KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Confidentiality Agreements, Trade Secrets and Working From Home, New Jersey Law Journal, authors Karol Corbin Walker, Krystle Nova and Reema Chandnani, March 11, 2022

With advancements in technology, working from home has become more prevalent. The COVID-19 pandemic exacerbated this trend when a large portion of businesses quickly transitioned their workforces to remote work. The shift to work-from-home disrupted many employers' protocols and practices for protecting confidential information and trade secrets, which exposed companies' sensitive information to a heightened risk of misappropriation by employees, as well as third-party hackers.

As a result of this forced work-from-home shift, many employers realized that productivity had not decreased and meanwhile cost benefits increased. Now, even as the COVID-19 pandemic becomes endemic, many employers plan to maintain full or partial remote work-from-home arrangements, at least for some of their employees in the future. While work-from-home does offer its unique benefits, the increased risk of information theft and cybersecurity threats are not going away, and it is important for employers and employees alike to understand what is required to limit their exposure when confidentiality and trade secret agreements are signed.

Both the Federal Defend Trade Secrets Act (DTSA), 18 U.S.C. §1836 et seq., and the New Jersey Trade Secrets Act (NJTSA), N.J.S.A. 56:15-1 et seq., allow employers to seek injunctive relief and damages for the actual loss suffered by the employer and any unjust enrichment enjoyed by the competitor as a result of any misappropriation, if certain criteria are satisfied. N.J.S.A. 56:15-3(a) and N.J.S.A. 56:15-4(a). A court may also award counsel fees and punitive damages—in an amount not exceeding twice that awarded for actual damages and unjust enrichment—in cases involving the willful and malicious misappropriation of a trade secret. See N.J.S.A. 56:15-4(b) and N.J.S.A. 56:15-6(a).

Because a hallmark of a trade secret is the necessity of shielding the information from competitors and the public, one such criteria is that the business has taken reasonable measures to maintain the secrecy of the information. See Sun Dial Corp. v. Rideout, 16 N.J. 252, 260 (N.J. 1954). A trade secret is misappropriated when it is: (1) acquired by a person who knows or has reason to know the trade secret was acquired by improper means; or (2) disclosed or used without express or implied consent. See 18 U.S.C. §1839(5). Therefore, if a business takes reasonable measures to maintain the secrecy of proprietary business information, and an employee or business competitor knew or should have known the information was obtained through improper means, then the employee or business competitor is liable for the misappropriation. Trade secret cases often turn on what a company did to keep its information secret. The more stringent measures a company puts in place to prevent misappropriation by members of its remote workforce, the more likely they are to prevail in seeking an injunction and other damages.

*For example, in one matter, the District of New Jersey held that an employer took appropriate measures in attempting to protect its proprietary business information. See Peoplestrategy v. Lively Emp. Servs., No. 320CV02640BRMDEA, 2020 WL 7869214, at *5 (D.N.J. Aug. 28, 2020), reconsideration denied, No. 320CV02640BRMDEA, 2020 WL 7237930 (D.N.J. Dec. 9, 2020). The plaintiffs in both of these cases applied for a preliminary injunction after their proprietary business information was stolen from former employees and another company (collectively "defendants"). In defending against the application for a preliminary injunction, defendants argued that plaintiffs waived any protections as they failed to "reasonably protect their confidential information" by allowing former employees to retain their company laptops which contained confidential information. The court disagreed with defendants' position. Instead, the court found that the company undertook reasonable measures, and ultimately granted the application for a preliminary injunction. Specifically, in addition to requiring their employees to sign confidentiality and non-disclosure agreements, plaintiffs also implemented a policy that prohibited employees from "storing company information on their laptops," requiring employees to return company information when they left, and employed a notice system that reminded employees of their obligation to keep plaintiffs' information confidential when they attempted to access information from the business' network. Id.*

The district court distinguished the Peoplestrategy matter from Maxpower Corp. v. Abraham, 557 F. Supp. 2d 955, 961 (W.D. Wis. 2008). In Maxpower Corp., the Western District of Wisconsin denied plaintiffs' application for a preliminary injunction. In making this determination, the court held that plaintiffs failed to take "reasonable measures to protect the confidentiality of [their] information." The only steps plaintiffs took to protect their trade secrets was to "restrict access to the facility and require passwords." The court was unimpressed and noted that these actions were normal business practices that all companies should implement regardless of whether

confidential information or trade secrets were at risk of being disclosed. The court's determination also rested on the lack of confidentiality agreements plaintiffs had with their employees, the failure to "emphasiz[e] the importance of keeping" proprietary information confidential, and the failure to have any procedures in place for employees to return confidential information when they separated from the company.

Furthermore, similar to Peoplestrategy, the Third Circuit held that a product company took reasonable measures to protect its trade secrets by implementing non-disclosure agreements in addition to "appropriate facility security measures." Par Pharm. v. QuVa Pharma, 764 F. App'x 273, 278 (3d Cir. 2019).

As discussed above, while confidentiality agreements provide some protection and should be utilized as a preliminary tool when protecting an employer's confidential information and trade secrets, these agreements alone will likely be insufficient in a potential misappropriation litigation.

Therefore, legal counsel should be consulted to assist in these measures, which include, but are not limited to, restricting employee access to sensitive information, marking confidential and proprietary information as such, requiring employees (especially certain employees with greater access to confidential information) to agree to confidentiality and post-employment non-compete agreements, prohibiting the removal of proprietary information from the workplace, implementing a notice system that identifies confidential information and the responsibility to protect same, and otherwise exercising reasonable diligence to maintain the secrecy of all proprietary information.

Although the following measures may not completely deter misappropriation by employees, they will increase employers' likelihood of prevailing in litigation that might ensue. They will also assist employees' understanding of their obligations under confidentiality agreements.

Remote Work Policies

Employers should provide employees a company policy that explains the employer's expectations about remote work and the handling of the company's confidential information. These policies should reinforce the employer's expectations and the employee's obligations of non-disclosure and/or confidentiality agreements. They should also emphasize that employees are required to take proper precautions to safeguard the company's secrets and other confidential information. Employers should require employees to sign off on these policies on a yearly basis. Additionally, depending on the size and resources of the company, these restrictions and notifications should include an email notification system that advises an employee when he or she is in breach of the company's policies. In that case, if the employee moves forward with sending confidential information externally, a company representative such as a member of the IT department, would get notified of the action. Internal remote work policies should also include trainings to advise employees of what is allowed, not allowed and how confidential information should be protected. Additionally, employers may want to consider banning the use of flash drives and personal cloud storage altogether. Limiting the number of storage repositories of sensitive data greatly helps to decrease the potential options by which an employee can misappropriate information.

Virtual Private Networks

Home wireless networks are much easier to breach than an employer's secure network because personal wireless networks usually have fewer security protocols in place. Employees accessing company servers remotely are generally granted access to a virtual private network (VPN). A VPN is a private, encrypted channel that will allow employees to directly access a company's network, while greatly minimizing the risk to the company's confidential information and trade secrets. VPNs are also beneficial as they allow employers to create and monitor remote workers' access logs that track files as they are opened, used and transmitted by each employee. VPNs also help prevent employees from downloading material onto their own personal hard drive.

Company-Issued Laptops

Issuing company-owned laptops to remote workers keeps sensitive information on company property and behind secure firewalls. The majority of misappropriation and unauthorized disclosures occur when workers take secrets and other confidential information with them to new jobs. Doing so becomes exponentially easier if the information is already stored on an employee's personal laptop that he or she is not required to return to the employer. Finally, keeping all work data on company-owned devices allows an employer to remotely "wipe" its information from the device immediately upon notification that an employee is leaving the company. If an employer issues computers or other electronic devices to employees, it must have a system in place for tracking these items. Further, employers should remind employees to secure any devices that contain sensitive data. For example, locking screens before stepping away from their computers or locking home office doors when the devices are not in use.

With the above preventative measures, an employer's likelihood of success before a court in enforcing confidentiality agreements that protect their trade secrets will substantially improve.

Krystle Nova *and* **Reema Chandnani** *are associates at Kaufman, Dolowich & Voluck, LLP, in Hackensack, and members of the New Jersey office's Labor and Employment Law Practice Group.*

Karol Corbin Walker, *is a partner with Kaufman Dolowich & Voluck, LLP in Hackensack, and Chair of the New Jersey office's Labor and Employment Law Practice Group.*