ARTICLES

Practical Steps for Addressing Employee Theft of Trade Secrets

Your client's former employee has stolen trade secrets—what do you do?

By John Duffey, Sarah Horstmann, and Ann Motl – April 21, 2022

This article aims to provide guidance to practitioners on how to advise their business clients on how to address theft of company trade secrets. If you are approached by a client with a former employee who has stolen company trade secrets, or with a new employee who is alleged to have stolen trade secrets from a former employer—how do you advise the client to proceed? This article provides practical steps to guide you through each scenario, from day one through potential litigation.

Scenario A: A Former Employee Has Stolen A Company's Trade Secrets.

Step 1: The client should gather information to determine the extent of the theft and establish that the information qualifies for protection.

The first step when one suspects that a former employee has stolen trade secrets or confidential information is to quickly gather information to determine the extent of the theft and establish that the information qualifies for protection. To begin, one should gather information about the former employee's company-issued electronic devices and accounts (including laptops, tablets, cell phones, and email accounts) and confirm that all devices have been returned and that access to company accounts and servers has been deactivated. The company should also confirm that all returned devices are preserved and sequestered and that they will not be altered, wiped, or reissued to another employee.

Next, one should review the employee's company-issued devices and accounts to determine the extent of the information stolen by the employee. For emails, you may want to review or perform searches of the past three to six months—or longer, if there is reason to believe that the employee was contemplating leaving the company earlier. To avoid altering data inadvertently, one should review the emails on the company server, if possible, rather than on the employee's laptop or other device. You may also want to suggest that the client perform a forensic review of the employee's company-issued devices to look for theft of trade secrets and confidential information. This forensic review will need to be conducted on an image of the device for preservation purposes, and therefore may need to be performed by an outside vendor if the client's company does not have this capability.

For guidance on forensic review of electronic devices, see the ABA's Business Torts & Unfair Competition Committee's Practice Points: *Forensic Examination of Electronic Devices*, Part 1 (March 18, 2021) and Part 2 (April 19, 2021). You may also want to work with the company involved to gather information about any personal devices and accounts the employee registered

on company systems or may have otherwise used for business purposes, to the extent that information is available, so that you can demand review of these devices and accounts.

To establish that the stolen information qualifies for protection, you will likely need to gather facts showing (1) why the stolen information is confidential, (2) what the company has done to maintain the confidentiality of the stolen information, and (3) how the improper disclosure of the stolen information would harm the company. Typically, you should be able to gather these facts through interviews of the employee's manager and colleagues. In these interviews, the company or interviewing lawyer should inquire about the employee's access to the particular information that was stolen, as well as the company's trade secrets and confidential information more generally. The company should also find out how the company has restricted access to this information, where it has stored this information (email, shared folders, hard copies, cloud-based storage sites such as Dropbox), and to whom the company has distributed this information.

You should also gather all company agreements with the employee (including any employee agreements, restrictive covenants, guarantee agreements, and severance agreements), as well as any other documents establishing the employee's duty to maintain the confidentiality of company information and return company property (including company policies, employee handbooks, exit acknowledgment forms signed by the employee, and post-termination letters).

Step 2: Send a demand letter.

Once you have an initial understanding of the extent of the theft of information and have established that it qualifies for protection, you should prepare a demand letter to the employee and, if applicable, the employee's new employer. You may want to attach as exhibits to the demand letter copies of any relevant agreements or documents establishing that the employee must return company property and maintain the confidentiality of company information along with, along with any written acknowledgment by the employee of these requirements. Your letter should also include the following demands:

- A demand that the employee identify (including by model and serial number as applicable) all personal electronic devices and accounts, including laptops, tablets, cell phones, email accounts, cloud-based storage accounts, and removable media (CDs, DVDs, USB drives, and external hard drives). You may want to limit this request to the devices and accounts that the employee used or accessed during a certain time range—for example the last six months or year of employment with the company—or, alternatively, the devices and accounts that the employee used in the course of performing work for the company or that the employee used to transmit or store any company information.

- A demand for third-party forensic review of the employee's personal electronic devices and accounts, including laptops, tablets, cell phones, email accounts, removable media, or cloud-based storage accounts. Alternatively, to avoid the time and expense of a third-party review, you might propose an informal process for the employee to perform searches of the devices, provide results, and delete information as necessary.

- A demand that the employee—and, if applicable, the new employer—preserve relevant communications, documents, and information.
- A demand for information about the employee's position with any new employer, including relevant details about the employee's responsibilities.
- A demand that the employee's work for the new employer be suspended until the matter is resolved.

Step 3: Consider options for litigation.

Hopefully, the former employee will comply with your demand letter and cooperate with your efforts to secure the company's trade secrets and confidential information. Should the former employee fail to do so, or should you learn that the former employee has inappropriately used or disclosed the company's trade secrets or confidential information, the next step is to consider litigation. The company may be entitled to bring one or more of the following types of claims:

- **Contractual**. If the former employee signed a non-disclosure covenant (or otherwise contractually agreed to protect the company's confidential information), you may have grounds to pursue a breach of contract claim.
- **Statutory**. Federal and state statutes protect trade secrets and provide a private cause of action to remedy misappropriation. If the former employee has stolen company information that satisfies the requirements for trade secret protection, the company may have grounds to pursue a trade secret misappropriation claim.
- **Common-law**. Many states recognize that employees owe their employers certain common-law duties, including the duty to protect the employer's confidential information. Importantly, these duties exist regardless of whether the employee has contractually agreed to protect the employer's confidential information. If your state recognizes these common-law duties, the company may have grounds to pursue a claim for breach of the former employee's duty of confidentiality (which is also sometimes referred to as the "duty of loyalty").

Scenario B: Your Client's New Employee Is Alleged to Have Stolen Information from a Former Employer

Step 1: Preserve and sequester information of the former employer.

The first step when a new employee is alleged to have stolen trade secrets or confidential information from a former employer is to discuss the allegations with the employee and ask the employee to identify all documents or information belonging to the former employer in the employee's possession, so that it can be preserved and sequestered.. The company also may want

to instruct the employee not to access any personal electronic devices or accounts that may contain the former employer's information.

In addition, depending on the nature of the allegations, the company might want to consider whether to suspend the new employee's access to company systems (such as email, intranet, and document storage systems), require return of company-issued devices, and cease the employee's job duties pending the investigation. The company should also consider searching its servers to confirm that the employee did not transfer any information of the former employer to the company.

Step 2: Gather background information regarding the employee's obligations to the former employer and your company.

You will also want to gather information from the employee regarding the employee's obligations to the former employer. This may include any written agreements with the former employer (including employee agreements, restrictive covenants, guarantee agreements, or severance agreements), and any additional documents that show a duty to return company property (including an exit acknowledgment form signed by the employee, or a post-termination letter from the former employer). The company should be cautious of any confidentiality provisions in these agreements that may impact its permission to view these documents.

The company may also want to gather any of its own company documents showing the employee's duty to return a former employer's trade secrets and confidential information before beginning work with the company, and the employee's promises not to have any trade secrets or confidential information of any former employer in his or her possession upon starting work with the company. Applicable documents may include the employee's employee agreement, guarantee agreement, employee handbook, or any representation signed at the beginning of employment in which the employee represented that he or she did not possess and would not use any trade secrets or confidential information of the former employer.

Step 3: Determine whether outside counsel will also represent the employee.

If the company has decided to engage outside counsel in an instance similar to this scenario 2, it will need to determine whether outside counsel will also represent the employee. Beyond a conflict of interest analysis, companies need to be prepared for a potential reimbursement request for attorney fees from employees. Many states have statutes requiring or permitting reimbursement or advancement of attorney fees, or both, for directors and employees, even those no longer associated with the company. *See, e.g.*, Del. Code. tit. 8, § 145; Cal. Corp. Code § 317; Minn. Stat. § 302A.521; N.Y. Bus. Corp. Law §§ 722–23, 725. Additionally, company bylaws may expand or limit any reimbursement requirements.

Step 4: Negotiate a forensic review.

If the former employer has demanded forensic review of the employee's personal devices and accounts, the company will need to decide if, and how, to proceed with that review, if any. One option is to propose an informal process for the employee to perform searches of the devices, provide results, and delete any information as necessary. If the company decides instead to agree to a third-party forensic review, it will need work with the former employer to select a vendor and prepare a protocol for the review that is narrowly tailored to the purpose of the review and preserves confidentiality and privilege. As noted above, the ABA's Business Torts & Unfair Competition Committee's Practice Points: *Forensic Examination of Electronic Devices*, Part 1 (March 18, 2021) and Part 2 (April 19, 2021), contain more information on forensic review, including negotiating a forensic protocol.

Conclusion

In sum, the practical steps above should serve as a framework to guide practitioners on how to advise their business clients when a former employee has stolen company trade secrets or if their new employee is alleged to have stolen trade secrets from a former employer. Surely, all of our clients hope this will never happen to their companies , but the retention of confidential information—both intentional and unintentional—by former employees is becoming more prevalent as our world becomes increasingly digital and mobile. Having a framework to guide your response will allow you to manage the situation as quickly and efficiently as possible.

John Duffey is a partner with Maslon LLP in Minneapolis, Minnesota. Sarah A. Horstmann is a shareholder with Fredrikson & Byron P.A. in Minneapolis. Ann Motl is an associate with Greenberg Traurig in Minneapolis.