Protecting Trade Secrets In The Remote Workplace

Insights
4.02.21

Since the COVID-19 pandemic began a year ago, employers have been forced to navigate rapid and ongoing changes to their operational landscape. Significant portions of the workforce are now in remote locations where employees are accessing company information on a daily basis, without in-person supervision and perhaps outside of the company network. While many of the changes associated with this paradigm shift have led to corporate sustainability and employee productivity, the new workplace is also creating significant challenges for protecting company information when remote employees leave the organization.

Take the currently pending *M3 USA Corp. v. Hart* case, which provides guidance for employers on protecting trade secrets with the loss of a remote employee, as well as associated jurisdictional issues to consider when commencing litigation against a remote employee. In this matter, M3, a Pennsylvania employer that provides research and support services to the health care industry, brought suit against Karie Hart, its former employee who worked from her home in New Jersey, and Atlas Primary Inc., Hart's new employer and M3's competitor.

M3's core allegations are (1) following Hart's resignation, she allegedly used her M3 laptop to misappropriate trade secrets and (2) Hart is soliciting M3 clients on behalf of Atlas and in alleged violation of her contractual obligations. Hart and Atlas, which is incorporated in Delaware and headquartered in Georgia, recently moved to dismiss M3's complaint for lack of personal jurisdiction.

The U.S. District Court for the Eastern District of Pennsylvania on January 29 granted the motion only with respect to M3's claim against Atlas for tortious interference with contract. The court otherwise denied the motion, determining that the court could exercise specific personal jurisdiction over all claims against Hart and all remaining claims against Atlas.

Takeaways On Jurisdictional Issues With Remote Employees

An understanding of the factual background is required: M3 is incorporated in Delaware and headquartered in Pennsylvania. When Hart applied for a position with M3, her resume listed her then-boyfriend's Philadelphia address even though she resided in Delaware. Prior to accepting employment with M3, Hart moved to New Jersey and worked remotely at her residence in New Jersey throughout her employment with M3. While she was employed at M3, Hart entered into two contracts. neither of which included a forum selection clause.

Having determined that the court could not exercise general personal jurisdiction over Hart, the court determined that it could exercise specific personal jurisdiction over Hart for all claims. Several points from the court's holding bear mention.

First, with respect to M3's breach of contract claims against Hart, the court analyzed whether Hart had purposeful contact with the commonwealth, whether the alleged breach of contract related to her contacts with the commonwealth, and whether exercising personal jurisdiction over Hart offended traditional notions of fair plan and substantial justice. In assessing this three-part framework, the court considered factors such as Hart using a Pennsylvania address when she applied for employment with M3; Hart having a key to access M3's Pennsylvania headquarters; Hart's travel to Pennsylvania for work purposes and her servicing of Pennsylvania customers; allegations that Hart misappropriated files from her M3 laptop, which she would return to M3's Pennsylvania headquarters; and Hart allegedly soliciting a M3 client that had operations in Pennsylvania.

Second, the court held that it could exercise specific personal jurisdiction over M3's claims against Hart pursuant to the Defend Trade Secrets Act and the Pennsylvania Uniform Trade Secrets Act because, as alleged, M3 would suffer monetary harm in Pennsylvania and Hart used her M3 laptop to access her Pennsylvania employer's information after her resignation.

Against this backdrop, the court's decision serves as a reminder for employers to consider jurisdictional issues that can arise with remote employees, particularly in the absence of a valid forum selection clause and for claims that may not be encompassed by a forum selection clause. In this remote world, employers should be revisiting their policies and contractual agreements with employees to ensure that such documents are carefully crafted to align with the remote workforce and, critically, to assess the pros and cons of including forum selection and consent to jurisdiction clauses and, if so, for what forum.

Takeaways For Trade Secret Protection

Hart was in possession of her M3 laptop for four days after resigning. M3 alleges that on the day after she resigned, Hart accessed files and folders on her M3 laptop pertaining to M3 clients, and that she also used a USB device on the laptop. M3 further alleges that on her first day of employment with Atlas, she continued to access M3 client files from the laptop before returning it to M3's Pennsylvania headquarters later in the day. M3 also alleges that Hart searched for pricing documents in the days leading up to her resignation, which would not have been required in the normal course of her job duties at that time.

While they are mere allegations at this point, M3's claims highlight the threat of trade secret misappropriation that employers are currently facing when a remote employee leaves the organization. In order to minimize the likelihood of departing employees engaging in this type of conduct and to minimize the risk of trade secret misappropriation, employers can consider taking several steps.

several steps.

1. Restrict Access

Take steps to ensure that company documents, files and folders are accessible to only necessary individuals and only when needed. Where the employee's use of a flash drive is necessary, an employer should issue a company-owned, encrypted drive to the employee. The company should maintain an inventory log of the devices that are issued, which will enable the company to know if the departing employee had one in their possession and whether one needs to be returned.

Employers may also want to prohibit employees from using their personal devices to access company data. Not only would this reduce the risk of data being stored on devices outside of the company's control, but it would also enable an employer to restrict the use of USB devices to those that are company-issued, encrypted, and that will only work on the company computer. From a collection standpoint, if an employee has only been using a company-issued device, then it will make recovering company information easier when the employee leaves the organization.

2. Proactively Work With Human Resources and Technology Personnel

Employers should work with their human resources and technology teams to establish specific procedures for handling the departure of a remote employee. By establishing procedures in advance, and ensuring that the human resources and technology teams know how to implement the procedures in the event of a departure, an employer will minimize the amount of time that the departing employee has access to company information. Some practices to consider:

- Maintain an inventory of devices that are in the possession of remote employees so that, upon termination of employment, the company will not be scrambling to determine what devices are in the employee's possession and risk the possibility of devices not being returned.
- Have procedures in place to ensure the immediate return of company devices that are in the remote employee's possession so that time is not lost in determining the logistics of the return.
- Establish a process for immediately disabling the employee's access to the company network, data and e-mail upon termination of employment.
- Prepare for employee exit interviews, with consideration being given to the topics to be addressed during the interview — e.g., reviewing the company information that was in the remote employee's possession, the process for purging/returning the information, and any additional post-employment obligations to which the employee may be subject) and to logistical issues for how the remote interview will be conducted.

Review Forensic Activity

M3 alleges that Hart accessed pricing documents immediately before her departure, which indicates that it performed a forensic analysis on her file activity. When an employee leaves the company, an employer should consider taking similar steps to review the employee's forensic activity to determine if they were accessing files outside of their normal role; if they were printing

activity to determine if they were accessing files outside of their normal role, if they were printing excessively, printing outside of the normal business hours, or printing highly confidential company information; and if they were emailing company information to a personal account.

Similarly, employers should review the employee's work devices to determine the employee's access to files stored locally on the devices and whether the employee used flash drives or other external data storage media on the devices.

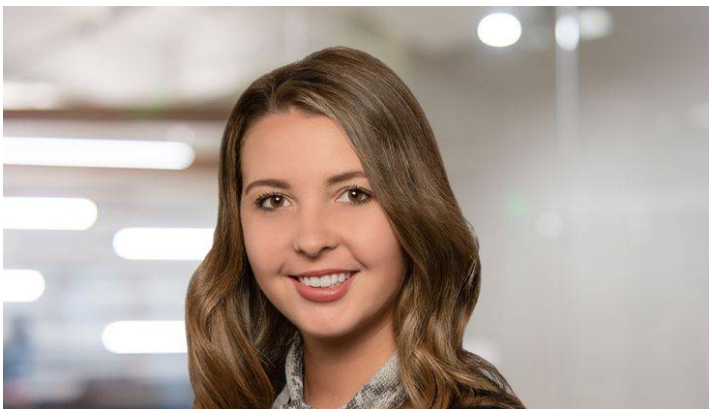
Conclusion

As the remote work era continues, whether through government mandate or if simply permitted by the employer, organizations will continue to experience the departures of remote employees. By taking proactive steps, such as those identified, employers can be in a better position to navigate departures when they arise and to protect their corporate interests.

This article originally appeared in Law360.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email



Kelsey E. Schiappacasse
Partner
610.230.2184
Email

Service Focus

Employee Defection and Trade Secrets

Trending

COVID-19/Vaccine Resource Center