LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

WEDNESDAY, APRIL 11, 2018

PERSPECTIVE

Don't let trade secrets walk out the door with departing employees

By Travis Anderson and Paul Cowie

An employee abruptly quits your company to join a competitor or create a rival company. The employee had extensive access and made use of your company's confidential proprietary information while still at the company. What do you do?

From smart-car technology to key customer lists, it has never been technologically easier for an employee to take, retain and misuse employer data. But there are important steps that can be taken to both mitigate the harm and prevent future problems when an employee with such access leaves the company:

First, immediately disable the employee's access to all company systems, including emails and servers. Immediately recover all company property from the employee, including laptops, tablets, smartphones, thumb drives and physical files. Ensure the employee provides you with the passwords for those devices, and that the employee has no cloud accounts for those devices. If the employee does have a cloud account synced to those devices, you should inspect the account for company files and work with an electronic forensics expert to remove the employee's access to those files without altering the evidence.

Second, determine whether the employee downloaded any company information onto his or her personal electronic storage devices. Analyze the company devices and shared drives used by the employee to identify evidence of downloads to external devices, file transfers, and data erasures. It is best to use an electronic forensics firm to conduct this analysis and ensure that evidence is preserved.

Third, review the employee's company emails for evidence of an intent to misuse company data, including by examining the hard drives of all electronic devices used by the employee. For example, we have unearthed business plans, pitch declarations, and shadow customer lists, and a list of employees to target for recruitment in the new venture, all generated by the employee on company devices. Records such as these not only show an intent to compete against the employer, but an intent to do so unlawfully through the use of the company's confidential information. Determine what steps, if any, he or she was taking toward securing a competitive advantage at his or her next endeavor. Also look for evidence that he or she was sending company data to third parties, as this will reveal co-conspirators.

Fourth, send a letter to the employee demanding the return of all company property, including devices and files. The letter should also remind the employee of the obligation to not use or disclose any of the company's confidential information. If you have reason to believe he or she has transferred company information to other devices, demand prompt production of those devices for inspection. If you have reason to believe he or she has disclosed company information to third parties, demand the employee provide a detailed list of those disclosures and cease and desist from any further misuse. If the employee has a new employer, put the new employer on notice of these issues, and demand the employer take all reasonable steps to ensure it does not access or misuse company information.

Fifth, if the employee's response to your letter is anything other than an unequivocal and complete return of all company property, and a satisfactory assurance that the employee has not and will not use this information, consult with your counsel and determine what further interim measures are feasible and warranted before resorting to litigation. For example, counsel could contact any of the employee's associates/ potential business partners identified in the forensic analysis of the employee's devices, and urge them to refrain from misusing the company's information and immediately disclose whether they have any such information in their possession.

Sixth, if you conclude that informal measures are not sufficient to prevent the employee from misusing company information and engaging in unlawful competition, decide with counsel whether to seek a temporary restraining order and/or a preliminary injunction from a court to prohibit the employee from misusing company information and forcing the employee to return any company materials still in his or her possession. Doing so will require persuasive evidence showing the employee has company trade secrets in his or her possession, has misused them or intends to do so, and that the company will suffer irreparable harm unless the employee is prevented from any further misuse of trade secrets. This significant undertaking will require declarations of key witnesses, records showing improper retention or dissemination of company information, and may require expert testimony from an electronic forensic analyst. In considering the petition, the court will consider: (i) how likely it is that the company will prevail on the merits of its claims, (ii) how severe the risk of irreparable harm will be if the injunction is not granted, and (iii) what impact the requested injunction will have on the targeted employee. If the circumstances are especially severe and time-sensitive, a court may issue a temporary restraining order even without advanced notice to, or briefing from, the employee. In that situation, the court will then set a briefing schedule to allow both sides to fully brief the issue of whether a preliminary injunction should be issued, which could remain in place until the litigation resolves.

Last, but not least, use this serious event as an opportunity to review your company's internal policies and procedures to ensure sensitive information is being protected. For example, the employee handbook and all agreements signed by the employee should specifically define what constitutes the company's confidential, proprietary information, how that information must be safeguarded, and the restrictions on its use. Remember that information can lose its trade secret status unless a company deploys reasonable measures to protect the information from disclosure. To that end, company policies should detail each employee's obligations to keep that information internal to the company, to only use it for the benefit of the company, and to return and otherwise refrain from using it upon termination of employment. Employees with access to sensitive company information should be required to sign a non-disclosure agreement as a condition of employment. And review your company's employee exit procedures to make sure employees return all company property before leaving and sign a statement verifying that they have no longer have any company property in their possession, including data and copies of that data.

This list is just a primer, and far from exhaustive. It is critical to consult an attorney with expertise in trade secrets at every stage of this process.

Travis Anderson *and* **Paul Cowie** *are partners in Sheppard Mullin's Labor & Employment practice. They can be reached at tanderson@sheppardmullin. com and pcowie@sheppardmullin. com, respectively.*

ANDERSON

COWIE