



NOW AVAILABLE: “Detecting and Preventing Fraud in Accounts Payable” By Peter Goldmann, this brand new book provides valuable insight into how fraudsters exploit your Accounts Payable systems and *how to stop them!!!* Click: <http://www.iappnet.org/ViewItem-468.do?parentCatId=305>

Dear Subscriber:

Here's your latest complimentary update of the valuable fraud-fighting content that subscribers to *White-Collar Crime Fighter* receive every month...

Industrial Espionage: Heightened Threat in Slow Global Economy

In today's global business climate it is a huge risk to ignore the risk of victimization by spies seeking to steal your proprietary data, trade secrets and intellectual property. Competitors, criminals and foreign governments are becoming increasingly aggressive in illegally gathering proprietary information.

Often, their tactics are electronic— such as hacking into secure networks. But remote electronic information theft is not always technologically feasible. Thus, if you underestimate the potential danger of being victimized by “human intelligence practitioners”, i.e. spies, you do so at great risk.

And in tough economic times like these, your organizations may be especially vulnerable to so-called “walk-in” sources of confidential information — employees concerned about losing their jobs or their homes who are thus motivated to sell such information without even being approached by outside spies.

SELF-DEFENSE MEASURES...

- Regularly and rigorously train employees with access to intellectual property— both in the US and abroad— to be alert to the highly deceptive and often hard-to-detect tactics of seasoned industrial spies. These tactics very often involve the offer of financial enrichment which itself can be a red flag of potential attempts to gain the confidence of an insider with access to proprietary information.
- Require all business partners to sign non-disclosure agreements.
- Conduct thorough background checks on prospective employees who may need access to sensitive information.
- Maintain maximum physical security of physical assets such as laptops, removable storage devices, etc.
- Implement and train employees to use a hotline or other reporting channel to

use when signs of espionage are detected.

***White-Collar Crime Fighter* source:**

Fred Burton, Vice President for Counterterrorism and Corporate Security at Stratfor, a private political, economic and military intelligence-gathering organization, www.stratfor.com. Burton was a special agent with the U.S. State Department's Diplomatic Security Service and is the former deputy chief of the counterterrorism division of the DSS. He was involved in the arrest of Ramzi Yousef, the mastermind of the first World Trade Center bombing in 1993. He can be reached at burton@stratfor.com. [For the entire article, subscribe now to *White-Collar Crime Fighter* at <http://www.wccfighter.com/subscribe>. You will receive not only the issue in which this article appeared, but also a FREE copy of the new book by Peter Goldmann, *Anti-Fraud Risk and Control Workbook*, published by Wiley & Sons, <http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470496533.html> — a \$50 value.]

Help for Frustrated FACT Act Implementers

After a year or more of confusion on the part of businesses and their lawyers, the Federal Trade Commission (FTC) has launched a Web site to help businesses and non-profits to come into compliance with the so-called Red Flags Rules on identity theft contained in the Fair and Accurate Credit Transaction Act (FACTA).

Businesses were originally required to be in compliance with the Red Flags Rule last November 1. The FTC will begin enforcing the rules on May 1.

In short, the Red Flags Rule is designed to force businesses and non-profits to implement anti-identity theft programs that alert organizations to the potential illegal use of personally identifiable information (PII) of employees, customers, medical patients, etc. such as Social Security numbers, driver's license numbers and medical information,

The new FTC site provides articles and guides for helping create identity theft prevention programs, a key requirement of the rules. The most useful offering is a "how-to" guide called *Fighting Fraud with the Red Flags Rule*

To obtain the guide and additional useful compliance information visit <http://www.ftc.gov/redflagsrule>

Case Study: A Yeoman's Job of Ripping Off Her Employer

Vista, CA Annette Yeomans— who apparently is anything but— confessed to stealing \$9.9 million from her employer of 15 years, Quality Woodwork, a privately-owned San Marcos, CA maker of custom cabinetry.

According to Sgt. Mark Varnau of the Sheriff's Financial Crimes Unit, Yeomans abused her position as the company's bookkeeper and apparent de facto chief financial officer, to write nearly 600 checks to herself between 2001 and 2007 in

amounts that totaled as much as \$100,000 per month.

In a classic case of total absence of internal controls, Yeomans was able to do as she pleased with the company's funds while, according to Sgt. Varnau, her husband, who worked at the same company as a cabinet installer, had no clue that his wife was stealing.

Considered a flight risk, the judge in the case held her on \$10 million bail after pleading guilty to multiple counts of embezzlement and grand theft.

Among her routine frauds, according to Sgt. Varnau, was charging up to \$25,000 a week on her personal credit card and then every Monday pay off the balance with a company check.

In other instances, she allegedly made out checks to herself and cashed them at ATMs and casinos. It is reported that Yeomans had a serious gambling habit and may have lost up to \$6 million of the total \$9.9 million in misappropriated funds at local and out-of-state casinos.

Apparently, neither these gambling junkets nor shopping trips to Italy raised any suspicion on the part of her husband who, miraculously is not charged with any crimes related to those of his spouse.

The same applies to the banks and credit card companies that were processing transactions related to her ill-gotten gains. It was not until her credit card company finally noticed in 2007 that Yeomans was paying off her personal credit card with Quality Woodworking checks that her scheme was uncovered.

Detective Vicky Armitage of the San Diego Sheriff's Department spent nearly a year gathering financial documents and records spanning the seven years of Yeoman's brazen thefts.

According to the DA's office, Yeomans faces up to 40 years in prison if convicted.

NOW AVAILABLE!!! FRAUDWARE 3.0
THE LATEST UPGRADE TO THE MOST EFFECTIVE
FRAUD AWARENESS TRAINING COURSE AVAILABLE

FraudAware®

Business Integrity and Compliance Solutions

Any Organization Looking to Stop the Bleeding
Of Fraud Losses in a Down Economy Needs This Training!

VIEW THE FREE NEW DEMO at
<http://www.fraudaware.com>