LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Strategies For Protecting Trade Secrets Amid Tech Layoffs

By **Miriam Kim** (February 22, 2023, 4:27 PM EST)

Miriam Kim

With the recent spate of mass layoffs in the tech industry, it is important for companies to protect trade secrets. This article discusses the risks posed to trade secrets amid tech layoffs, as well as some steps companies can take to protect trade secrets when offboarding or onboarding employees.

Trade Secret Risks

Since the beginning of the year, approximately 375 tech companies have laid off over 105,000 employees, according to Layoffs.fyi, a website that has been tracking tech layoffs since the start of the pandemic.[1]

At the same time, a recent analysis of U.S. Bureau of Labor Statistics data by an industry trade group, CompTIA Inc., indicates that the tech unemployment rate fell to 1.5% in January, suggesting that many laid-off workers are being rehired.[2]

As employees move from one job to another in the tech industry, there is a risk that trade secrets do not remain secret. When thousands of employees are laid off, departing employees may intentionally or inadvertently retain trade secrets or confidential documents.

And when a competitor hires some of those employees, there is a risk that the employees will transfer or disclose trade secret documents to their new employer or use trade secret information in their heads.

Strategies to Protect Trade Secrets

Companies seeking to protect their trade secrets in this job market should keep in mind the required elements of a trade secret under the Defend Trade Secrets Act.

First, the owner has taken reasonable measures to keep such information secret. Second, the information derives independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[3]

To ensure the secrecy of trade secrets, companies should take steps to protect trade secrets when offboarding or onboarding employees.

Offboarding Employees

Here are some of the steps companies can take to protect trade secrets when employees are laid off or depart for other reasons:

Deactivate Access

Some tech companies have chosen to protect trade secrets by deactivating employees' access to company laptops, email, databases and accounts immediately prior to informing employees they are being laid off and potentially as early as midnight prior.

While it may be unnerving to discover you have lost system access and a job overnight, this is one practical way to protect the confidentiality of trade secrets when laying off a large group of employees. At a minimum, companies will want to deactivate a laid-off employee's access promptly upon their separation from the company.

Data Loss Prevention and Other Tools

Many companies utilize data loss prevention and other software in order to investigate suspicious activity, such as downloads of thousands of files shortly before an employee's departure.

Internet histories and other forensic evidence on a company laptop may also be used to uncover attempts to cover one's tracks, such as running a Google search for how to wipe a drive without leaving a trace, and then actually wiping the hard drive.

Confidentiality Agreements

Courts have held that requiring employees to sign a confidentiality agreement is a reasonable measure to maintain the secrecy of trade secrets. But the Federal Trade Commission recently proposed a rule banning noncompete clauses, which it defined to include a "non-disclosure agreement between an employer and a worker that is written so broadly that it effectively precludes the worker from working in the same field."[4]

While it is not yet clear whether the proposed FTC rule will be adopted and survive any legal challenges, companies may want to review the scope of any confidentiality agreement that applies to former employees to see if it defines confidential information so broadly as to serve as a de facto noncompete that prevents the worker from seeking or accepting work with a competitor.

Noncompete Clauses

While there have been increasing efforts to ban noncompete clauses, only three states — California, North Dakota and Oklahoma — currently prohibit employee noncompete clauses in all but limited circumstances, such as the sale of a business.

This means that some forms of noncompete clauses can still be enforced in 47 states. A company should consider whether it can use noncompete clauses as a way to prevent departing employees from misappropriating trade secrets.

Certification of Clean Departure

Companies should consider asking departing employees to certify that they have returned all company devices and returned or deleted all confidential documents obtained during their employment.

The certification can include a reminder to double-check all locations where electronic or hard copy documents may be stored, such as portable storage devices, smartphones, cloud accounts and boxes in a home office or garage.

Reminders of Confidentiality Obligations

Some laid-off employees have trade secret information in their memory that cannot be returned or deleted, such as a key process parameter or the confidential status of a forthcoming product. Therefore, it is a good practice to remind departing employees of their confidentiality obligations, including by giving them a copy of their confidentiality agreement.

Reminder Letters

If a company learns that a previously laid-off employee is now working for a competitor, it may want to consider sending a letter reminding the former employee not to use or disclose confidential information belonging to the former employer.

Onboarding Employees

Just as there may be a risk of trade secret misappropriation when employees leave a company, there may be risks when new employees join. Here are some of the steps companies can take to mitigate the risk of misappropriation when onboarding a new employee, particularly from a competitor.

Recruiting and Interviews

When recruiting competitors' current or former employees, it is important not to request, invite or encourage the disclosure of former employers' trade secrets.

A seemingly innocent question, such as "Tell me about an engineering problem you solved at your last job," could be misunderstood unless the interviewer cautions the candidate not to disclose others' confidential information.

Noncompete Clauses

A new employer may want to determine if a prospective employee is bound by an enforceable noncompete agreement that creates potential exposure for the company. In some states, a new employer may also consider asking prospective employees to agree to a noncompete clause to protect trade secrets for some period of time after the employee leaves the company.

Certifications of Clean Arrival

Companies should consider requiring new employees to certify that they have not retained any confidential documents belonging to a former employer. Incoming employees should be reminded to

double-check that they have not retained a former employer's confidential documents on personal devices, portable storage devices, cloud accounts and any other location.

Protective Agreements

Companies may consider requiring new employees to sign an agreement that includes a promise not to transfer, disclose or use a former employer's confidential documents or information during their employment.

Confidentiality Agreements

Employers should require new employees to sign a confidentiality agreement promising not to improperly retain, access, use or disclose company confidential information during or after their employment.

For the reasons discussed above, companies should be careful not to define confidential information too broadly. Pursuant to the DTSA, any agreement with an employee that governs the use of trade secret or confidential information should include a notice of the whistleblower immunity.[5]

Training

Training can be used to help incoming employees distinguish between information that can be a trade secret versus information that generally is not. Training may include practical examples relevant to the company's business, guardrails against misconduct and who to contact if you have questions.

Conclusion

These are just some of the strategies companies can use to protect trade secrets. The Sedona Conference's Trade Secret Working Group also offers additional guidance on how to protect trade secrets during the entire life cycle of the employment relationship.[6]

Even when companies adopt reasonable measures to protect trade secrets, employees may misappropriate trade secrets belonging to the company, a customer or a supplier. In the middle of mass layoffs, the risk of misappropriation is heightened.

If a company uncovers wrongdoing, it should send the individual a demand letter, work to recover company confidential information, and consider whether legal action is appropriate.

Miriam Kim is a partner at Munger Tolles & Olson LLP.

[1] https://layoffs.fyi/.

[2] https://www.comptia.org/newsroom/press-releases/comptia-restates-tech-jobs-report-to-clarify-bureau-of-labor-statistics-data-revision.

[3] 18 U.S.C. §1839(3).

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/p201000noncompetenprm.pdf.

[5] 18 U.S.C. §1833(b).

[6] https://thesedonaconference.org/node/10020.