The Wonders of Modern Technology
By Pete Kennedy, CPA, CVA

I recently attended a seminar that focused on popular types of fraud schemes. One area that was addressed was the many ways modern technology can be used to either commit or conceal fraudulent activity. Quite an eye-opener! I poked around on the Internet to see what is out there and even with my limited imagination I found a few examples.

If you’ve used the company credit card for personal reasons and need a fake receipt to cover it up, just type “fake receipts” into Google. There are literally dozens of websites that promise to provide an authentic-looking receipt that will make that on-line poker tournament registration look like a four-course business meal.

Next, let’s say the bookkeeper needs to get the boss’s password for on-line account access so he / she can make that pesky personal car payment. No problem – using Google again look for “password hacking software” and again there is a choice of many that promise to do the trick – some are advertised as being free.

OK, now let’s say you need to fake a signature to authorize a bogus expenditure. It’s YouTube to the rescue! All you need is a copy of the legitimate signature and there are helpful videos of a variety of methods from rudimentary tracing to sophisticated Photoshop transfers. One of the contributions was from a person whose moniker was “Worksuxs” so I have a feeling some of the methods have been tried and passed muster in a work environment.

Alright, now the bookkeeper needs some quick cash. A fake check would do the trick! Those are too easy, but now how to cover it up? Once again, just Google “fake bank statement” and a laundry list of providers will appear. Interestingly, they are not advertised as a way to perpetrate fraud, but as a great way to get better organized or to “pick up chicks” (just when you thought this couldn’t get any weirder….). Now I’ve been married for 15 years so I’ve been out of the dating game for a while, but I can’t recall being asked to bring a bank statement to a date – possibly the dating scene has changed radically. By the way, the same site advertises fake referrals and fake UCC statements.

It is important to know that just about any document can now be easily faked. In 2004, the management at Parmalat dummied up a letter verifying a $5 billion cash account to fool their auditors, reportedly running it through a fax machine several times so it would appear authentic. The phony cash was needed to balance out nonexistent sales that had been reported to meet revenue targets. In the 8 years since 2004, advances in computer software have made “running it through the fax machine” unnecessary.
The possibilities to circumvent password controls and cover up fraud with phony documentation are seemingly limitless. Are organizations at the mercy of computer-savvy fraudsters? Not necessarily. Let’s go back to a few basics with internal controls that have nothing to do with documentation.

The “control environment” is the first line of defense against fraud in any organization. In a nutshell, this refers to the tone at the top, the ethical expectations of all involved and how those expectations are communicated to employees. An organization with a lax control environment is much more fertile ground for a fraud to sprout. Where management cuts corners even in small and seemingly insignificant ways, it sends a message to the rank and file. Are senior management and board members meticulous at following controls themselves? Are controls strictly enforced across the board? Are the ramifications of failing to adhere to control processes clearly communicated?

In a 2010 study of reported fraud cases, a fraud at a nonprofit organization was almost 7 times more likely to be reported by a tip (43.2%) than by the examination of documents (6.5%). The overwhelming majority of those tips came from rank and file employees reporting suspicious behavior or circumvention of controls on the part of their peers or managers. An established fraud hotline or formalized anonymous reporting procedure made a pronounced difference in reporting rates. Organizations with such a mechanism were even more likely to have it reported via the hotline (47.1% vs. 33.9% without). At organizations with hotlines, the frauds were detected sooner and with a lower average loss.

An organization’s system of controls should not begin and end with documents. A strong control environment and a formal mechanism for voluntary anonymous reporting of suspicions can make a huge difference in the susceptibility of your organization to fraud.

For help setting up a fraud reporting hotline, please contact Pete Kennedy or any other member of our Nonprofit Practice team at Cover & Rossiter at (302) 656-6632.

Cover & Rossiter, P.A. (www.CoverRossiter.com) is one of the most respected and experienced CPA firms serving the accounting, tax and audit needs of the nonprofit community in Delaware.