FEBRUARY/MARCH 2024

A PUBLICATION OF LAW BULLETIN MEDIA

CHICAGO LAWYER

TRADE SECRETS

PROACTIVE PREVENTION

Why a robust trade secret program is critical

By JENNIFER KENEDY and JORDEN RUTLEDGE

In the era of heightened information mobility facilitated by artificial intelligence, cloud storage and remote work, the potential for proprietary company information to be illicitly accessed and misused has escalated. Protecting trade secrets in this environment is more important now than ever. A robust trade secret program prevents unauthorized access but also effectively positions a company for litigation in cases of misuse.

IDENTIFY YOUR TRADE SECRETS

The term "trade secret" can encompass nearly any type of information in any form, so long as it is secret, provides an economic advantage to the owner and is the subject of reasonable measures to keep it confidential, according to 18 U.S.C. Sec. 1839. A company attempting to protect its information through trade secret law should identify what can be classified as a trade secret.

By definition, a trade secret cannot be publicly known, nor can it be generally known within a particular trade. The trade secret must be defined with particularity at the time the secret was divulged. This follows the general principle that a would-be defendant must receive some notice of what activities to avoid.

The level of particularity required to establish a trade secret (and plead a claim) is a frequently litigated topic. Generally, courts do not find trade secrets that are vaguely defined or overly inclusive. In *IDX Systems Corp. v. Epic Systems Corp.*, the 7th U.S. Circuit Court of Appeals held that a description of underlying certain software features were too vague because the plaintiffs "effectively assert[ed] that all information in or about its software is a trade secret."

Courts disfavor catchall phrases, such as defining trade secrets as "including various combinations of the following …" Companies should, therefore, pinpoint information that holds (1) economic value, (2) is confidential, and (3) can be precisely defined. The company can then establish a routine system, overseen by supervisors, to periodically identify and communicate the company's valuable information. This will enhance employee awareness and the likelihood of succeeding on a future claim.

PROTECTIVE MEASURES

The law varies by jurisdiction, but the first line of defense in preventing unlawful disclosure is having employees sign agreements, which may include the following.

a) Confidentiality agreements: A robust but targeted confidentiality agreement (1) puts the employee on notice that they will be exposed to confidential information; (2) defines the confidential information with some particularity; (3) prevents unauthorized use or distribution of such information; and (4) delineates the steps to return confidential information at the end of employment.

b) Covenants not to compete: Although falling out of favor with the Federal Trade Commission, various courts and state legislatures "non-competes" prevent an employee from directly competing against a former employer. These agreements must be reasonably limited in time and scope. Generally, if an ex-employee is competing against an ex-employer by using trade secret or confidential information, courts are more likely to enforce a non-compete.

c) Non-solicitation agreements: Non-solicitation agreements prevent the departing party from soliciting clients, customers, or employees of the former employer for a specified duration. By signing such an agreement, parties commit to refraining from engaging in activities that may undermine the interests of their former employer, reducing the likelihood that an employee would divulge confidential trade secrets.

A trade secret protection program must include appropriate security measures. Although "absolute secrecy" is not required, Courts look at the totality of the measures taken to determine if they are reasonable.

With the rise of remote work, companies should have clear rules about cloud storage, as some programs allow users to seamlessly open and transfer documents between devices. By allowing such transfers, a company risks having a court find its security measures were too lax to maintain a trade secret claim.

The following are some examples of security measures courts would look at: requiring passwords to be frequently changed; monitoring employees' internet access and use; keeping logs of who accessed critical information; limiting access to confidential information to a "need to know" basis; encrypting information; implementing two-factor authentication; running semi-frequent security tests; and enforcement of policies regarding shredding of documents at home and return of information when employment ends. CL

Jennifer Kenedy is on Locke Lord's Executive Committee and a former firm vice chair and managing partner of its Chicago office. Kenedy has been lead trial counsel in trade secret misappropriation and other bet-the-company litigation nationwide. Email her at **jkenedy@lockelord.com**

Jorden Rutledge is an associate at Locke Lord LLP. He is on the firm's AI committee. He writes on trade secrets and artificial intelligence. Email him at **jrutledge@lockelord.com**