Ten Actions You Can Take Now to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

Businesses face increasing threats to valuable trade secrets and other critical business information.

To combat those threats, we believe companies should invest in a strong trade secret protection program.

This includes development of appropriate policies, procedures, and smart enforcement strategies to help prevent trade secret theft or disclosure before it happens.

Fredrikson & BYRON, P.A.

In this guide, you will find 10 Actions you can take (right now!) to better protect your company's trade secrets.

Fredrikson & BYRON, P.A.

If you have any questions along the way about how to implement these 10 steps…

Contact one of the authors:

Teresa Thompson
612.492.7347
tthompson@fredlaw.com

Norah Olson Bluvshtein
612.492.7299
nolsonbluvshtein@fredlaw.com

Sten-Erik Hoidal
612.492.7334
shoidal@fredlaw.com

David Waytz
612.492.7401
dwaytz@fredlaw.com

Fredrikson & BYRON, P.A.

1

Action One:

Update Your Policies

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

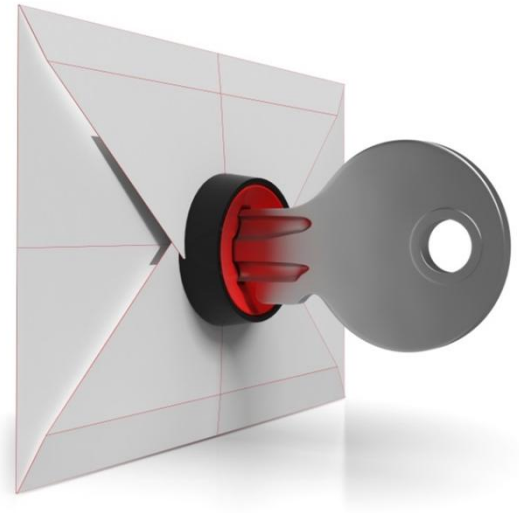
Fredrikson & BYRON, P.A.

The first step employers can take to prevent employee theft or improper disclosure of company trade secrets is to make sure relevant employee policies are current and up-to-date.

Why does this step matter? Well, for one thing, outdated policies fail to protect your business *and* they can really backfire.

For example, in *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), during the course of litigation with a former employee, a company hired a forensic vendor to obtain all data stored on a company laptop used by that employee. During her employment, the former employee had used her company computer to access a ***personal, password-protected email*** account through which she exchanged emails with her attorney.

The forensic image captured those personal emails and the company and its attorneys wanted to use the emails in the defense of the lawsuit. ***Unfortunately, the company's electronic use policy was found lacking***. The company's policy stated that no emails were considered private or personal, and relayed that the company had the right to review, access, and disclose all matters on the company's system.



Regardless, **the court found the company's policy was too vague** to put the employee on notice that a personal email account exchanging attorney-client privileged communications could be accessed and read (as compared to a work email).

- ✓ As a result, **the emails had to be returned**, they could not be used in the litigation and the court contemplated awarding sanctions against the company and its lawyers for failing to return the attorney-client privileged communications.

- ✓ Because the company's policy did not adequately address the company's right to monitor personal emails accessed on the company's system, **the company lost a key avenue to discover relevant evidence**. In a trade secret case, that source of evidence may have been critical, and the outdated policy language created a significant obstacle.

So if you are taking a look at the status of your company policies, which ones should you update? Key policies to be updated include electronic monitoring policies, IT acceptable use policies, and other policies that address the use of email, internet, social media and mobile devices (including “bring your own device” policies). Additionally, consider updating confidentiality and trade secret protection policies, and include a policy that addresses removable media, such as flash drives.

Lastly, to make sure your policies don’t become antiquated due to changes in technology, **we recommend that you review your policies from time to time (typically annually).**

This may not be rocket science, but having the foundation of up-to-date, comprehensive trade secret protection policies is an essential first step.

2

Action Two:

Get Your Agreements Right

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

This action focuses on protecting trade secrets through the use of employee confidentiality, nondisclosure, noncompetition and nonsolicitation agreements.

These agreements 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 employee confidentiality and non-compete agreements.

One item to keep in mind as it relates to confidentiality agreements, is that the desire to include everything but the kitchen sink in the definition of "confidential information" must be tempered by the fact that **if "everything" is confidential, then nothing is.**

Another wrinkle is that federal agencies, such as the Equal Employment Opportunity Commission (EEOC) and National Labor Relations Board (NLRB) **are attacking overbroad confidentiality provisions**, arguing that such provisions interfere with employee rights under federal labor and employment laws.

For example, in *Muse School CA v. Trudy Perry*, a NLRB Administrative Law Judge (ALJ) ruled that the MUSE elementary school's confidentiality policy violated the National Labor Relations Act (NLRA) because its prohibition against disclosing confidential information included not only MUSE trade secrets and confidential business information, but also information about MUSE employees and "compensation paid to MUSE owners and employees." This type of restriction, according to the NLRB, "suppresses" employees' right under the NLRA to discuss their wages and other terms and conditions of employment, and is unlawful.

Additionally, while the school argued that it could not have violated the NLRA because it never actually enforced the confidentiality language, the ALJ disagreed, **ruling that even maintaining such language is a violation** of the NLRA.

In *EEOC v. CVS Pharmacy, Inc.*, the EEOC attacked a severance agreement used by CVS Pharmacy, Inc. that included a confidentiality clause prohibiting the employee from disclosing confidential information without prior written permission of CVS's chief human resources officer. The EEOC argued that **this policy was unlawful because it infringed on employees' right to talk to the EEOC, participate in an investigation, and file a Charge of Discrimination**.

So, what does all of this mean?

In a nutshell, it means that having well-crafted, enforceable contracts in place with your employees is a critical part of any trade secret protection program.

Have you reviewed your contracts recently to see if they protect what you need them to protect, while not overstepping employee rights?

3

Action Three:

Create a Culture of Confidentiality

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

Creating 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.

A culture of confidentiality is also important when seeking to support a claim for trade secret misappropriation. **If an employer cannot show that it took reasonable steps to maintain the secrecy of its information, it may not be able to establish a claim for misappropriation.**

For example, in *Alpine Glass v. Adams*, 2002 Minn. App. LEXIS 1392 (Minn. Ct. App. 2002), an employer failed to provide employees a written policy prohibiting them from taking home confidential information and the company did not appropriately limit dissemination of confidential information. The court, noting that “an employer may not merely intend that materials be confidential,” found that **the employer failed to undertake any effort to keep its information confidential**. As a result, the employer did not have a protectable interest in information it believed was confidential.

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.

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).

The **second part** of establishing a culture of confidentiality is to **“walk the walk.”**

This means consistently treating confidential information like it is confidential.

- An employer can waive its protectable interest by placing information in the public domain.
- For either physical or virtual files, employers should place these files in secure locations.
- Employers should also ensure that only the employees who need access have access.
- You may also consider employing other security features from encryption to simple steps such as requiring employees to log out when they step away from their computers.
- Labels and watermarks reading “CONFIDENTIAL” or “TRADE SECRET” should also be used to identify protected information.

Finally, employers should **provide confidentiality training sessions** to employees with access to protected material to remind them of their confidentiality obligations and the importance of protecting the company's protected material.

The employer should also **give employees periodic reminders** regarding their confidentiality obligations, which the employees are then required to acknowledge in writing.

Ultimately, these steps will help an employer demonstrate in court that it has taken active steps to protect confidential information.

4

Action Four:

Be Smart About Smartphones

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

To prevent employee theft or improper disclosure of trade secrets, employers must be aware of the risks associated with smartphones and mobile devices.

When considering the use of mobile devices, a company should first decide whether to use **company-issued devices** or to allow employees to use their own personal devices (so-called "**Bring Your Own Device**" or "BYOD").

One clear advantage of **BYOD is that it reduces employer expenses** and may improve employee engagement. However, a company using a BYOD program runs the risk of losing control over confidential information and data if a well-drafted BYOD policy is not in place.

Additionally, if an employer terminates an employee who has been using their own device, there is a greater risk of misappropriation. **For high-risk employees or employees with access to a great deal of critical information, a company-issued phone may be best** because the employer retains the most control over the data on the phone.

In terms of how **to prevent employee theft or improper disclosure of company data via smartphone**, employers should implement basic measures, such as requiring employees to password-protect their phones, but they also should **consider additional protections**, including:

- Establish a policy that permits remote wiping of the phone when employment is terminated (or earlier if necessary).
- Limit the employee's ability to download apps onto the smartphone. Some apps may compromise the phone's security, and in turn, any confidential information.
- Establish procedures and checklists for ensuring the safe return of company devices. For example, when an employee returns a company phone, always verify the SIM card is still in place.

- Security breaches can occur through lost or stolen devices, so consider what information employees can access on smartphones, and how access can be limited in the case of a lost or stolen phone.
- Implement electronic monitoring and privacy policies that encompass smartphones and mobile devices.
- For employees who travel, consider policies that require encryption when traveling or that mandate use of a “clean” device that is devoid of critical or sensitive information.
- Mobile devices are ubiquitous in today’s workplace, and the risks they pose to a company’s trade secrets are significant. However, by implementing affirmative rather than reactive policies, employers can protect their data.

What policies and procedures does your company implement regarding mobile devices?

5

Action Five:

Watch Out for Social Media Pitfalls

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

Employee Social Media Use

Social media presents unique challenges related to the protection of confidential and trade secret information. For one, it's still a relatively new concept – at least as far as the courts are concerned – and the law is still trying to catch up.

For example, in *Cellular Accessories for Less v. Trinitas, LLC*, the company claimed a former employee's LinkedIn contacts constituted trade secrets and should be protected as such. In that case, however, neither the plaintiff nor the defendant offered any evidence of whether the employee's privacy settings were set to keep his contacts secret or not. As a result, it was impossible to determine the very basic concept of whether the information was actually a secret.

This demonstrates the need to be thoughtful about addressing how your company and your employees are using social media. For example, in this instance, **had the corporation prohibited an employee's ability to upload company contacts to LinkedIn via a policy or an agreement with the employee, it would have had a better opportunity to prove that it took steps to keep those contacts confidential.**

In addition to contacts being disclosed on LinkedIn, employees may either intentionally or inadvertently disclose confidential information on other forms of social media, such as Facebook.

For example, employees venting about work could disclose confidential product information, protected health information, strategic marketing information, or sensitive/non-public financial information.

Under most circumstances, we would not hesitate to advise an employer to terminate an employee who intentionally discloses trade secret information on social media. However, employers are smart to be wary of terminating employees for their social media activity because of the flurry of so-called "Facebook Firing" cases coming out of the National Labor Relations Board. Because employee posts that relate to an employee's terms and conditions of employment (as that is construed by the NLRB) may be protected, employers must tread carefully before terminating an employee for his or her social media post. That being said, employers must also balance that risk with their need to protect company trade secrets.

What would happen, for example, if an employee leaked trade secrets on his or her Facebook page but did so in the context of a group discussion about working conditions?

Better to think about this up front and provide some training to employees about why disclosure of trade secrets on social media could harm the company and result in disciplinary action or even termination.

Lastly, when investigating a leak of trade secrets via social media, employers should also be conscious of the requirements of various states' social media password legislation. **Those laws typically prohibit employers from asking employees for their login and password information**, but sometimes there are exceptions for workplace investigations.

It is best to consult legal counsel when there is any question about your right to access an otherwise private social media site.

How does your company balance the benefits of employees using social media to tout your company's products and brand with the risk that employees may provide too much information – including confidential trade secret information – in their posts?

6

Action Six:

Telecommuting Employees – Out of Sight Shouldn't Be Out of Mind

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

Telecommuting and Confidential Information

As technology advances, more employees are telecommuting – either full-time or sporadically.

To do their work remotely, **employees often need to be able to access and work on sensitive company information from their home office equipment**. Employees may also need to store confidential information in both paper and electronic format in a home office or on personal computers.

As a result of this, companies can lose control over protective measures that help limit improper access, storage and dissemination of critical and sensitive information by employees.

Additionally, when employees are in the office, they have very little expectation of privacy with regard to conduct engaged in on company systems, or in their office spaces. However, employees do have a reasonable expectation of privacy in their homes. As a result, if employees store information at home, those employees can make it very difficult for an employer to collect confidential information in the employee's possession after the employment relationship ends.

So, what can organizations do to protect themselves?

The first step should be to **look at your existing policies** – acceptable use, confidentiality, and electronic monitoring policies – **to ensure that they extend to telecommuters**. If they don't – revise them. You should also consider developing a separate telecommuting policy – to cover both those employees who telecommute full-time and those that work remotely from time to time.

The second step should be to **have every full-time telecommuter sign a telecommuting agreement**. In general, the ability to work from home is a benefit to the employee so outlining responsibilities of the employee when working remotely is reasonable and necessary. The telecommuting agreement will also help you outline expectations of the employee – including the actions you expect the employee to take to protect sensitive and confidential information. It should also outline whether the organization is going to provide the electronic resources necessary for the employee to work remotely (laptops, printers, internet access, etc.), or whether the employee is expected to use his/her own equipment.

As a third step, companies should look at security. If the employee uses his/her own equipment, you will want to **ensure that your network security policies and procedures extend to home computers and laptops** which connect to your systems. These network security features may include firewalls, anti-virus protection, secure networks, file encryption, secure remote connections, authentications, and passwords. Companies may also consider requiring remote employees to keep locked files and file cabinets and prohibit access to the working area by non-employees, including others who reside in the employee's home.

As a final step, companies should **consider how to retrieve property and files during and after employment**, and gain the employee's consent, in writing, for the employer to have the right to monitor and enter the home work area.

Are your "out of sight" employees also out of mind?
If so, consider reviewing the recommended steps above.

7

Action Seven:

Identify Red Flag Behaviors

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

How to Identify Red Flag Behaviors

Employees may 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**.

The FBI's publication, Insider Threat: An Introduction to Detecting and Deterring an Insider Spy, provides a list of characteristics to look for, including the following:

- Greed, financial need (excessive debt or overwhelming expenses), or vulnerability to blackmail (extra-marital affairs, gambling, fraud.)
- 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, etc.
- Divided loyalty – allegiance to another person, company, or country.
- Compulsive or destructive behavior, or family problems: drug or alcohol abuse, other addictive behaviors, marital conflicts, or separation from loved ones.
- Employees who are laid off, subject to a reduction in force, passed over for a promotion, terminated, demoted, or required to follow a performance improvement plan.

Similarly, organizational factors may play a role, including how information is handled, the ease of access to sensitive information, and training.

To highlight why identification of potential risks is important, review the White House report on the mitigation of trade secret theft from U.S. companies. The examples of trade secret theft noted in the report include the following:

- 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.
- 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.
- 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.

Do you agree with the FBI's assessment of red-flag behaviors?
Are there others that should be considered?
How does your company monitor and evaluate these types of behaviors?

Action Eight:

Make the Most of the Exit Interview

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

How can you make the most of this standard HR procedure? **The exit interview is a critical opportunity** to discuss return of property and find out an employee's new employment plans.

The following steps can help make an exit interview a strategic part of a plan to protect confidential information:

- ✓ Go beyond "soft" questions that ask about the employee's experience at the company. 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 can be a red flag**. If you obtain information that raises a red flag, then 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.

Exit Interview Checklist - Continued

- ✓ Have the employee disclose what information he/she has in paper or electronic format on personal devices, at home, or in cloud-based storage. 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.

- ✓ Create an IT protocol for terminating access to any company electronic systems (including when to cut off access) and follow it each time. This protocol should include any remote access to company systems – whether via a smart phone or laptop.

- ✓ Consider working with a mobile device management company to better control your smart phones, or use one of the many available mobile device management apps to better manage company data on any mobile devices, including remote wiping all company data from any mobile device upon termination. Again, a protocol should be set up to ensure that all devices with company information are wiped of company data.

- ✓ If the employee is subject to confidentiality and/or non-compete agreements, remind the employee of their ongoing obligations. Similarly, review any separation or severance agreement to emphasize the obligation to preserve confidential information.

- ✓ If the employee discloses the identify of his/her new employer and that employment appears to violate the employee's non-compete agreement, use the exit interview as an opportunity to remind the employee of any non-compete obligations and the company's intention to enforce such obligations.

- ✓ Immediately following the exit interview, send the departing employee a letter reminding them of continuing obligations to the company to honor any agreements – including the obligation to not use any company information.

Creating a process that your HR team follows during every exit interview will help you facilitate the return of company information whether that information has been purposefully taken by a departing employee, or if an employee has inadvertently retained company data.

Do you have proper exit interview procedures in place?

9

Action Nine:

Be Pro-Active and Preserve Evidence

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

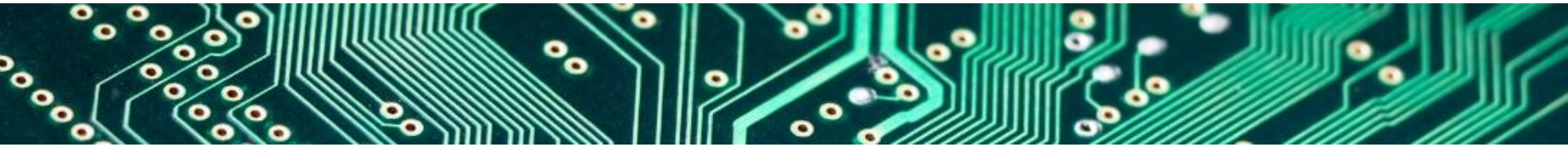
www.networkedlawyers.com

Fredrikson & BYRON, P.A.

The Importance of Being Pro-Active and Preserving Evidence of Employee Misconduct

Act Quickly

Acting quickly can help identify breaches of confidential information and prevent loss of customers, trade secrets, or other valuable information. Additionally, prompt action is critical in the event you seek injunctive relief because courts will expect and demand that the employer show it acted quickly to protect its interests before jumping into court.



Analyze Risk

If an employee resigns with notice, complies with an exit interview, returns all property, and is not going to work for a competitor, there may not be a significant risk of intentional disclosure or theft of trade secrets, but employers should still be wary. **Employers should also remember the potential for inadvertent disclosures.** **Ensure that the employee is reminded of their continuing obligations to protect confidential and trade secret information even after their employment has ended.**

Conversely, if the employee resigns without notice, refuses an exit interview or is vague about their future employment plans, be aware that these are all red flag behaviors. In situations like this, employers should strongly consider working with their IT folks (or better yet, a forensic vendor) to preserve evidence and investigate to determine if the employee downloaded, printed, or emailed any confidential information prior to giving notice.

By being pro-active and acting quickly, employers have a much better chance not only of winning in court on a trade secret misappropriation case, and also:

- ✓ **Discovering the theft much sooner in the process and containing the damage as much as possible**
- ✓ **Stopping the theft in the first place**

Has your business encountered an actual or suspected theft of trade secrets?

How did you respond? What could you have done better?

10

Action Ten:

Enforce Your Rights

Ten Actions You Can Take Now
to Protect Your Company's Trade Secrets

www.networkedlawyers.com

Fredrikson & BYRON, P.A.

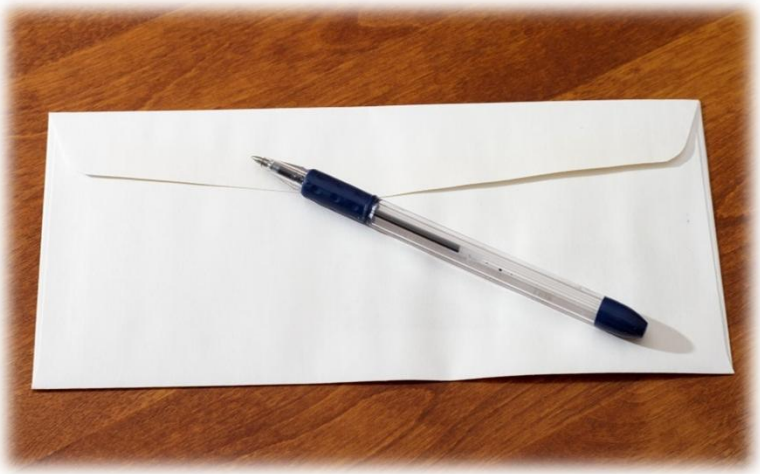
Legal Action Companies Can Take to Enforce Their Intellectual Property Rights

There are pre-litigation steps companies can take which may be enough to protect against improper use or disclosure of information, but **employers should be prepared to immediately deploy a full range of enforcement measures** when they discover a significant theft of proprietary and confidential information.

or

?

In terms of **pre-litigation steps**, **a letter of continuing obligations reminds the employee of the 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.



If you know an employee has your information, **a cease-and-desist letter** demanding that the employee return all company property, including any confidential or trade secret information, can show a former employee that you are serious about protecting confidential information.

Employers can also 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.

When deciding whether pre-litigation steps are appropriate, seek advice of counsel – sometimes you may need to move right into litigation in order to best protect your information.

If litigation is necessary, you may need to act quickly to obtain injunctive relief and stop the employee from using or disclosing your information.

Employers may be able to assert 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, misappropriation of confidential information, and breach of duty of loyalty.

Additionally, civil remedies are not the only option. **In some cases, criminal penalties may be available** under the Economic Espionage Act, the CFAA and the SCA, and other applicable statutes. If the employee's actions warrant, you may wish to involve law enforcement (federal or local) to help to protect your confidential information and prevent further damage. **If you choose this route, you should involve law enforcement as soon as you suspect your confidential information has been compromised.**

This concludes our ten actions- we've tried to highlight practical steps you can take to both prevent trade secret theft and enforce your rights.

We hope that you've found this information and our insights helpful for your organization.

Fredrikson & BYRON, P.A.

About the Authors

netWORKed Blog Authors Contributing to this Guide Include:

Teresa Thompson
612.492.7347
tthompson@fredlaw.com

Norah Olson Bluvshtein
612.492.7299
nolsonbluvshtein@fredlaw.com

Sten-Erik Hoidal
612.492.7334
shoidal@fredlaw.com

David Waytz
612.492.7401
dwaytz@fredlaw.com

For More Posts Like This...

Visit our Blog:
www.networkedlawyers.com