WHITE-COLLAR CRIME FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 14 NO.2
FEBRUARY 2012

IN THE NEWS

SEC Missed Much More Than Just Madoff

It turns out the Securities and Exchange Commission missed more than just the $50 billion Bernard Madoff Ponzi scheme.

According to former SEC Inspector General David Kotz, in the years leading up to the financial crisis, the SEC became aware of red flags about activities occurring on Wall Street. But the agency did not take meaningful action to stop these questionable financial practices.

Example: Prior to the Bear Stearns bailout in 2008, the SEC was well aware of the dangerous obsession on the part of Bear Stearns management with short-term results and the disregard for risk management, as well as its increasing concentration of mortgage securities, but it did not exert influence over Bear Stearns or take any action to limit these risk factors. Kotz likened the SEC's lack of effective oversight of investment banks in pre-crisis Wall Street to that of the numerous failed calls for action in the Madoff Ponzi scheme.

As to whether the SEC has changed its approach to securities fraud regulation, the recent string of high-profile insider trading investigations suggests it has. Whether it is enough to change the toxic attitude on Wall Street that led to the crisis remains to be seen.

White-Collar Crime Fighter **source:** H. David Kotz, Managing Director, Gryphon Strategies, corporate investigation, litigation support and due diligence service providers. David is the former Inspector General of the SEC. He can be reached at hdkotz@gryphon-strategies.com.

IN THIS ISSUE

Norman Katz, CFE, CFS, *Katzscan Inc.*

SUPPLY CHAIN FRAUD

How It Happens and How to Prevent It

The term "supply chain fraud" is often associated with dishonest activities in the procurement function. That is an extremely myopic perspective.

Reason: Supply chain frauds can happen in operational areas such as purchasing, sales order processing, invoicing, payments, distribution (picking, packing, shipping, receiving), inventory control, fixed asset management, sales commissions and manufacturing.

The supply chain extends throughout an organization—encompassing not just the relationships with external customers and suppliers but also the relationship between internal customers and suppliers. As such, there are just two supply chains an organization must be concerned with—the inbound supply chain and the outbound supply chain.

There are just two supply chains an organization must be concerned with—the inbound supply chain and the outbound supply chain.

Key: Once the supply chain is viewed as movement through the organization without regard to walls or geographic boundaries, it becomes apparent that more supply chain activities occur within an organization than outside of it, and are thus more readily controllable because they are directly within the organization's sphere of influence.

Result: With greater control over processes and software systems, it becomes easier to detect fraudulent activities…understand how the fraud was perpetrated…and then shore up the internal controls to reduce the chances of the fraud occurring again.

YOU AND YOUR CUSTOMERS

What is moved between a supplier and a customer—whether internal, external or a combination—can include raw materials, components, finished goods, money, services, data or documentation. From the perspective of fraud or loss prevention, it does not matter. What matters is that something moves from a supplier to a customer. That movement is expected to be whole or complete in that there is no expectation that whatever was moved from the supplier to the customer must be moved back from the customer to the supplier. The same metrics and key performance indicators (KPIs) used to grade supplier performance externally can thus be applied to internal supplier performance as well.

Caution: Abnormal behavior that is an indicator of possible fraudulent activity can include seemingly perfect behavior too, so don't just think that because everything seems to be running smoothly that it actually is. Fraud is an act of deception and concealment used for the perpetrator's personal gain. Fraud gains can be direct—such as immediate payoff—or indirect such as a favor done at a later date.

In the supply chain process, a laundry list of frauds must be screened for. *Examples:*

- Tainted or poor quality goods with falsification of quality assurance testing by the organization after a supplier's goods are accepted.

•Stolen incoming or outgoing shipments (in whole or in part).
•Bribery from suppliers.
•Kickbacks from sales people.
•Theft or sabotage by a disgruntled employee, contractor, customer, competitor or supplier.
•Financial deception against stock price.

DETECTION DIRECTIVES

Detecting fraud in the supply chain often requires the use of software to record and control transactions and a migration from paper to paperless transactions.

The software which records and controls supply chain activities—including purchasing, accounting, sales order processing, manufacturing, distribution, inventory, etc.—is the organization's primary business software system, generically referred to as Enterprise Resource Planning (ERP). The ERP system houses the transaction records and other data related to the organization's customers, vendors, employees and products.

USING YOUR ERP AGAINST SUPPLY CHAIN FRAUD

Important: To limit fraudulent activity, your ERP system should place restrictions on transactions by user role as well as limits by quantity or amount.

Example: Only users authorized to purchase goods should be permitted to execute purchase orders. Within this user "designation of authority," there should also be limits to what the user can do, such as making no purchases over a certain quantity or dollar amount within a defined time period.

The same should apply to sales order entries.

When user limits must be exceeded for a particular one-time reason, electronic authorization from a manager should be required within the ERP system. And don't forget to ensure that audit logging exists and is turned on!

Details: Audit logging should capture changes to data fields and record all transactions executed along with the user identification and date/time of the transaction. No user—not even a system administrator—should have the authority to alter the audit logs.

Reason: Audit logs can be analyzed during fraud investigations to determine if data was changed to cover a fraudster's tracks. Analysis of audit logs to identify patterns of data entry or data modification can also be used to look for potential fraudulent activities in their early stages.

BARCODES TO BEAT THE BAD GUYS

Barcode scanning is commonly used for picking, packing, receiving and inventory counting activities. EDI transactions include purchase orders, electronic bills of lading, invoices, credit/debit adjustments and payment remittances.

Objective: With formerly paper-based transactions now in electronic format, they can be efficiently audited and cross-checked for accuracy and integrity…and signs of fraud.

Example: Using barcode scanning during the receiving process you can electronically match goods received from a supplier against the detail of the purchase order.

But don't stop there. Compare the purchase order to the EDI Advance Ship Notice even before the goods are physically received. Then compare the invoice to the electronic receiving data to ensure that you are only paying for

WHITE-COLLAR CRIME FIGHTER

Editor
Peter Goldmann, MSc, CFE
Consulting Editor
Jane Y. Kusic
Managing Editor
Juliann Lutinski
Senior Contributing Editor
David Simpson
Associate Editor
Barbara Wohler
Design & Art Direction
Ray Holland, Holland Design & Publishing

White-Collar Crime Fighter (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 2417 Havershire Dr., Raleigh, NC 27613. www.wccfighter.com. Subscription cost: $295/yr. Canada, $345.

Mission Statement

White-Collar Crime Fighter provides information of maximum practical value to organizations and individuals involved in all facets of investigating, detecting and preventing economic crime.

This community includes law internal auditors…fraud examiners…regulatory officials…corporate security professionals…senior executives…private investigators…and many more.

The editors of *White-Collar Crime Fighter* strive to gather and compile the most useful and timely information on economic crime issues.

Comments, suggestions and questions are welcome. Please fax us at 203-431-6054, or E-mail us at editor@wccfighter.com. Visit us on the Internet at www.wccfighter.com.

what you received and not what the supplier is invoicing for, which may be inferior-quality goods, short quantities or excess quantities. Any suspicious discrepancies can thus be found at the point of infraction or at least at the point where an infraction can be first detected.

Key: By implementing software controls and data audits along with defined procedures and clear operation steps, the organization is not only more likely to detect supply chain fraud but also to deter fraud as well.

With formerly paper-based transactions now in electronic format, they can be efficiently audited and cross-checked for accuracy and integrity… and signs of fraud.

Key: This is a perfect example of the critical theory that fraud prevention is greatly influenced by the degree to which potential perpetrators perceive the likelihood of getting caught.

EASIER SAID THAN DONE

While supply chain fraud detection and reduction is a good risk management strategy, selling senior management on implementing an anti-fraud program may fall on deaf ears when it is viewed as simply one more expense on top of the organization's already costly risk management program.

Effective: Explain to top management that ERP systems, automatic identification and EDI are the actual backbones of supply chain operations and are used to increase accuracy and efficiency. Wrapping operations improvement projects with fraud detection and prevention programs is a smart combination that equates to a greater return on investment.

Fraud detection and reduction programs must exist within standard supply chain operating procedures so as not to disrupt or increase the cost of throughput and prevent employees from performing their jobs to the fullest.

***White-Collar Crime Fighter* source:**
Norman Katz, CFE, CFS, founder, Katzscan Inc. In January 1996 Norman Katz founded Katzscan Inc. (www.katzscan.com), a Florida-based consulting firm specializing in supply chain technologies and operations with a niche in supply chain vendor compliance. www.supplychainfraud.com.

INTERVIEWING INSIGHTS

Don Rabon, CFE, *Hamlet's Mind*

How to Begin a Fraud-Related Interview

One of the students in my regular interviewing training classes once said, "To me, the introductory phase of an interview is the most difficult. During that time, I am trying to establish rapport…seeking to get a 'read' on the subject…and trying to determine the best approach to obtain the information needed."

Conducting an effective interview in a fraud case is certainly not the easiest thing in the world to master. However, some segments of the interviewing process are harder than others and the student is right—the beginning is almost always the toughest!

SO HOW DO YOU START?

It might seem obvious to some, but the best way to break the ice is to use an open-ended question such as, "David, before we get started, if you will tell me about yourself."

Key: Initiating a fraud-related interview in this way cleans the proverbial slate, establishing a social framework for the interviewer and the interviewee by just talking.

Quickly showing the interviewee the palms of your hands and calling the subject by his or her first name as a preface to "before we get started, if you will tell me about yourself," is an extremely effective way to open the interview.

Reasons: Addressing the interviewee by name focuses his or her attention, while showing the palms of your hands indicates honesty and openness.

Moreover, the words "before we get started" tell the subject that the interview has not yet begun and prevents the subject from becoming prematurely defensive.

Using "we" in the opening phrase conveys the message that you've already established a collaborative relationship with the interviewee. By contrast, using "you" can easily establish a finger-pointing or accusatory tone which is especially unhelpful at the outset of an interview.

WHAT TO EXPECT

Though you're still in the very early stages of the interview, the opening response of the subject may reveal clues as to his or her innocence.

Important: How the interviewee chooses to describe herself can provide useful insight into her thinking and point to possible connections to motivations for committing fraud.

Example: A fraud suspect may describe himself by saying "Well, right now I'm taking care of my mother. She has been ill for the last several months and I am trying to help her get through this medical and financial crisis. I have sublet my apartment and moved in with her to watch over her and offset some of her expenses."

Key: If the interviewer is experienced in the area of fraud, he or she will be familiar with the Fraud Triangle whose element of Pressure explains that fraudsters often do what they do to relieve such financial problems as excessive credit card debt, loss of income due to unemployment, addictions to gambling or illicit substances, or unexpected life crises such as divorce…or, as in the example above, the onset of costly medical problems with a family member.

REVEALING SOMETHING ABOUT YOURSELF

Equally important for the success-

Continued on pg. 4

CARD FRAUD

Latest Facts and Anti-Fraud Strategies for Beating On-Line Credit Card Crime

Latest research from payment management company CyberSource indicates that after two years of declining losses to online fraud the trend reversed itself in 2011.

Details: Following losses of $2.7 billion in 2010, merchants reported an estimated total of $3.4 billion in online fraud losses in 2011.

Latest research from payment management company CyberSource indicates that after two years of declining losses to online fraud the trend reversed itself in 2011.

To enhance the effectiveness of anti-fraud measures, CyberSource offers these defensive measures:

•To optimize the manual review process, focus on how your reviewers can access information in the most direct way possible.

Helpful: Use a case management system that can consolidate all of the information relating to the order in one place. Provide a structured framework and checklist for investigating orders to your review team, which help to streamline the process and ensure consistency in dispositioning orders.

Also important: Measure the performance of your review team by looking at key metrics—such as orders reviewed per day, length of time in the queue, chargebacks from the manual review process by reviewer.

Aim: To identify areas for improvement at both the reviewer and team level.

•To focus the review team's efforts on truly questionable orders, maximize the number of automated decisions. Analyze the profiles of orders that are accepted during manual review and determine if there are common characteristics from which you could build effective "auto-pass" screening rules.

Rule of thumb: One-half of orders that are manually reviewed should be accepted. Order acceptance and rejection rates that materially exceed 50% often signal opportunities to shift more of the manual order evaluations to automated screening.

•To minimize overall chargebacks, take steps to reduce your exposure to "friendly fraud." Defined as a situation in which a customer disputes a legitimate credit card transaction, falsely claiming fraud or non-delivery of goods, friendly fraud is hard for retailers to identify and nearly as costly as criminal fraud.

Helpful: Clearly specified terms and conditions that the customer must acknowledge at the outset.

Follow this with other safeguards, such as confirmation E-mails, activation links or other online validations that require customer action.

Example: If your business is subscription-driven, send an E-mail to the address provided, with a link to activate the account.

Results: If the E-mail address is phony, then the fraudster will be unable to activate the account. Second, if the E-mail account is valid, once the activation URL is clicked, you have a trail that you can use in the event that the cardholder disputes charges.

Aim: To put yourself in a better position to deter fraud or re-present any subsequent chargeback.

•To optimize your fraud management operations, maximize automated order screening capabilities while streamlining workflow for your review team. Use a "decisioning" system that enables you to create screening criteria based on order attributes, as well as results and information provided from a host of verification and validation services.

Look for portals where case management systems are integrated with relevant third-party data sources. Reviewers should access one consolidated tool rather than having to leverage multiple systems.

Also effective: Define and measure your key performance indicators (KPI) throughout the fraud management lifecycle. Understand your performance baseline and objectives, so you can identify where you can fine-tune your fraud management operations. That which gets measured, gets improved.

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

2012 Online Fraud Report: Online Payment Fraud Trends, Merchant Practices and Benchmarks, from CyberSource, www.cybersource.com.

Continued from page 3

ful launch of a fraud-related interview is the interviewer's disclosure of carefully selected personal information.

Example: If the subject mentions that he spent a lot of time in a particular city or region and you are familiar with the area, state that you also "know the place well and have been there several times"…or something to that effect.

Aim: To continue building the foundation of rapport that is so critical to getting the subject to gradually open up and share details that are critical to the fraud investigation.

The more personal information you can get the subject to reveal, the easier it will be to coax incriminating or other incident-related details from him or her.

Once the subject has shared key details about her relationships with her parents and/or siblings…her experiences growing up and other key developmental and psychological characteristics, you can begin to build on this information to enhance the subject's "comfort level" to the point where he or she begins to divulge key details of the fraud.

Example: With regard to relating to the interviewee and building a "person-to-person" connection, the interviewee by now has provided a valuable list of facts on which to build. *Most of us...*

•Have a family that is functionally challenged to one degree or another.

•Have gotten in "trouble" in school or at home at least once during our childhood.

•Have at one time or another found it necessary to talk our way out of trouble by bending the truth.

Significance: By listening closely and getting through to what the interviewee is really saying, an interviewer should have no trouble identifying one or more life experiences or behaviors that he or she has in common with the subject and which can thus be used to establish the all-important impression on the part of the subject that you are both just two people talking.

Based on the personal information that has been shared by the subject to this point, you can develop an approach for launching into the "guts" of the interview. *Examples:*

•Write down the key points of the interviewee's self-description.

Continued on page 5

Continued from page 4

•Create an open-ended question for each key element of the subject's self-description.

Bottom line: In fraud-related interviews, no element is more important than the very beginning of the session. As the interviewer, you should strive to minimize the formality of the session from the very start. Instead, coax the interviewee to open up and reveal details about his or her personal background and personality.

The more personal information you can get the subject to reveal, the easier it will be to coax incriminating or other incident-related details from him or her.

Key: Every detail that the subject shares represents an opportunity for you to learn more about the subject and presents the potential for establishing a link between what he or she says and the actual fraud…and eventually to an admission of guilt.

All of this important "activity" typically occurs in the first several minutes of the interview…which is why it is so important that it be used to maximum possible benefit.

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

Don Rabon, CFE, former Deputy Director of the North Carolina Justice Academy in Henderson, NC. He currently teaches a series of interviewing courses and seminars throughout the country. His newsletter, *Hamlet's Mind,* is available by contacting Don at dwrabon@msn.com or 828-606-9167.

More from Rabon… Interviewing Skill Enhancement Exercise

Have an experienced interviewer observe you conducting an interview. Ask the person to provide honest, constructive assessment of your interviewing skills… with an emphasis on the first three minutes of your interaction with the interviewee.

Use the feedback from your expert to develop a plan to remedy any weaknesses he or she observed in the first few minutes of the interview.

Key: Becoming a better interviewer hinges directly on integrating best practices from others with more experience than you have.

PROTECTING BRAIN POWER

Paul McCormack, CFE, *Connectics*

Intellectual Property Protection in Today's High-Theft Climate

As some victim organizations can attest, theft of intellectual property* can do more damage than the theft of cash. An organization can find ways to boost sales to replace money that was stolen, but once a trade secret is no longer "secret," the damage is irreversible.

Many organizations look to the legal system to punish the individual or their employer who stole their trade secrets. Certainly, the courts can help. However, if your organization is unable to demonstrate that it had the appropriate protections in place, the courts may not look kindly on a claim of trade secret theft.

As some victim organizations can attest, theft of intellectual property can do more damage than the theft of cash.

Key: Be proactive! Invest the time and effort to protect your company's intellectual property.

Protecting your company's intellectual property requires three components:

***Component #1:* A legal foundation.** A qualified attorney can identify all of your company's intellectual property and help ensure that the appropriate legal protections are in place.

***Component #2:* An intellectual property (IP) theft prevention program.** Once the legal foundation is in place, protecting intellectual property on a day-to-day basis requires a multi-pronged approach. *An effective program contains critical elements including:*

☐ New-hire screening.

☐ Segregating and limiting access to the organization's intellectual property.

☐ Confidentiality agreements for new and existing employees.

☐ Data mining metrics to detect excessive access to protected data or printing activity.

☐ Robust investigation policies and procedures in the event intellectual property is stolen.

☐ Access to suitably qualified intellectual property theft prevention and investigation professionals.

***Component #3:* Ongoing threat assessment.** Protecting your IP requires commitment. As soon as your organization allocates less attention to protecting its intellectual property, the probability that it will be stolen increases dramatically.

LEGAL LABYRINTH

In addition to stringent federal trade secret protection laws, each state determines its own scope of protection granted to an organization's trade secrets. The courts regularly wrestle with how best to balance the need of the organization to protect its trade secrets with the rights of individuals to use the knowledge that they have accumulated during their employment to further their careers. There is no "bright line" that all courts look to in order to provide companies with trade secret protections. *However, typically courts will apply the following criteria:*

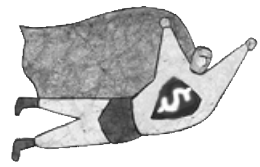
•Is the information kept secret?

•Is it readily accessible to all employees or only shared with those who have a defined business need to access it?

Continued on page 6

*Intellectual property (IP) is best defined as proprietary information owned by an organization, such as copyrights, trademarks (including product name(s), logo, slogan or package design), trade secrets (like a restaurant's secret recipe) and patents.

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Why Codes of Conduct Don't Stop Fraud …And How to [Potentially] Change That

In a recent article in *Compliance and Ethics Professional Magazine*, compliance and ethics expert Alexandre da Cunha Serpa points out that most corporate Codes of Conduct are way too lengthy and complex to be understood let along complied with.

Da Cunha Serpa further writes that organizations would serve themselves well by replacing their old Codes with what he refers to as a simple "Three Laws of Employee Behavior." *These laws are...*

- An employee may not injure his/her employing company or, through inaction, allow his/her employing company to come to harm.
- An employee must obey the orders given to him/her by his/her employing company, except where such orders would conflict with the First Law.
- An employee must protect his/her own job and personal interests, as long as such protection does not conflict with the First or Second Laws.

Problem: As has been discussed in previous issues of *White-Collar Crime Fighter*, most Codes fail not only because of their excessive length and complexity, but also because of their failure to specifically address the issue of fraud.

Fortunately, Da Cunha Serpa acknowledges that, "I have never suggested that the Three Laws of Employee Behavior are the ultimate solution to fraud or misconduct...and neither is any other code of conduct, ethical code…"

"An adequate compliance and ethics program, or fraud deterrence program, will need a lot of other components to properly achieve its objectives, but all of them will need to start with a set of expected behavior rules, to which I propose the simplest possible solution, the Three Laws of Employee Behavior."

Bottom line: Organizations must either scrap or simplify their Codes of Ethics or Compliance or Conduct…and supplement them with comparably simple but hard-hitting policies and procedures describing what constitutes fraud and what will happen to an employee should he or she engage in fraudulent conduct.

***White-Collar Crime Fighter* source:** Alexandre da Cunha Serpa is Country Ethics and Compliance Officer for Novartis Brazil, in São Paulo Brazil, writing in *Compliance and Ethics Professional Magazine,* www. corporatecompliance.org.

The E-Whistleblowing Trend

The traditional and the most popular method used by whistleblowers to report a fraud incident is the telephone hotline.

However, organizations have started to focus on additional options for capturing the information, with a particular focus on Web-based reporting.

Details: While Web sites have been a part of many organizations' incident capturing tools for years, they have picked up traction over the past two. In 2008, only 5.58% of all incidents were submitted within a Web form. By 2010 the figure stood at 8.31%. Based on preliminary tracking of data in 2011, that level is continuing to grow.

Prediction: For 2011, 10% to 15% of all incidents will prove to have been reported via a Web-based whistleblower form.

Reason: A younger workforce and its high comfort level with sending information through Web-based forms. As Generation Y continues to expand in today's workforce, the growth trend will continue, along with those for texting and social media.

Important: The increase in Web reports has not resulted in an increase in the number of tips being submitted. It will, however, have an impact on the data collected in whistleblower tips. While there are advantages associated with both types of tips, a person-to-person call typically results in the gathering of more detailed material that not only aids in determining the next steps associated with the incident report, but also a more familiar setting for the participant submitting the report, creating a more comfortable environment for them to reveal their identity.

***White-Collar Crime Fighter* source:** "2011 Corporate Governance And Compliance Hotline Benchmarking Report" published by The Network, leading hotline service provider, www.tnwinc.com.

- Is the information well known to individuals within the industry or profession that normally deals with this kind of information?

Example: Do employees at another company have a detailed understanding of what your organization deems to be "secret" information?

- Does the information provide the owner of the trade secret a competitive advantage because it is not known by competitors?
- Is the company able to demonstrate that it has taken reasonable steps to keep the information a secret such as requiring confidentiality agreements and limiting access?
- If the trade secret is stolen, is the company prepared to show that the accused had access to the information in question?

CASE STUDY

An employee intent on stealing intellectual property will always find the "path of least resistance." *Consider the following case…*

Beginning in 2008, Yuan Li, a former research scientist for the pharmaceutical giant, Sanofi Aventis, accessed, downloaded, transferred and subsequently registered 6,000 proprietary Sanofi chemical structures as the property of Abby Pharmatech. Li owned a 50% interest in Abby Pharmatech.

Sanofi subsequently discovered that rival Abby Pharmatech was advertising the stolen compounds on its Web site—including a number of compounds that were not yet in the public domain. Law enforcement later found a document on Li's laptop called "AbbyPharmatech," which contained a list of 144,000 compounds many of which had corresponding Sanofi control numbers.

Sanofi Aventis had taken a number of steps to protect its intellectual property including confidentiality agreements, conflict of interest statements, a code of conduct and invention assignment agreements. They frequently informed employees of the confidential nature of their work as well as restricted access to its facilities to those with a defined business need. They also required researchers to secure their lab notebooks under lock and key. Sanofi Aventis also maintained an encrypted document management system, and restricted access to its computer systems.

With all of these measures in place, how did Yuan Li manage to steal so

much of Sanofi Aventis' intellectual property?

Answer: Li transferred Sanofi intellectual property to her personal home computer by E-mailing the information to her personal E-mail address as well as saving company data to a USB thumb drive.

SELF-DEFENSE

How could Sanofi have prevented this damaging theft? *In addition to the three-part prevention strategy mentioned above, the following specific measures are essential…*

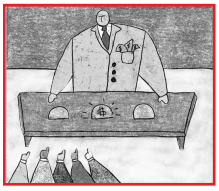
- Monitor all employee E-mails and internet access.
- Disable or block USB ports on the engineers' computers.
- Monitor employee access to servers.
- Track the number and type of documents printed by each employee.
- Install "key stroke" monitoring software on computers to log all entries made at each computer.

Challenge: There are no "silver bullets" to protect your intellectual property. *However, the following represent some of the best practices—in addition to those that Sanofi should have had in place:*

- Prepare an inventory of your organization's IP.
- Ensure that it is appropriately segregated and access is granted to only those with a defined business reason to have it.
- Develop threat analysis that identifies specifically which assets are most at risk of theft.
- Conduct a company-wide assessment of each department's ability to protect intellectual property.
- Conduct a physical security risk assessment of all facilities as well as key suppliers and outsourcing partners.
- Develop and deploy significant incident procedures to be followed in the event that intellectual property theft takes place.
- Ensure that the new employee hiring process does not inadvertently share intellectual property.
- Conduct training for executives, engineers and scientists regarding the fundamentals of IP prevention.
- Review confidential waste disposal processes and compare with industry best practices.

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

Paul McCormack, CFE, a partner at Connectics where he leads the firms' fraud practice. Paul is also former vice president of Fraud Detection for SunTrust Banks in Georgia. He can be reached at pmccormack@connectics.biz.



THE CON'S LATEST PLOY...

From *White-Collar Crime Fighter*'s files of new scam, scheme and scandal reports

Logan County, KY

Double billing scheme took dollars out of the pockets of new client's employees. Kevin D. Gettings was arrested after having allegedly embezzled over $220,000 from Gerald Printing starting in 2004.

According to the arrest warrant, Gettings was working as a sales representative for Gerald Printing in 2004. In that capacity, he negotiated an agreement with Houchens Food Group to print their retail store signs. Houchens is listed by *Forbes Magazine* as one of the largest 100% privately held companies in North America

A few months after closing the deal with Houchens, invoices began being paid by Houchens Food Group to "Printers Ink" for materials and services actually provided by Gerald Printing.

According to the warrant, the additional invoices being paid to Printers Ink were issued based on false information provided by Gettings to Houchens. Gettings told Houchens that Gerald Printing could not perform all the work they had agreed on and a second company, Printers Ink, would be used to complete the project each month.

From that point, Houchens paid both Gerald Printing and Printers Ink each month until June 21, 2011.

The total amount paid to Printers Ink by Houchens was $222,011.84, according to the arrest warrant.

Surprise, surprise: In textbook fashion, the warrant also states that an investigation of the case revealed that Printers Ink does not exist except for a PO Box and a bank account set up by Gettings. All actual physical work for Houchens was in fact done by Gerald Printing and the funds were being diverted to Printers Ink at the direction of Gettings.

The charge of theft by unlawful taking over $10,000 is a Class C felony in Kentucky and, if convicted, carries a minimum penalty of five years in prison and a maximum penalty of 10 years.

San Mateo County, CA

Mosquito control fraud. A former finance director for the county agency charged with protecting the public from mosquitos pleaded not guilty Friday to stealing more than $450,000.

Background: Jo Ann Dearman, otherwise known as Joanne Seeney, is currently in custody on a separate embezzlement case and $250,000 bail.

Co-defendant and former bookkeeper Vika Sinipata previously pleaded not guilty to the latest charges. Each woman is charged with eight counts of embezzling public money from the San Mateo County Mosquito and Vector Control District. The hefty loss discovered by an outside audit led to charges for Dearman and Sinipata but also questions of how the district overlooked Dearman's prior criminal history which includes two different embezzlement convictions.

District General Manager Robert Gay has since said the district is implementing new policies, including background checks, which were not in place when Dearman was hired in 2008. Prosecutors say Dearman, the district finance director, and Sinipata, her bookkeeper assistant and accounting supervisor, embezzled the funds between 2009 and 2011 by giving themselves extra pay at a higher pay rate, fraudulently awarded themselves paid time off, excessively contributed to their deferred compensation funds, used credit cards for personal purchases and electronically transferred money into their own accounts. The theft came to light after a boardmember questioned expendi-

tures in the district's pesticide account and was dissatisfied by the response from Dearman. The district hired outside auditors who reported more than $635,000 was missing, much of it in the last fiscal year. The district contacted the County Counsel's Office which in turn handed the matter to the District Attorney's Office for further investigation. The district's numbers might be closer to the actual loss but prosecutors are only alleging the amount they can prove, District Attorney Steve Wagstaffe said previously. At the time of Dearman's employment, she had been prosecuted in two different embezzlement cases, including one in which she ran up more than a half-million dollars on her boss's credit card. In March, she was sentenced to two years and eight months in prison on the two cases and ordered to pay restitution. The district plans to pay for the audit and forensic accounting costs, possibly up to $100,000, through insurance reimbursements and civil suits. At the time the district went public, authorities confirmed Dearman's alleged involvement but stayed mum on Sinipata because she had quit her job when the investigation launched and remained at large.

West Dover, VT

Another case of "crime pays." The Office of the United States Attorney for the District of Vermont stated that on January 12, 2012, Senior United States District Judge J. Garvan Murtha sentenced Sharon Johnson, 63, of West Dover, Vermont, to 37 months in prison for conspiracy to commit health care fraud. Judge Murtha also ordered Johnson to pay restitution to Mutual of Omaha Insurance Company in the amount of $1,395,755.42.

Johnson previously pled guilty to one count of conspiracy to commit health care fraud and mail fraud. As part of the plea agreement, Johnson admitted that she had obtained more than $1 million in fraudulent proceeds from Mutual of Omaha.

Mutual of Omaha discovered the fraud during a 2006 audit of its claims processing system, and referred the matter to the FBI. Subsequent investigation revealed that Rachel Lenagh, a then-employee of Mutual of Omaha, had paid almost $1.4 million in fraudulent claims to Johnson. Investigators also discovered that Lenagh processed payment to Johnson on claims for which there were no supporting medical bills or other relevant documentation, and that these fraudulent payments occurred at Johnson's direction.

On October 17, 2007, a federal grand jury sitting in Omaha, NE, returned a seven-count indictment against Johnson and Lenagh. Lenagh pled guilty in Nebraska to conspiracy to commit health care fraud and was sentenced on February 6, 2009, to 24 months in prison and restitution in the amount of $1,395,755.42.

The United States Attorney commended the FBI in Nebraska and Vermont and the United States Postal Inspection Service in Nebraska for their work in this case.

New York, NY

Guilty but not guilty of stealing big-league trade secrets. Sergey Aleynikov, a former Goldman Sachs computer programmer who was convicted of stealing proprietary code from the bank's high-frequency trading platform in 2010 and sentenced to eight years in jail, was out on bond in mid-February following an appeals court's reversal of the conviction. There was no accompanying explanation but the judges indicated that an opinion would be forthcoming.

Problem: The evidence against Aleynikov was strong. Goldman's attorneys were able to successfully argue that Aleynikov's alleged theft of the highly valued computer code was a direct violation of the Economic Espionage Act which protects corporate trade secrets.

Goldman reportedly paid Aleynikov $400,000 per year for his code-writing services. Another firm—Teza Technologies—reportedly lured him away from Goldman with an offer of three times what Goldman was paying him.

The appeal's court's forthcoming opinion could have significant bearing on the legal consequences of creating and handling the misappropriation of corporate secrets.

COMING SOON IN

White-Collar Crime Fighter...

- **Five overlooked facts about fighting fraud**
- **Detecting and preventing procurement fraud**
- **Information security strategies for non-technical decision-makers**
- **Locating hidden assets in fraud cases**