Strategies for Protecting Your Trade Secrets and Data from the Insider Threat – a Law Enforcement and Litigation View

Shena B. Crowe
FBI
Brooklyn Center

Teresa M. Thompson
Fredrikson & Byron PA
Minneapolis

Minnesota CLE's Copyright Policy

Minnesota Continuing Legal Education wants practitioners to make the best use of these written materials but must also protect its copyright. If you wish to copy and use our CLE materials, you must first obtain permission from Minnesota CLE. Call us at 800-759-8840 or 651-227-8266 for more information. If you have any questions about our policy or want permission to make copies, do not hesitate to contact Minnesota CLE.

All authorized copies must reflect Minnesota CLE's notice of copyright.

MINNESOTA CLE is Self-Supporting

A not for profit 501(c)3 corporation, Minnesota CLE is entirely self-supporting. It receives no subsidy from State Bar dues or from any other source. The only source of support is revenue from enrollment fees that registrants pay to attend Minnesota CLE programs and from amounts paid for Minnesota CLE books, supplements and digital products.

I. Introduction

A. Businesses face increasing threats to valuable trade secrets and other critical business information. The problem is exacerbated by a number of factors:

1. Business data is stored in a number of formats and locations and employees bring this data home.

2. Additional awareness is needed so employees understand the risks of storing business information on personal devices.

3. Many IT departments are unable to track when trade secrets or critical information leaves the company.

4. Foreign governments are targeting U.S. companies and their employees to steal trade secrets.

B. Trade secrets are valuable and the losses to companies can be significant:

1. A former Ford Motor Company employee copied 4,000 Ford documents onto an external hard drive that he took to China. Ford valued the loss at $50 million.

2. A DuPont research chemist whose work resulted in a proprietary chemical process sold the trade secrets to a Chinese university. DuPont valued the loss at $400 million and the chemist was sentenced to 14 months in federal prison.

3. A Valspar employee stole trade secrets and attempted to pass them to a paint company in China. The employee bought a plane ticket to China but was apprehended by the FBI and sentenced to 18 months in prison. Valspar estimated the value of the trade secrets at between $7 and $20 million. "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

C. Companies that invest in establishing a strong trade secret protection program - incorporating policies, procedures, and smart enforcement strategies will be in a better position to prevent company data disclosure or theft before it happens.

D. Companies that forge relationships with local law enforcement – before a breach occurs – will be in a better position to investigate and seek assistance from law enforcement should a theft of trade secrets occur.

II. Build a Strong Foundation for Your Trade Secret Protection Program

Building a strong foundation for your trade secret protection program will provide you the ability to better protect your information into the future. Taking these steps will also arm you with the evidence needed to support an enforcement action. There are several components to that strong foundation.

A. Identify Your Company's Trade Secrets.

You cannot protect your company's trade secret information unless you know what information might actually be a trade secret. Therefore, identification of the company's trade secrets is a key first step in building the foundation of your program. Once you have identified that information, you should also know where that information is stored or accessed, and what steps the company has taken to protect that information.

This is an important step when your company is looking to begin an enforcement action – whether civil or criminal. If you can't identify your trade secrets, or what steps you have taken to protect those trade secrets, your outside counsel, or the prosecuting attorney, will face difficult challenges in court.

1. Practical Takeaways and Checklist.

☐ Determine what information is confidential or trade secret.

- Is the information publicly available?
- Does the information give the company a competitive edge?
- Do the company's competitors know about the information?
- Would the information damage the company if the information is compromised?

☐ Determine who has access to such information.

☐ Determine where your company stores trade secret information.

☐ Determine what steps you have taken to protect that information.

- Do you have physical and electronic security measures? Examples include: access controls for the building and areas within the building, locked doors and cabinets, password protected files or encryption, ID badges for employees.

- Have you restricted where the information is stored or when employees can access the information?
- Do your employees label documents as confidential and trade secret?
- Have you limited access to confidential information and trade secrets to a discrete group of individuals who have a "need to know" in order to perform their jobs?

☐ Periodically review this information to make sure only confidential and trade secret information is being treated as such, that only those employees with a need to know have access to the information, and that the information is secure. This is an on-going process!

☐ If someone takes information, what tools do you have to prove they took it?

B. Use Appropriate Contractual Provisions.

Agreements protecting confidential and trade secret information, whether through confidentiality and non-disclosure agreements, or through noncompetition and nonsolicitation provisions, can provide great protection, but they can also be full of tricks and traps if not well-drafted or properly executed.

Multi-state employers are at especially high risk if their agreements are not well drafted because state law varies widely. For example, some states such as California and North Dakota prohibit non-compete agreements in almost all circumstances and many other states have unique and idiosyncratic laws limiting or restricting noncompete agreements. Evolving technology makes updating agreements important to ensure the company receives the benefit of the contract they believe they are entering into.

1. Key Agreements and Their Elements.

(a) Confidentiality and Nondisclosure Agreements. These agreements should be thorough and well-drafted in order to encompass all the information an employer seeks to keep confidential. In addition to binding employees to confidentiality agreements, companies should enter into nondisclosure agreements with suppliers, vendors, contractors, and other entities with access to trade secrets and/or proprietary and confidential information. Even well-drafted confidentiality and non-disclosure agreements won't always prevent trade secret theft. Cautious

and careful selection of which third parties a company shares its secrets with is also key.

Example: A company entered into a contract with a manufacturer that required the company to divulge certain proprietary technology. The agreement contained nondisclosure provisions. The CEO attended a trade convention and saw the manufacturer at a competitor's booth that was displaying the company's proprietary technology. The company sued and won $25 million in damages. *LBDS Holding Company, LLC v. ISOL Technology Inc. et al.*, 6:11-cv-00428, (E.D. Tex. Aug. 16, 2011).

(b) Noncompetition and Nonsolicitation Agreements. These agreements should be drafted in consultation with an attorney to ensure they are valid in the states where the company employs employees. These agreements also should be reviewed regularly to ensure that they comply with state laws.

(c) Assignment of Inventions. Assignment of inventions, whether as a stand-alone agreement or as a provision in a confidentiality or noncompete agreement, should define the scope of the employee's obligation to disclose inventions to an employer and define what kinds of inventions are assignable. The employer should ensure that when an invention is assignable, they receive total ownership of the invention.

(d) Return of Property. Each of the agreements above should contain a provision dealing with the return of company property. This provision should obligate an employee to return all company property, including documents, folders, reports, phones, computers, and other devices upon termination of employment. The agreement should reach all company property within the employee's control, whether the property is on company premises, the employee's residence, the employee's personal phone, computer, or other device, or any cloud-based storage that the employee has access to. The provision should also cover the deletion or destruction of any electronic copies of the information, with a carve-out provision for litigation holds.

2. Practical Takeaways and Checklist.

- ☐ Review the confidentiality clauses in your agreements. Have you sufficiently defined the company's confidential and trade secret information? Have you made clear that access to and use of such information shall be solely for the benefit of the company and not the employee?

- ☐ Include confidentiality clauses in employment agreements for those employees who will have access to confidential and trade secret information.

- ☐ Insure you are using a non-disclosure agreement with any third parties given access to confidential data is critical for protecting confidential information and trade secrets.

- ☐ Use non-compete agreements when appropriate. These agreements can provide enhanced protection to employers by creating barriers to competitive activity for departing employees and effectively prohibiting them from using the employer's trade secrets and confidential information for a competitor.

C. Implement Clear, Enforceable Policies Related to Authorized Use of Company Property.

Outdated policies may not protect your business. If you do not update your policies regularly (recommended at least annually), you run the risk of failing to protect against behavior or technology use that compromises or discloses confidential information.

Example: A company's policy stated that no emails were considered private or personal, and that the company had the right to review, access, and disclose all matters on the company's system. An employee used her company computer to access a personal, password-protected email account through which she emailed with her attorney. The company obtained the contents of the email via forensic imaging. A court determined that the company's policy was too vague to put the employee on notice that this type of personal email account would be accessed and read, and that accordingly, the employee had not waived the attorney-client privilege in the communications. The policy was too vague because it did not put employees on notice that the employer would review personal emails saved on a hard drive, or monitor the contents of, emails sent from a personal account. *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010).

1. Important Policies.

You will want to review the following policies:

(a) Electronic Monitoring. Without a policy putting employees on notice that they do not have an expectation of privacy in their company computer use, including internet usage, email, and access, employers may face higher risk if they later want to monitor employee communications via email, or employee internet use and other similar activities. An electronic monitoring policy that puts employees on notice of such monitoring is important. This policy must be carefully crafted, however, to avoid violating federal and state laws regarding electronic monitoring. Computers covered by the policy will also need to display a banner or "click-through" by which employees acknowledge the policy upon entry into the computer system.

Example: An employer violated the Stored Communications Act (SCA) by accessing an employee's password-protected personal email account via a company computer and reading the employee's personal emails. The employer's electronic monitoring policy was limited to "company equipment" and the court found that this did not permit access to emails stored on offsite servers, such as Google. *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

Example: A court permitted SCA claims to proceed where the employer accessed an employee's Facebook and Twitter account while the employee was on medical leave. The employee's passwords were stored on the company's servers; however, the employee had not given the company authority to access these accounts. The employer posted comments on the employee's accounts without her authorization or knowledge. *Maremont v. Susan Fredman Design Group, Ltd.*, 2011 U.S. Dist. LEXIS 140446 (N.D. Ill. Dec. 7, 2011).

(b) Electronic Use. All companies should have a policy that addresses the use of email, internet, and social media. This policy should extend the company's policies on harassment, discrimination, and retaliation to the employees' email, internet, and social media use. The policy should also prohibit employees from disclosing confidential information via email or social media but should make clear that the policy is not intended to infringe on

employees' rights to discuss working conditions (which is protected under the National Labor Relations Act (NLRA)).

(c) A Mobile Device or BYOD Policy. A mobile device or bring your own device (BYOD) policy can also be important. These policies should establish that employees have no expectation of privacy and the device is subject to employer electronic monitoring. The policy should also establish security measures, such as requiring employees to register the device, set forth reporting measures if the device is lost, and define appropriate use. The policy should also set procedures for how to "wipe" company information from the device when necessary, including a disclaimer that a remote wipe may destroy personal information stored on the device.

(d) Confidentiality and Trade Secret Protection Policies. In addition to policies focusing on electronic devices, employers should also implement confidentiality and trade secret protection policies that clearly define the types of information that the employer considers confidential and set forth expectations that employees not disclose or use this information unless authorized or in the scope of their employment. The policies should define confidential and trade secret information to include information stored in both paper and electronic format, and provide examples of appropriate and inappropriate uses.

(e) Removable Media. Whether as a stand-alone policy or incorporated into an electronic use policy, remember to have policy language addressing use of removable storage media, such as USB's, to prevent information from walking out the door. Decide whether you want to prohibit the use of removable storage devices to download company documents or other information without permission.

(f) Data Classification and Handling Policy. This policy provides definitions for classifying data and information that is created, stored, used, collected, processed or transmitted by the company.

(g) Social Media Policy. Include in the social media policy, language that outline expectations that employees should never externally disclose, discuss, publish or share data or information about the company's business, customers or employees. This includes casual comments about products, projects, and office

activities may result in unintentional disclosure of confidential information.

2. Practical Takeaways and Checklist.

- ☐ Review all policies that touch on protection of confidential information or that give your company the right to monitor and review an employee's actions while working on your company-owned devices.
- ☐ Implement an electronic policy that alerts employees that computers are company property and remind them that the company reserves the right to monitor employees' emails, internet, and computer use (i.e., that the employee has no expectation of privacy).
- ☐ Have a banner or click-through on employees' sign-in to a computer system or protected database.
- ☐ Insure you have protocols for monitoring employee data/conduct and follow them.
- ☐ Be smart about smartphones and employee use of personal devices when accessing Company data (implement appropriate BYOD policies, update your acceptable use policies).

III. Conduct Training for Company Employees About Why Protection of Information is Important and How Employees Can Protect Information.

Employees who understand what they must do to help the company protect trade secret information will be in a much better position to do so. Training provides you the avenue for insuring that employees know what information might constitute a trade secret, how the company's trade secret protection policies apply to them, what the employee can do to better protect company trade secrets, and how to report misuse of trade secrets.

A. Create a Culture of Confidentiality.

Creating a culture of confidentiality in your organization will help your employees better understand the importance of trade secret protection. The first part of establishing a culture of confidentiality is to "talk the talk." This means training employees and managers on how to protect confidential information and why it matters by explaining and giving examples of confidential and trade secret information.

Additionally, an employer should establish "dos and don'ts" regarding data security, focusing on both intentional and inadvertent disclosures as well as appropriate and inappropriate use.

Employers should also warn employees of the consequences of disclosure, which may include discipline, termination, and even legal action.

When thinking about a culture of confidentiality, go beyond the written word and establish a workplace culture that ***treats confidential information like it is actually confidential.*** This will help prevent inadvertent disclosures, as well as deter intentional ones.

The second part of establishing a culture of confidentiality is to "walk the walk." This means consistently treating confidential information like it is confidential. For example:

- Don't put trade secret information in the public domain – a company can waive its protectable interest by placing information in the public domain.
- Secure your files – for either physical or virtual files, employers should place these files in secure locations.
- Treat information on a need to know basis – companies should ensure that only the employees who need access have access.
- Employ additional security features – for example, you can consider employing security features from encryption to simple steps such as requiring employees to log out when they step away from their computers.
- Mark information CONFIDENTIAL – labels and watermarks reading "CONFIDENTIAL" or "TRADE SECRET" should also be used to identify protected information.

B. Practical Takeaways and Checklist.

- ☐ Train employees and managers on how to protect confidential information and why it matters by explaining and giving examples of confidential and trade secret information. Tell them who to contact if they think someone has violated the policies.
- ☐ Establish dos and don'ts regarding data security, focusing on both intentional and inadvertent disclosures as well as appropriate and inappropriate use.
- ☐ Include both a detailed outline of *what* information is confidential as well as *how* employees should handle that information.
    - Employees may be instructed to store "hard copy" confidential information in a secure location such as a locked drawer or file

cabinet and not to remove it from company premises without authorization.

- For electronic information, employees may be instructed to not store or save confidential information on non-company cloud-based storage or on personal media and to instead, only store or back-up information on a drive provided by a supervisor or manager.

☐ Warn employees of the consequences of disclosure, which may include discipline, termination, and legal action.

- Note that legal action can include criminal prosecution in addition to civil remedies, as in the case of a staff engineer at a medical technology company who was charged with claims under the Economic Espionage Act after allegedly downloading 8,000 files containing trade secret and other proprietary information. The employee was allegedly planning to leave the country with the information. *U.S. v. Maniar*, No. 2:13-mj-06085 (D.N.J.) (criminal complaint filed June 4, 2013).

- Know that there are outside resources available to you for training purposes and that the FBI can supplement your trade secret training.

☐ Provide training/refreshers on confidentiality. Give annual reminders regarding confidentiality and ideally have employees sign acknowledgments. Annual refresher training sessions also help to demonstrate to a court that the employer has taken active steps to protect confidential information.

☐ Tell employees what to do if they think someone has violated the policy.

IV. Make the Most of the Exit Interview

The exit interview can present a good opportunity to discuss return of property and find out an employee's new employment plans. An exit interview can also be an opportunity to discover some of the red flag behaviors outlined below.

A. Practical Takeaways and Checklist.

☐ Go beyond "soft" questions that ask about the employee's experience at the company.

- ☐ Ask open-ended questions such as, "What data do you plan to take with you?"

- ☐ Ask where the employee is going to work next and in what capacity. If an employee is honest, you will gain a great deal of insight into what potential exposure there may be. If the employee is vague or refuses to answer, this is a potential red flag.

- ☐ Consider your next steps, including involving your IT department to determine if information has already been taken.

- ☐ Ask the employee for all passwords for work-related computers, devices, accounts and files and then change the passwords.

- ☐ Conduct a return of property review, whereby the employee discloses all company information or devices in their control.

    - Set up a procedure for their return and set a deadline. Collect all keys, access cards, badges, company credit cards, and other property.

    - Have employees disclose what information they have in paper or electronic format on personal devices, in their home, or in cloud-based storage they have access to.

    - Offer assistance from IT staff in returning the information and wiping any devices.

    - At the end of the review and collection process, have the employee sign an acknowledgment that all company property and information has been returned.

- ☐ If the employee is subject to confidentiality and/or noncompete agreements, employers should remind the employee of their ongoing obligations.

- ☐ Review any separation or severance agreement to emphasize the obligation to preserve confidential information.

- ☐ Send the departing employee a letter reminding them of continuing obligations.

V. Put Yourself in a Position to Detect and Respond to Trade Secret Theft.

Employees take information in a variety of ways, from simply printing the information and taking it home to maliciously deleting or altering information. While not all instances of employee sabotage can be identified before or soon after it happens, watching for certain "red flag" behaviors can help identify problems before they result in major breaches of confidential information. Companies that have a process in place to better respond to those red flag behaviors, whether via electronic monitoring or other investigative methods, will be in a better position to detect trade secret theft and take action to prevent the employee from using or disclosing that information.

A. Potential Red Flags

(See: The FBI's publication on the Insider Threat: An introduction to detecting and deterring an insider spy. http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat)

In its Publication on Insider Threats, the FBI provides the following list of characteristics to look out for (this is a summary of the list – for the complete listing, please see the link above):

1. Personal Red Flags:

(a) Greed or Financial Need: (Excessive debt or overwhelming expenses), or vulnerability to blackmail (Extra-marital affairs, gambling, fraud.)

(b) Feelings of anger/revenge against the organization: This can stem from problems at work, a lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

(c) Divided Loyalty: does the employee have an allegiance to another person or company, or to a country besides the United States?

(d) Compulsive or destructive behavior, or family problems: drug or alcohol abuse, or other addictive behaviors, marital conflicts or separation from loved ones.

(e) Employment: Employees who are laid off, subject to a reduction in force, or are terminated. Similarly, employees who are passed over for a promotion, demoted, or are subject to a performance improvement plan.

In *U.S. v. Kibalko*, an ex-Microsoft employee who was charged with trade secret theft had received a poor performance review, and threatened to

resign over it unless it was changed, then proceeded to misappropriate information. The ex-employee was charged with leaking trade secrets to a blogger in France, including information on a pre-release version of an operating system. The ex-employee had uploaded proprietary software, including a pre-release software update, to his personal cloud-based storage account before leaking it. Case No 2:14-mj-00114-MAT (W.D. Wa. 2014).

2. Organizational Factors

(a) Information Handling: The availability of access to proprietary, classified, or other protected materials, or providing access privileges to those who do not need it. Not marking/labeling proprietary or classified information.

(b) Access: The ease that someone may exit the facility (or network system) with proprietary, classified or other protected materials, or the perception that security is lax and the consequences for theft are minimal or non-existent.

(c) Training: Employees are not trained on how to properly protect proprietary information.

(d) Working from Home: Undefined policies regarding working from home on projects of a sensitive or proprietary nature.

(e) Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.

3. Behavioral Indicators.

(a) Employees, who without need or authorization, take proprietary or other material home via documents, thumb drives, computer disks, or e-mail, or seeks proprietary or classified information on subjects not related to their work duties.

(b) Employees show an interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors, or an unusual interest in the personal lives of co-workers.

(c) Employees remotely access the computer network while on vacation, sick leave, or at other odd times, or work odd hours without authorization.

(d) Employees disregard company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

(e) Employees have unreported foreign contacts (particularly with foreign government officials or intelligence officials), unreported overseas travel, or take short trips to foreign countries for unexplained or strange reasons, or engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

B. Have Your Ducks in a Row on Electronic Monitoring.

Companies that have thought through a detection and response strategy will be in a better position to act and react immediately. This requires some work by several departments – including, legal, HR, security and IT.

1. Have your policies updated and in place. If your company intends to use electronic monitoring as a detection tool – then your company's electronic monitoring and/or electronic use policies must provide notice to employees that the company will monitor employee conduct while using company provided electronic resources. That policy should further remind employees they have no reasonable expectation of privacy in their communications.

2. Have a process in place to quickly implement effective electronic monitoring. Having a policy in place may not be enough. Companies that want to take action must also be able to implement electronic monitoring quickly and efficiently. To do so, this requires up-front work by your legal, security and IT teams. (See the checklist questions below to determine your readiness to effectively respond to a threat of trade secret theft).

C. Be Prepared to Conduct a Forensic Review.

Acting quickly can help identify breaches of confidential information and prevent loss of customers, trade secrets, or other valuable information. Additionally, courts look to see how an employer acted in response to a problem and if the employer acted quickly to protect its interests. However, companies must also be cautious not to alter or destroy evidence in the response process. If you have the internal IT resources – make sure that everyone knows about the need to adequately protect the data. When uncertain, have an external forensic firm on your short list to contact to conduct that review and insure that information is appropriately

A company that has preserved evidence has a much better chance of successfully enforcing its rights against an employee or former employee.

D. Know When to Involve Law Enforcement.

Law enforcement can play a significant role in your detection and response to potential trade secret theft. Knowing when to involve law enforcement and who to call is important. It is best to think about these issues before you are faced with a theft or suspected theft of trade secrets.

E. Practical Takeaways and Checklist.

If you have an effective detection and response strategy in place, you should be able to respond to the following questions:

- ☐ Do you know what kind of monitoring you would like to conduct?
- ☐ Do you have the IT resources to conduct effective monitoring?
- ☐ Do you have an approval process internally to validate the decision to monitor? Who gives final approval?
- ☐ Do you have employee consent to conduct that monitoring?
- ☐ Are there any privacy considerations you must consider in the jurisdiction where you want to conduct electronic monitoring?
- ☐ Do you need to obtain a forensic image of the data before doing any further investigation (and under what circumstances)?
- ☐ How are you going to review the results gained from electronic monitoring?

- Who are you going to monitor? (i.e. everyone, or, will you monitor on a case by case basis?) If you monitor on a case by case basis, what criteria have you chosen to use to "qualify" an individual for electronic monitoring?

- Do you have a relationship with local law enforcement? Do you know when you should contact law enforcement for assistance in your investigation?

VI. Take Action to Enforce Your Rights

Courts often look to see that a company has acted quickly to protect its confidential information. Oftentimes, pre-litigation steps may be enough to protect your information, but companies should be prepared to deploy a full range of enforcement measures in the case of serious breaches of proprietary and confidential information.

A. Pre-Litigation Steps.

1. A letter of continuing obligations reminds the employee of their obligation to keep information confidential even after the employment relationship ends. This letter can help prevent inadvertent disclosures and may dissuade employees who are considering disclosing information from engaging in the prohibited behavior.

2. A cease-and-desist letter can show a former employee that you are serious about pursuing protection of confidential information. Consider adding language regarding the return of any remaining company property and reiterating the former employee's post-employment obligations in a strongly worded way.

3. Consider sending a letter to the employee's new employer putting them on notice that the former employee owes confidentiality obligations to his or her former employer. However, act cautiously and with the advice of counsel in order to avoid claims for tortious interference.

4. Involve law enforcement early and where appropriate. If you know or suspect that a significant theft of trade secrets has occurred, contact law enforcement to discuss your investigation.

B. Litigation.

1. Civil litigation may involve bringing a variety of claims such as breach of contract, Computer Fraud and Abuse Act ("CFAA") and/or Stored

Communications Act ("SCA") violations, misappropriation of trade secrets (under state or federal law), misappropriation of confidential information, and breach of duty of loyalty.

2. Additionally, civil remedies are not the only option. In some cases, criminal penalties may be available under the CFAA and the SCA. If the employee's actions are severe enough, contacting law enforcement may also help to protect your confidential information and prevent damages.

(a) A staff engineer at a medical technology company was charged with claims under the Economic Espionage Act and trade secret theft after allegedly downloading 8,000 files containing trade secret and other proprietary information. The employee was allegedly planning to leave the country with the information. *U.S. v. Maniar*, No. 2:13-mj-06085 (D.N.J.) (criminal complaint filed June 4, 2013).

(b) A former employee at a headhunting firm was sentenced to one year in prison for violations of the CFAA, trade secret theft, and conspiracy after allegedly taking source lists and other trade secrets to set up a competing business. *U.S. v. Nosal*, CR08-0237EMC (2014).

VII. Conclusion

Despite technological advances and increasing threats to proprietary information, proactive companies can take significant steps to protect against intentional theft and inadvertent disclosure of its confidential and trade secret information.