Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 38 • NUMBER 6 • JUNE 2026

Don't Wait for a Breach: Safeguard Trade Secrets Before a Legal Dispute

By Armin Ghiam and Andre Earls

In a significant legal battle between tech giant Apple and biotechnology company Masimo a federal jury awarded Masimo $634 million after finding that the Apple Watch infringed upon Masimo's blood oxygen monitoring patents. The case hinged on whether the health-tracking features were sourced from Masimo's trade secrets.

This verdict, one of the largest for consumer technology in the country, underscores the high stakes for IP creators and highlights the importance of proactively protecting trade secrets and patents. It demonstrates that clear documentation, vigilant enforcement, and a readiness to defend innovations in court can yield substantial remedies and act as a deterrent against potential infringement by even the largest industry players, encouraging other inventors and companies to safeguard their proprietary technologies from unauthorized use.

This article explores steps that companies can take to proactively protect their valuable trade secrets.

PROTECTING TRADE SECRETS

The process begins with identification and classification. Companies should conduct thorough internal audits to identify and document all valuable information that qualifies as a trade secret. Once identified, these trade secrets should be distinctly classified and labeled, differentiating them from other forms of confidential or proprietary information. It is advisable to establish task forces or committees dedicated to regularly reviewing and surveying the company's trade secrets, much like the processes many organizations use to monitor and protect their inventions.

Controlling access to trade secrets is essential. Access should be strictly limited to employees or contractors who need this information to perform their work. Organizations should implement robust physical security measures, such as locked rooms and badge access, alongside strong IT security controls, including encrypted drives, firewalls, and comprehensive access logging.

A cornerstone of trade secret protection is the use of confidentiality agreements. Every employee, contractor, or business partner who may be exposed to trade secret information should be required to sign non-disclosure agreements (NDAs) before any sharing occurs. Further, all employment and contractor agreements should contain clear confidentiality clauses specifically addressing trade secret information.

Employee training and well-defined policies reinforce these protections. Regular training sessions

The authors, attorneys with Hunton Andrews Kurth LLP, may be contacted at aghiam@hunton.com and aearls@hunton.com, respectively.

should be held to educate staff on the importance of maintaining secrecy and the consequences of unauthorized disclosure. Additionally, these sessions should emphasize reporting the creation of new trade secrets to management, as well as promptly notifying management of any breaches or misappropriation of trade secrets.

While having clear, written policies and guidelines is essential, it is equally important that these policies are presented in a format that employees can easily read, understand, and actually review. If policies are overly complex or inaccessible, they lose their effectiveness in communicating important information to employees.

Ongoing monitoring and auditing are critical for early detection and prevention of unauthorized access or leakage. Both physical and digital access to trade secrets must be monitored, and special attention should be paid to proprietary information such as formulas, algorithms, source code, and engineering designs. Regular audits of security protocols, employee compliance, and third-party access help ensure the effectiveness of these measures.

Managing third-party relationships is another key consideration. Contracts with third parties should clearly define responsibilities and set out remedies in the event of a breach. Additionally, vendors, partners, and consultants should be carefully vetted before any trade secrets are shared. Even the strongest contractual language may offer limited protection if a vendor is located in a jurisdiction where the contract cannot be enforced. In such cases, the effectiveness of the contract may be significantly diminished.

A well-developed incident response plan prepares an organization to react swiftly to suspected leaks or thefts. Such a plan should include protocols for investigation, containment, and legal recourse, and designate the chief legal representative as the point of contact for all data-related incidents.

Exit procedures must also be robust. When an employee leaves the organization, an exit interview should remind them of their continuing obligations regarding trade secrets. All access to company systems must be revoked immediately, and any devices or documents containing trade secrets should be recovered or destroyed.

Finally, legal protection and enforcement round out the strategy. Trade secret protection strategies should be regularly reviewed and updated to comply with relevant laws, such as the Defend Trade Secrets Act.[1] Organizations must be prepared to enforce their rights in court if misappropriation occurs, including seeking injunctions and damages where appropriate.

CONCLUSION

By integrating these steps, companies can create a strong foundation for trade secret protection, minimizing risk and ensuring they are ready to defend their valuable information when needed.

Note

1. 18 U.S.C. § 1836.