Now More Than Ever, Automakers Must Protect Trade Secrets

Posted in Alert on September 10, 2021

AS FIRST PUBLISHED BY *LAW360* ON SEPTEMBER 9, 2021

Automotive companies can expect more complex trade secrets disputes in the future, and should prepare in advance to deal with them. With all the new vehicle technologies being developed by an increasing array of competitors, coupled with supplier consolidation and employee transience, confidential and proprietary information is more valuable than ever — and at greater risk than ever.

This is likely to lead to more offensive and defensive trade secret misappropriation claims of growing complexity, including those with and without merit. Sophisticated automotive companies will plan accordingly.

Automotive Trade Secrets

Whether you are a manufacturer, supplier, retailer, remarketer, software provider, lender, charging company or transporter, and whether you are working with electric vehicles, autonomous vehicles, artificial intelligence, advanced driver-assistance systems, customer relationship management, digital retailing or other trending automotive technology, it is highly likely that your intellectual property, as broadly construed, is one of your most important business assets — and that it will be increasingly at risk of exposure in today's rapidly evolving supply chains.[1]

Leaks can occur through nefarious means, like corporate espionage, bribery and intentional breaches of confidentiality. But they can also occur accidentally, through negligence and oversight, and still cause great competitive harm.

Recent high-profile trade secret disputes in the auto industry abound. For example, Tesla Inc v. Khatilov, a case in the U.S. District Court for the Northern District of California that was settled last month, concerned a Tesla software engineer alleged to have stolen 26,000 files of code that automated a broad range of business functions.[2]

Faraday & Future Inc. v. Evelozcity Inc., decided by the U.S. District Court for the Central District of California in 2018, concerned the alleged theft of $1 billion worth of electric vehicle artificial intelligence.[3] And in Eagle Harbor v. Ford, a case decided in 2011 by the U.S. District Court for the Western District of Washington, Ford prevailed at trial on a counterclaim that the plaintiff's patents were crafted on confidential technical documentation obtained from a Ford supplier.[4]

Obviously, certain IP can be protected through advanced formal registration in the form of patents, trademarks and copyrights. But there remains a large subset of valuable confidential information that cannot be adequately protected through one of those mechanisms for technical, cost and/or timing reasons.[5]

Nevertheless, legal protection can still often be built around that information under federal and state trade secrets law. And the protection can last indefinitely, as long as the information remains secret and valuable.

A trade secret is any business information that is subject to reasonable efforts to preserve its confidentiality, and has independent value because it is not known or ascertainable to the public.[6] For automotive businesses, this might include undisclosed software code, battery component formulas, AI deep learning data sets, manufacturing processes, customer lists and research and development reports.

Trade secrets used or intended for interstate commerce are generally protected by the federal Defend Trade Secrets Act, or DTSA, which provides for a civil action in federal court for most instances of trade secret misappropriation.[7] The DTSA also allows for ex parte seizure orders, injunctive relief and expanded damages in certain cases, including potentially unjust enrichment, exemplary damages, royalties and attorney fee awards.[8]

Likewise, most states have adopted a version of the Uniform Trade Secrets Act, which has overlapping coverage, and allows a private state action for injunctive relief and various categories of monetary damages, subject to state-specific variation.[9]

Any potential trade secret claim by or against your company should be promptly evaluated. Usually, time is of the essence in limiting the competitive harm and/or resulting damages.

Importantly, there are prudent steps any automotive company should take before a dispute arises to prevent trade secret disclosures — and, by the same token, to improve its claim to trade secret protection if an unauthorized disclosure nevertheless occurs. Here are a few

of the most effective actions to consider:

Trade Secret Audits

A savvy automotive company will regularly review and categorize its most valuable trade secrets, perhaps as part of a broader IP audit. This would at least include:

- Identifying the company's valuable secrets;
- Documenting their actual and intended use;
- Mapping the historic and planned disclosure of that information within and without the company;
- Confirming that appropriate confidentiality or nondisclosure agreements are in place with those parties covering the relevant secret(s);
- Verifying that appropriate security restrictions are in place to track who accesses secrets and when and to prevent unauthorized access, including both physical protections (e.g. door/file locks, electronic key cards, etc.) and digital hurdles (e.g. passwords, encryption, etc.); and
- Confirming that the company has thorough written policies restricting access to and use of secret information to narrow need-to-know situations.

Vendor Vetting

Automotive businesses should pay special attention to third party suppliers and vendors with whom trade secret information needs to be shared. Such parties may have similar relationships with competitors, overlapping production lines and somewhat lower incentives to rigidly protect your trade secrets.

Certainly, they should be interviewed carefully on those topics prior to engagement, and likely be put under robust NDAs that not only protect your trade secrets from disclosure, but also segregate competitors' secrets from your products and personnel. A defensive trade secret claim can be just as damaging and disruptive as an offensive one.

There are many considerations for such an NDA to improve your future litigation or arbitration position. Most notably, the company will want to define protected confidential information in a sufficiently broad way to cover truly valuable known/present and unknown/future proprietary information, but not so broadly that the concept loses all meaning and cannot be enforced by a court.

Additional terms to consider are: favorable choice of jurisdiction and venue for any dispute; damage enhancements/limitations; attorney fee shifting; contractual limitations period to lengthen or shorten the statutory period;[10] choice of law; streamlined injunctive relief procedures or standards; self-help information seizure rights; and potential incorporation of statutory definitions (e.g., from the DTSA) for trade secrets, misappropriation, etc.[11]

Personnel

In a similar vein, employees and contractors with special access to, or roles in, the creation of trade secret information should be considered for NDAs, and should sign appropriate IP restriction policies. This should be made a routine consideration for new hires, and should include clear representations that the new employees are not bringing, and will not use, any secret or sensitive information from prior employers.

Departing personnel should have their access to confidential information cut off immediately, should be carefully interviewed about any confidential information they may have, and should be asked in writing to return all such information.

Then, where necessary, their new employers might be put on notice of their prior access to sensitive information, and warned not to use or allow use of it — perhaps with a formal request for such assurances. And, again, each of these tools should be reviewed periodically as part of the regular trade secrets audit discussed above.

Conclusion

Courts will generally help those that help themselves. In the trade secrets context, that means requiring specific proof of reasonable measures to protect the confidentiality of the information at issue. By being proactive and planning ahead, automotive enterprises can better protect their valuable trade secret assets.

Jason S. McCarter is a member and chair of the automotive practice at Miller & Martin PLLC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g., Jason McCarter and Elizabeth Marquardt, Cos. Must Consider Electric Vehicles' Unique Risk Profile, Law360 (2021) (https://bit.ly/3Dg1j5H) (discussing EV supply chain evolution and gaps).

[2] Tesla Inc. v. Khatilov, Case No. 4:21-cv-00528 (N. Dist. Cal. 2021).

[3] Faraday & Future Inc. v. Evelozcity Inc., Case No. 2:18-cv-00737 (C. Dist. Cal. 2018).

[4] Eagle Harbor v. Ford, Case No. 3:11-cv-05503 (W. Dist. Wa. 2011).

[5] For example, even after the initial costs and hurdles of obtaining formal patent protection, U.S. patents can be challenged and invalidated on various grounds. See, e.g., Christopher Hutter, Using the U.S. Patent and Trademark Office to Neutralize Invalid Patents, https://www.cooleygo.com/us-patent-and-trademark-office-neutralize-invalid-patents-ptab-digest/.

[6] See 18 U.S.C. § 1839(3); Uniform Trade Secrets Act § 1.4, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e19b2528-e0b1-0054-23c4-8069701a4b62.

[7] See 18 U.S.C. § 1836.

[8] See id.; see also Jason McCarter and Robert Kohse, Auto Cos. Should Take Note of Recent DTSA Case Law, Law360 (2016), https://www.law360.com/articles/869203/auto-cos-should-take-note-of-recent-dtsa-case-law.

[9] See UTSA § 1 et seq.

[10] Otherwise, the statute of limitations for misappropriation claims is three years under the DTSA and the model UTSA. See USC § 1836(d); UTSA § 6.

[11] See 18 U.S.C. § 1839.