is under no obligation to provide additional information; however, receiving such information can often facilitate the investigation.

At the conclusion of an investigation, the appropriate report recipient will post a concluding comment similar to “the investigation has been completed; thank you for using the RIT Ethics Hotline to report your concern.”

The RIT Ethics Hotline is a great option for employees to utilize when they are uncomfortable about bringing a concern forward in person. Every report is taken seriously and is appropriately investigated. If you have any questions about the Hotline, please contact me at smmiaca@rit.edu.

~~ Contributed by Steven Morse
Assistant Vice President
Institute Audit Compliance & Advisement

What Were They Thinking?!

A woman from Harrisburg, Pennsylvania was charged in October of 2013 with using a college-issued credit card to purchase hundreds of thousands of dollars worth of gift cards online using funds from the Harrisburg Area Community College (HACC) campus. Nancy Rockey, age 55, was the vice president of College and Community Development until her February 2012 resignation after the discovery of her fraud scheme.

The gift cards to Target™, which totaled over $228,000, were used to purchase non-work-related items for herself, friends, and family members. Following the purchases, Rockey created fake invoices which were sent to the HACC Finance Office in an attempt to cover up the fraud being committed.

Prosecution of the case was performed by Assistant US Attorney Joseph J. Terz, while the FBI, as well as the Dauphine County Criminal Investigations Division, investigated the case.

On November 14, 2013, Rockey pleaded guilty to the wire fraud charges placed against her, and could face up to 20 years in federal prison as well as a fine depending on the nature of the circumstances and the history of the defendant.

Lesson Learned: This could have been detected sooner with a more thorough review of detailed department financial statements (e.g., ledger reports) by Rockey’s supervisor.


~~ Contributed by Patrick Didas
Associate Director
Institute Audit Compliance & Advisement
Inform RIT

Inform RIT is a recurring column provided by the RIT Information Security Office. The column highlights current issues and initiatives that impact the RIT community. In this issue, we’ll talk about secure use of mobile devices. Our thanks to Professor Rick Mislan and the Department of Computing Security for providing core information for the article below.

Using your Mobile Device Safely
Mobile devices (smartphones, tablets, iOS devices, etc.) pose difficult security risks. They’re often personally-owned and may not have the security controls you would expect on a laptop or desktop computer. Organized crime is funding development of malware to attack mobile devices. It’s important to understand what types of security controls you should use to protect both yourself and RIT.

There are a number of ways in which information on a mobile device may be breached: theft of the device, attacks on your service provider, wireless hijacking or "sniffing," and unauthorized access. Because mobile devices may be more easily stolen or compromised, users of these devices must take precautions when using them to store or access Private or Confidential Information.

Private Information and Mobile Device Use
We recommend that Private Information NOT be accessed from or stored on mobile devices. If Private Information must be accessed from or stored on a mobile device, then the information on the mobile device must be encrypted. Password protection alone is NOT sufficient.

To ensure that RIT information will remain secure, you should use only devices that provide encryption while information is in transit and at rest.

Security requirements for handling RIT Private, Confidential, and other information may be found in the Information Access and Protection Standard <www.rit.edu/security/content/information-access-protection-standard>.

General Guidelines for Mobile Device Use at RIT

Understand Your Device

Configure mobile devices securely. Depending on the specific device, you may be able to:

Enable auto-lock. (This may correspond to your screen timeout setting).
Enable password protection.

Use a reasonably complex password where possible.
Avoid using auto-complete features that remember user names or passwords. You may want to use a password safe application where available.

Ensure that browser security settings are configured appropriately.
Enable remote wipe options (third party applications may also provide the ability to remotely wipe the device; if you're connecting to mymail.rit.edu with ActiveSync for email and calendaring, you may wipe all data and applications from your device remotely from mymail.rit.edu).

“I believe in evidence. I believe in observation, measurement, and reasoning, confirmed by independent observers.

I’ll believe anything, no matter how wild and ridiculous, if there is evidence for it.

The wilder and more ridiculous something is, however, the firmer and more solid the evidence will have to be.”

- Isaac Asimov, scientist and writer (1920-1992)

(continued on p. 4)
**Disable Bluetooth** (if not needed). This will help prolong battery life and provide better security.

**Ensure that sensitive websites use HTTPS in your browser URL on both your computer and mobile device.**

**Know your mobile vendor’s policies** on lost or stolen devices. Know the steps you need to take if you lose your device. Report the loss to your carrier ASAP so they can deactivate the device.

**Use appropriate sanitation and disposal** procedures for mobile devices.

**Use Added Features**

**Keep your mobile device and applications on the device up to date.** Use automatic update options if available.

**Install an antivirus/security program** (if available) and configure automatic updates if possible. Like computers, mobile devices have operating systems with weaknesses that attackers may exploit.

**Use an encryption solution** to keep portable data secure in transit and at rest. WPA2 is encrypted. 3G encryption has been cracked. Use an SSL (HTTPS) connection where available.

**General Tips**

**Never leave your mobile device unattended.**

**Report lost or stolen devices and change any passwords** (such as RIT WPA2) immediately.

**Include contact information with the device:**

On the lock screen (if possible). For example, "If found, please call RIT Public Safety at 585-475-2853. "Engraved on the device or inserted into the case.

For improved performance and security, register your device and connect to the RIT WPA2 network where available.

**Get informed**

Visit the RIT Information Security website <www.rit.edu/security> to read the security standards, access security tools and software, or find out more ways to protect yourself.

~~ Contributed by Ben Woelk
Program Manager
Information Security Office

**Watch IACA’s Monday Minute video series here!**

This monthly one-minute video series focuses on opportunities for improving internal controls; we hope that you find the information beneficial. If you have questions, feel free to contact anyone in the IACA office using information on our webpage.
As explained in the last Quaestor Quarterly, the COSO Framework (an internationally recognized standard against which the adequacy and effectiveness of an organization’s internal controls are evaluated) was updated in May 2013 to further define the principles underlying the five components of internal control (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring). According to the COSO Framework (the Framework), these principles are fundamental concepts that must be present and functioning in order to achieve an effective system of internal control. In addition, the Framework includes points of focus or characteristics that are examples of behaviors or processes that one would expect to be in place in order to conclude that the related principle is in fact present and functioning. This edition of the COSO Corner will summarize the first principle relating to the Control Environment component of the Framework, as well as the related points of focus (or expected controls).

**Principle 1 –** The university (including its board, management, and all faculty and staff members) demonstrates a commitment to integrity and ethical values. Key characteristics (points of focus) relating to this principle include:

- The Board of Trustees and management at all levels of the entity demonstrate through their directives, actions and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
- The expectations of the Board of Trustees and senior management concerning integrity and ethical values are defined in the entity’s standards of conduct and understood at all levels of the organization.
- Processes are in place to evaluate the performance of individuals and teams against the expected standards of conduct.
- Deviations from the university’s expected standards of conduct are identified and remedied in a timely and consistent manner.

Are you familiar with the RIT Compliance Policy and Code of Ethical Conduct? [http://www.rit.edu/academicaffairs/policiesmanual/sectionC/C0.html](http://www.rit.edu/academicaffairs/policiesmanual/sectionC/C0.html)


~~ Contributed by Nancy A. Nasca
Senior Internal Auditor

---

### Training Opportunities Provided by IACA

IACA’s Internal Controls and Fraud in the Workplace class is two and one half hours in length and is required to receive the RIT Accounting Practices, Procedures and Protocol Certificate of Completion. However, anyone interested in learning about internal controls and fraud prevention is welcome to attend.

To learn more about these important topics, sign up for IACA’s Internal Controls and Fraud in the Workplace class at the CPD website: [http://www.rit.edu/fa/cpd/leadership/internalcontrolsandfraud.html](http://www.rit.edu/fa/cpd/leadership/internalcontrolsandfraud.html)

---

**Upcoming Session:**

April 29, 2014 -
1:30pm - 4:00pm
2140 Louise Slaughter Hall
As the Executive Director of Dining Services, I have experienced working with IACA during multiple audits; most recently a revenue audit. I believe that when most people hear the word "audit" or "compliance," there is a natural anxiety of what will be "found." I believe that an audit’s purpose is not to simply point out areas of improvement but to also highlight strengths of an organization. The IACA staff are experts in their field and continually keep us abreast of new developments to improve our internal controls with a practical approach.

One thing we thoroughly appreciated was the in depth information that was provided in the summary reports. This went well beyond just improving internal controls based on processes. We were also given recommendations in terms of staffing and segregation of duties that may perhaps enhance our customer service. Dining Services can be very complex; as there are nuances about our department that are unique as compared to other departments within the University. IACA’s ability to adapt and spend the necessary time to understand our business before giving recommendations was greatly appreciated. It was evident they wanted to ensure a positive customer experience. Our management team, including myself, felt the feedback was thorough, fair and an overall good exercise to keep us in position of pro-activeness rather than reactiveness.

~~ Contributed by Kory Samuels
Executive Director
Dining Services

---

**Question:**
I heard that auditors say, “Trust but Verify.” What does that mean?

**Answer:**
This phrase is often used by auditors to emphasize the importance of verifying information. We all realize that trust is an important component of any successful relationship; professional or personal. In a business environment where it is imperative that employees at all levels of the organization trust one another, it is equally important to verify transaction specifics in order to protect the integrity of the individuals involved in a transaction, the control environment, and the organization. This verification may be achieved by a thorough review of original supporting documentation.

Remember that trust is not a control, so go ahead and trust………but verify.
Pop Quiz Challenge

Take the Pop Quiz Challenge! Correctly answer the question below and you will be entered in a drawing to win a prize valued at $15. One lucky winner will be chosen randomly and notified by email.

**Question:** According to the article, *Another Way to Share Your Financial, Compliance, and Ethical Concerns - The RIT Ethics Hotline*, what happens first after a report is made?

A. A department investigation occurs immediately following the report.
B. A general receipt acknowledgement is posted in the system.
C. A small group of senior RIT managers receive the report and dispatch it to the appropriate department(s) for investigation.
D. Additional questions are immediately asked of the reporter.

_Post your answer to our Quiz webpage at:_
https://www.rit.edu/fa/iaca/content/quiz

The winner’s name and answer will be included in the Spring ’14 Quaestor Quarterly Newsletter.

******************************************************

Congratulations to Helen Adamson from the College of Liberal Arts for correctly answering the Fall issue’s Pop Quiz question.

The question and the correct answer were:

According to the article, *What is the Standard by Which Internal Controls are Evaluated?*, “Control Activities” are...

A. …often known as “Tone at the Top” and refer to the ethical values of senior management
B. …specific processes designed to mitigate the risks which would prevent an organization from achieving its objectives
C. …both external and internal and must be identified
D. …crucial components of an effective internal control system enabling management to successfully conduct, manage, and control its operations