WILSON SONSINI

Trade Secrets: How to Protect These Increasingly Important Assets

Amy Candido (WSGR), Ariel Anaba (WSGR) & Galya Blachman (Enliven Therapeutics)

March 21, 2024

What Trade Secrets Do You Have?

Defend Trade Secrets Act

- Trade Secrets are "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:
  - (A) the owner thereof has taken reasonable measures to keep such information secret; and
  - (B) the information derives independent economic value, actual or potential, 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."

Examples of Life Sciences Trade Secrets

- Manufacturing processes
- Development research, including preclinical data
- Supplier lists
- Sales and distribution methods
- Consumer profiles
- Analytic tools and methods
- Cell culture media
- Drug formulations
- Drug delivery technologies

Trade Secret v. Patent Protection

- Using trade secrets to protect IP has the following advantages:
  - Does not require as much effort or uncertainty as pursuing patent protection, which can take years.
  - Trade secret protection does not depend on the AIA's "first-to-file" rule.
  - Trade secret protection can potentially exist in perpetuity, unless the trade secret loses its value or is disclosed.
  - Patents may only be issued for inventions that are useful and novel under section 101, but trade secret protection extends to broader categories of information.

- In light of the Supreme Court's recent decisions limiting the scope of patentable subject matter for biotechnology and pharmaceutical companies, trade secret protection has increasing attention. But, trade secret protection requires vigilance.

Assess The Risks to Your Trade Secrets

- External threats
  - Hackers, competitors, foreign governments
- Insider threats
  - Employees, corporate insiders
  - Remote working environment
- Potential acquisitions, business alliances or other transactional agreements
- Misappropriation as a result of theft, bribery, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means

- One study of trade secret cases from 1950-2008 found that in *85%* of the cases the alleged misappropriator was either an employee or business partner of the trade secret owner.
- A 2009 Symantec study found that *half* of employees who left their jobs kept confidential data of their former employers.

Take "Reasonable Measures" To Protect Your Trade Secrets

- Trade secret owners are required to take "reasonable measures" to maintain secrecy.
  - Courts assess what efforts are reasonable "under the circumstances" based on the nature and value of the trade secret, the ease of theft, the extent of the threat of theft, and the particular field of knowledge or industry.
  - What efforts are reasonable may differ based on the size and resources of the business.

- Security measures need not be "extreme and unduly expensive." But, courts expect reasonable steps specifically designed to protect disclosure of the trade secrets above and beyond "general protective measures."

- Companies should seek to strike a balance between the information security processes that will provide effective protection and legal enforceability of their trade secrets and other business realities, including cost, operational efficiency and information sharing demands necessary to drive innovation and support business operations.

Consider Identifying Trade Secret Information for Employees

- Consider defining in clear and simple terms what information is considered a trade secret and what is expected of employees who have access to that information.
  - Depending on the trade secrets, specificity may be appropriate in some cases, while broad categories may be sufficient in others.

- Courts emphasize the importance of advising employees of the existence of a trade secret as a "reasonable" measure to protect it.
  - In *United States v. Tien Shiah*, 2008 WL 11230384, at *18-19 (C.D. Cal. Feb. 19, 2008), the district court found Broadcom's security measures "barely satisfie[d] the standard of reasonableness," highlighting the fact that Broadcom's "overbroad" designations of information as confidential made it hard for employees to determine what information was actually confidential. The court stated that Broadcom should have made it clear to employees what information is a trade secret and how to handle that information.

Limit Trade Secret Access to Those With A Need to Know

- Employers should consider limiting access to trade secrets to only those persons, groups or departments with a ***"need to know"*** in order to do their jobs.
  - One study found that a court is over 18 times more likely to find reasonable efforts if the trade secret owner adopted "need to know" rules.
  - Similarly, not limiting access to employees with a "need to know" has been cited as evidence of a lack of reasonable efforts even where the company had nondisclosure agreements with its employees, because the alleged trade secret information "was readily accessible 'on a shared computer network' that 'could be reviewed by anyone who had access to the computer system'" in *Cumulus Radio Corp. v. Olson*, 80 F. Supp. 3d 900, 912 (C.D. Ill. 2015).

Use Passwords and Secure Logins To Access Corporate Networks

- When it comes to electronic trade secrets, courts look for password protection as a necessary condition to finding that reasonable measures were taken.
  - Some courts find passwords are "not enough" because passwords are "normal business practices in any business." Adding, "[a]n employer must use additional measures to protect the confidentiality of information he considers to be a trade secret." *Maxpower Corp. v. Abraham*, 557 F. Supp. 2d 955, 961 (W.D. Wis. 2008).

- Using passwords to limit access to specific employees with a "need to know" or to restrict access to particular systems, or specific drives, folders, files or even documents is cited approvingly as a reasonable measure.

- Password-protection increasingly involves password strengthening requirements, password renewal requirements, or multi-factor identification.

Consider Using Firewalls or Other Security Software to Protect Your Network

- Consider using firewalls or other similar security software to protect your trade secrets by creating a barrier between your trusted internal network and untrusted external networks, such as the Internet and your employees' various home networks.
  - Courts may expect even more sophisticated security measures for larger, more sophisticated businesses and businesses subject to known cyber-threats.
- Courts have cited firewalls, file transfer protocols, intrusion detection software etc. as "reasonable measures."
- Additional measures to consider, depending on the circumstances, include data loss prevention software, network segregation, avoiding aggregating trade secrets in a single centralized network location where a breach could be severely problematic, and stress testing to ensure that all systems and system security measures function properly.
- Consider encryption for any particularly high value trade secret information, such as any "secret sauce" technical information in a highly competitive industry where, if the information got out, the business would be severely damaged or destroyed.
- Consider monitoring employee access to trade secret information, whether by monitoring employee computer usage, network access or otherwise, as courts have cited this as evidence of "reasonable measures."

Consider Requiring Employees Working From Home to Use Secure Technologies

- Consider holding employees to the same standards for protection of company information working from home as when working from the office, and clearly communicate policies and procedures specific to working from home.
- Depending on each company's circumstances and the nature and value of their trade secrets:
  - Consider requiring certain minimum home security measures for home Internet, including password protection, multi-factor authentication, and a VPN or other encrypted/protected means to access the company's system
  - Consider requiring a company-sanctioned level of anti-virus software and anti-malware software with updates
  - Consider requiring all devices used for remote access are password protected, have hard drive encryption and remote-wipe capability
  - Consider restricting employees' network access to locations, segments etc. that the employees needs to do their job and consider restricting or prohibiting ability to download trade secrets
  - Consider imposing USB and other portable device restrictions
  - Consider imposing software app whitelisting or blacklisting to limit potential risks from untested or unknown computer programs
  - Consider using email filters to restrict communications from and to potentially risky or suspicious locations, to prevent transmission of particular files, and to guard against phishing or malware attempts that could risk trade secrets

Consider Marking Trade Secrets

- Consider whether it is feasible to consistently mark or otherwise label your trade secrets – for example, with a legend, label, footer, digital watermark or electronic tag on trade secret documents or files.
  - You may set up reminders that pop up every time an employee logs into the company's systems or a particular database to act as a reminder about the need to keep such information secret.

- Marking puts employees and others on notice that the information is a trade secret and is evidence the company took reasonable efforts to protect it.

- The lack of marking may be cited as a lack of reasonable efforts to protect trade secret information. However, if a company undertakes a program to mark its documents, but then fails to do so or does so inconsistently, that can be problematic. Inconsistent labeling may be cited by courts as undermining a company's secrecy efforts.

Consider A Written Trade Secret Policy

- Courts look for the existence of a written policy identifying what information the company considers to be a trade secret and how such information should be handled as evidence of reasonable measures.
  - *Menzies Aviation (USA), Inc. v. Wilcox*, 978 F. Supp. 2d 983, 995 (D. Minn. 2013) (finding reasonable measures not shown because, among other things, plaintiff did not provide defendant employee with "a policy designating the information as confidential")
  - *J.H. Wright & Assocs., Inc. v. Engerson*, 2000 WL 1848135, at *8 (S.D. Ala. Dec. 1, 2000) (finding reasonable measures not established where "written policy generally requiring confidentiality" did "not list manufacturer drawings or bill of materials as covered documents")
- Adopt clear policies on the use, sharing and management of confidential, proprietary, and trade secret information.
  - Prohibit access to trade secret information to only those employees with a clear ***need to know.***
  - Ensure employees understand what the company considers confidential, proprietary and trade secret information.
  - Address post-termination obligations.
  - Memorialize prohibition against using trade secrets of former employers.
  - Include clear BYOD policies, if allowed.

Consider Whether to Allow Employees To Use Personal Email or Personal Devices

- Whether to allow employees to use their personal email and/or personal devices for work can be a difficult decision as it may have significant cost savings, but is not without risks.
  - Some courts have cited an employee's use of his or her personal email, cellphone or personal computer for work purposes as evidence weighing against the employer's protection of its trade secret information.
  - But, other courts have found that employers used "reasonable measures" to protect their trade secrets, despite employees storing trade secrets on their personal cellphones or personal computers, where there were other protections in place.
    - Ex. Only employees with a "need to know" who had signed confidentiality agreements not to disclose the information.
    - Ex. Only employees who obtained approval from senior management first.

Consider Risks Posed By Generative AI Tools

- Whether to allow employees to use generative AI tools is another challenging question.
  - One solution to prevent the disclosure of trade secrets through generative AI is to prohibit the use of generative AI for work related tasks entirely.
  - Alternatively, employers may establish protocols to limit who can operate and interact with generative AI systems and/or limit what can be used as inputs.
  - Consider updating agreements, policies, handbooks, and related materials with guidance on the use of generative AI that employees are likely to use in the workplace.
  - Monitor and audit the use of AI tools in the workplace.
  - Employee training to raise awareness of risks and teach responsible use.

Consider Providing Comprehensive and Ongoing Training

- Consider training employees regarding information security, including identification of the company's trade secrets and how they should be handled, on a regular (at least yearly) basis.
  - May be a need for specialized training for particular groups with regular access to more sensitive or valuable information.
  - Training is an important "reasonable measure."
- An employee's level of exposure to trade secrets should influence the degree of training and protection obligations imposed on the employee.

Require Employees With Access To Trade Secrets To Sign Confidentiality Agreements

- Requiring employees to sign a confidentiality or non-disclosure agreement before providing access to any trade secrets is a critical reasonable measure.
  - The agreement should specifically describe categories of proprietary information and trade secrets, and include covenant not to improperly access, use, disclose or retain such information outside of or following employment.
    - May require time limit as to confidential information, depending on the jurisdiction and may be invalidated if too broad in scope of what it purports to claim is confidential.
  - Beware overly broad employee nondisclosure agreements, as they may be treated as restrictive covenants and not enforced. Agreements should not include general skill and knowledge or restrict future employment.
  - Beware including a marking requirement – if not followed by the company, courts may not protect the trade secrets.
- Agreement should also include requirements that the employee has not retained any information belonging to their former employer, will not disclose or use any information of their former employer and will abide by the terms of any agreements with their former employer.

Consider Employee Onboarding Protocols

- Consider establishing rigorous onboarding protocols for newly-hired employees to make sure they come in clean!
  - Do due diligence and, if needed, place employee in an area that may carry less risk.
- New hire training must reiterate obligations to protect former employers' confidential information.
  - Return all former employer's property.
  - Don't bring to the company any property of a former employer.
  - Don't use or disclose former employer's confidential information.
- Obtain signed certification that new employee attended the training.
- Instruct other employees not to communicate with the new employee about high risk subjects.
  - Consider using outside counsel to vet projects that pose particular risk and/or use a clean room for such projects.
- Special caution when hiring lots of employees from same company in a short period.
- Where warranted, periodically review and analyze the employee's email and computer activities through smart forensic searches in an attempt to ensure no contamination.
  - For example, not allowing new employee to "commit" code to the corporate "code bank" without careful review to assess its origin.

Consider Employee Offboarding/Termination Protocols

- Conduct exit interview reminding employee not to use (even from memory) or disclose the company's confidential information and that of any third parties to which the employee had access.
  - Retrieve company property and records. Obtain information on new employer.
- Send letter to departing employee reminding him/her to adhere to post-employment confidentiality obligations and asking him/her to certify (i) they do not have possession of, have not given and will not give any confidential information to a competitor and (ii) they have returned all company property, equipment, devices, and information.
- Promptly disconnect network, email and voicemail access of departing employees.
- Consider preserving forensic images of devices and accounts of departing employees who had access to confidential, proprietary and trade secret information
  - Preserve all equipment used to access the Company's systems.
  - Check emails to ensure that no confidential information was sent to a competitor/new employer or the employee's personal email.
  - If foul play is suspected, conduct a forensic exam.
- Consider letter to new employer advising of former employee's obligations and warning the new employer of the risk of permitting the new employee to disclose any confidential information.

Require The Return of Any Trade Secrets At the Termination of Employment

- Requiring employees to sign a confidentiality or non-disclosure agreement before providing access to any trade secrets is a critical reasonable measure.
  - The agreement should specifically describe categories of proprietary information and trade secrets, and include covenant not to improperly access, use, disclose or retain such information outside of or following employment.
    - May require time limit as to confidential information, depending on the jurisdiction and may be invalidated if too broad in scope of what it purports to claim is confidential.
  - Beware overly broad employee nondisclosure agreements, as they may be treated as restrictive covenants and not enforced. Agreements should not include general skill and knowledge or restrict future employment.
  - Beware including a marking requirement – if not followed by the company, courts may not protect the trade secrets.
- Agreement should also include requirements that the employee has not retained any information belonging to their former employer, will not disclose or use any information of their former employer and will abide by the terms of any agreements with their former employer.

Take Prompt Action If You Suspect Any Unauthorized Disclosure of Trade Secrets

- If you learn of, or even suspect, any unauthorized disclosure of trade secrets or breach of security protocols, you should take prompt action in response in order to protect your trade secrets and demonstrate "reasonable measures."
  - Ideally, you should have an Incident Response Plan to follow in the event of a disclosure or breach.
- If you delay too long in taking action against a potential misappropriation, a court may find that you did not take "reasonable measures" to protect your trade secrets and dismiss your claims.

Have and Follow an Incident Response Plan, If Necessary

- Investigate the facts immediately
  - Interview witnesses and obtain declarations
  - Gather and image computers, phones, USB devices, email accounts
  - Maintain chain of custody documents
  - Conduct a forensic analysis
  - Photograph workspace
  - Review printer logs
  - Analyze security video and entry and exit logs
- Retain counsel experienced in trade secret cases
- Consider sending cease and desist letter
- Consider involving law enforcement
- Determine the "trade secrets" at issue
- Consider promptly seeking an ex parte temporary restraining order or seizure order

Thank you

Amy H. Candido
Partner, San Francisco
acandido@wsgr.com
D: 415-947-2043

Ariel C. Green Anaba
Of Counsel, Los Angeles
aanaba@wsgr.com
D: 323-210-2985

WILSON
SONSINI