Exploiting a Position of Trust

By Joseph M. Palmar, CPA CFE CFF

A trusted vendor, a long time business associate, or a close friend; we all have them and rely on them. When a close friend or business associate does the unexpected and violates a trust, the hurt cuts to the heart. Seemingly, there is no real way to stop the pain as it stays with you, at least in the back of your mind. You may even call yourself into question –"I should have known better" or "How did I miss this?" No one likes getting burned, but the impact is far greater when the opportunist is a trusted individual upon which you rely.

Vendors hold a unique position in our business lives. They provide necessary services to our companies, deliver goods, and depending on the length of their relationships, sometimes become part of the family. This, at times, leads us into a false sense of security not only regarding the quality and pricing of those goods and services, but also the integrity of the vendor.

How can this false sense of security be prevented? Is there anything we can do to avoid or prevent a violation of trust? One way is to ensure transparency in our business relationships. Do you really know who you are doing business with or have you fallen asleep at the wheel because the particular vendor "*assists at all hours of the day or night" or "employs the go to people that get the job done?"*

According to the Association of Certified Fraud Examiners' 2014 Report to the Nations, approximately 5% of a company's gross revenues are lost to fraud annually. While clearly this does not only encompass vendor related fraud, decision making may be impacted by identifying undisclosed relationships of vendors. Employing preventative measures to uncover "what you don't know" may mitigate the hurt associated with an exploitation of trust.

This was the case with Valeant Pharmaceuticals International and its initially undisclosed captive pharmacy Philidor. Valeant was a darling of Wall Street. Hedge funds and "smart money", piled into the stock as the company's revenue skyrocketed. It was seemingly all based on a new business model. The company developed a strategy to create a drug giant that focused on distribution and let someone else do the research. The plan was, of course, controversial and required rapid acquisitions to make it work. Valeant became one of the hottest healthcare stocks in recent years by buying other firms' medicines and then swiftly hiking their prices by as much as 500%.

However, allegations began to surface that Valeant's true success may have been built on not only price gouging, but a secret network of specialty pharmacies, and fraud. In fact, the Southern Investigative Reporting Foundation was the first to detail the odd ties between Valeant and a rapidly growing specialty pharmacy that appeared to be controlled by Valeant, Philidor. Interestingly, the relationship had ***never been disclosed to Valeant shareholders***. An investigation by the Wall Street Journal further discovered that Valeant employees were frequently involved with the operations at Philidor and used fake aliases including those of comic book characters, like Peter Parker, to hide their identities.

In fact, it wasn't until later, on one of Valeant's conference calls, that the company first disclosed it had purchased Philidor for $100 million. It later acted to cut its ties to Philidor and subsequently disclosed that the pharmacy would shut down immediately. However, by this point the stock had fallen from a high of $260 per share to about $90! *Highlighting yet another example of how what you don't know can and will hurt you.*

So what do you do to protect your company and the reputation of its directors and officers? Knowing all you can about who you are doing business with is a great place to start. Do they have undisclosed relationships with any other company, other vendors already existing in your company's vendor master file, your employees, or other key stakeholders? Do your vendors' officers have criminal records, are their business licenses active and in good standing, have you checked them against sanctioned listings such as Office of Inspector General (OIG) or Excluded Parties Listing (EPLS)? Are there pending lawsuits or liens against them?

A robust on-boarding process coupled with proper training of line staff in both payroll and accounts payable departments is essential. Things to consider include:

- Avoid potential conflicts of interest and identify undisclosed relationships through a thorough vendor credentialing process. This will ensure that your company is comfortable with the vendors they are doing business with. This can be accomplished through a system such as VETTED®. As part of this credentialing process vendors should be required to disclose any and all ownership interest they have in other organizations. All such disclosures should be thoroughly investigated.
  Note: Vendors could be charged a nominal fee to offset incremental costs of credentialing vendors or pay directly to the third party provider, effectively, resulting in a zero cost solution.

- Require all employees, especially those in key decision making positions, to sign a conflict of interest statement requiring them to disclose any and all relationships they may have with businesses and/or individuals; including any relevant investments.

- Validate all new and existing vendors to the IRS website. Ensure that all vendors are legitimate, have valid FEIN's. No vendor should be approved/added without a properly completed W9 and valid FEIN.

- Identify and remove all duplicate vendors.

- Have one department assigned the responsibility to on-board vendors. A single point of entry for on-boarding of vendors is not only a best practice it also affords you a systematic review of the vendor master file in order to minimize duplicates and/or errors.

- Develop a standard naming convention to be used in the vendor setup process as a means of avoiding duplicate vendors.

- Limit access to the vendor master file to the same department assigned the responsibility of on-boarding vendors.

- Develop appropriate segregation of duties between vendor setup in the system and the review and approval of that setup.

- Only a limited group of approved individuals should be allowed to add, modify, or in any other way change or adjust vendor data. A log should be maintained of all modifications and reviewed by an independent manager.

- A complete review should be made of all vendors in the accounts payable database with specific attention to vendor address. Duplicates and those with different names but sharing the same address should be investigated thoroughly.

- If a vendor has multiple remit to addresses, setup one vendor (as opposed to multiple vendors) with multiple remittance addresses.

- Remove all employees from the accounts payable master file and process expense reimbursements through payroll as an Employee Expense Reimbursement (EER).

- Any vendor with no activity for the preceding 15 months should be de-activated.

- Periodically and systematically review and compare vendor, employee, and other related data (i.e. physicians, professors, students, dependents, beneficiaries, etc.) in an effort to identify duplicates, errors, irregularities, and anomalies. **Note:** This can be accomplished via a service like that offered by Database Queries®. Findings should be communicated to the appropriate level of management and a corrective action plan should be developed, implemented, and reviewed.

- Require all vendors to do regular background checks of all their employees and subcontractors that have access your data and/or facilities.

Vendors are trusted business partners. They are often familiar with confidential and strategic plans for your company. In many cases, they have access to personal identifiable information (yours and/or your client's) and/or key operating systems.

Once a fraudulent vendor gets into your system, it is like a Trojan horse or computer virus that upon release could cause havoc. Losses due to misappropriations may cost companies hundreds of thousands if not millions of dollars; not to mention loss of reputation, future revenue, and/or career potential for those at the helm.

Our experience shows that well intentioned and highly educated managers, even in effective and excellently controlled environments, can often leave themselves and their organizations vulnerable to fraudulent vendors. They simply don't know what they don't know; a blind spot that can really hurt you and your organization!