Published on *The National Law Review* https://natlawreview.com

Software Code Theft: Are You Protected?

Article By:

Bruce A. Fox

Robert M. Weiss

The case of Sergey Aleynikov, a former Goldman Sachs programmer who was criminally indicted for stealing software code relating to the bank's high-frequency trading applications, serves as a useful reminder that software, like any valuable asset, can be a tempting target for would-be wrongdoers. Though Mr. Aleynikov's criminal conviction under the Economic Espionage Act was recently overturned by the U.S. Court of Appeals for the Second Circuit, Goldman Sachs can still pursue a civil remedy against Mr. Aleynikov for trade secret misappropriation. But a misappropriation claim requires that a victim has taken concrete steps to gain the benefits of trade secret protection for the subject asset. Therefore, Goldman's chances of prevailing in a civil action depend largely on whether it took the appropriate steps, preliminarily, to protect its software as a trade secret.

Elements of a Trade Secret

In order for a piece of information to constitute a trade secret, a holder must: (1) derive *actual or potential economic value from the information* because it is not readily ascertainable by others and (2) use *reasonable efforts to maintain the secrecy of the information*.[1] As long as these two basic criteria are met, a trade secret can encompass nearly any type of subject matter, unlike patents (which are limited to novel and non-obvious inventions) and copyrights (which are limited to original works of authorship). Also unlike patent and copyright protection, trade secret protection stems from state law, not federal law. Therefore, although the basic doctrine of trade secret law is fairly consistent throughout the U.S., there are nuanced differences among the states with respect to how the doctrine is applied in practice.

Demonstrating the Elements for Software

It is normally not difficult to demonstrate that software fulfills the first criterion of a trade secret, "actual or potential economic value," even if the software's functionality is not as exotic as Goldman Sachs's high-frequency trading applications. Ultimately, any compilation of proprietary software code that potentially gives a company a competitive advantage should be able to meet the economic value requirement.[2] It is the second criterion, requiring a company to use reasonable efforts to maintain secrecy, that can often be difficult to meet.

There is no universal checklist of procedures that will ensure a company has met the secrecy requirement. There are, however, some fundamental processes that companies should implement rigorously in order to confer trade secret status on proprietary software. These include:

- Limiting both physical and electronic access to proprietary software code, and associated documentation, to those personnel having a need for such access in order to perform their duties;

- Entering into non-disclosure agreements with all employees and consultants who will have access to the software code;

- Entering into non-disclosure agreements with potential business partners (both suppliers and customers) before engaging in discussions regarding the functionality of the software;

- Ensuring that software license agreements with customers contain both confidentiality obligations *and* prohibitions against reverse engineering or decompiling the software;

- Adding comments within the source code to the software, and notices to any associated documentation, stating that the software is proprietary and confidential;

- Conducting periodic audits in order to identify any potential weaknesses in the security of the proprietary software code and taking prompt remedial action if weaknesses or unauthorized access is discovered; and

- Periodically communicating to the company's personnel, both orally and in writing, the confidential nature of the company's software code.

Certain Contractual Provisions to Watch For

As noted above, one of the means by which a company can demonstrate that it has met the secrecy requirement of a trade secret in its treatment of software is to restrict disclosure of the software to those who are subject to a protective agreement, such as a license agreement or confidentiality agreement. There are certain provisions that are common to such agreements that require careful consideration as they relate to trade secrets:

Survival of Confidentiality Obligations. Parties to a confidentiality agreement often resist signing up to confidentiality obligations that survive indefinitely, since a lot of information grows "stale" over time. This is problematic for a party who will disclose trade secrets during the course of the relationship: Upon the expiration of the parties' confidentiality obligations, the secrecy requirement may cease to be met, thus jeopardizing the trade secret status of the information that was disclosed. Therefore, a party who intends to disclose trade secrets during the term of a contract should try to extend the confidentiality period for trade secrets (as opposed to other types of confidential information) so that it lasts as long as trade secret status is maintained under applicable law.[3]

Limitation of Liability Clauses. It is common for license agreements and other software-related contracts to include a limit of liability clause that prevents a non-breaching party from recovering indirect and consequential damages or making claims for direct damages in excess of a designated dollar limitation. One might assume that an intentional malefactor, such as a party who has misappropriated trade secrets received under a license, would not be able to shield himself from liability on the basis of such a clause. However, some courts have indeed upheld a contract's limitation of liability clause to limit the damages that a party may seek for misappropriation of trade secrets.[4] Thus, a party who will disclose trade secrets during the term of a contract is well-advised to exclude breaches of confidentiality obligations from the scope of any limitation of liability provision. For good measure, a discloser of trade secrets should try to add an exception to the limitation of liability clause for "any violation or misappropriation of a party's intellectual property or other proprietary rights."

Conclusion: Vigilance is Key

It is self-evident that proprietary software code and other technical information (such as database contents, technical schematics, functional requirements, and proprietary business processes) are valuable assets to almost any business. But it is important to remember that establishing and maintaining trade secret status on such materials requires a fair amount of effort. Indeed, many companies that successfully safeguard their trade secrets do so by establishing a comprehensive trade secret protection program throughout the organization and appropriately training their personnel with respect to the program. Such trade secret protection programs typically have four main elements: (i) they establish a set of business processes designed to identify new trade secrets as the business acquires or develops information as part of its business; (ii) they institute specific rules as to how to safeguard different types of information (for example, the rules for customer lists will differ from the rules for proprietary software code); (iii) they provide guidelines for how to remedy violations and security breaches; and (iv) they provide a mechanism for reexamining and updating the protection program on a periodic basis, in a formalized way, to ensure that it remains consistent with the company's business processes.

While trade secret protection may require additional vigilance on your part, protecting your economically valuable secrets is essential in maintaining a competitive edge. Trade secret protection can serve as an important supplement to other forms of intellectual property protection; and it is good to keep in mind that your software is a distinct type of intellectual property, as to which you should take certain proactive steps in order to obtain and preserve its trade secret status.

[1] Uniform Trade Secrets Act ("UTSA") § 1.4.

[2] *See*, *Decision Insights, Inc. v. Sentia Group, Inc.*, 311 Fed. Appx. 586, 592–94 (4th Cir. 2009).

[3] Here is how such a survival clause might be drafted: "The obligations of the parties with respect to Confidential Information shall remain in force and effect at all times during the term of this Agreement and: (i) with respect to Confidential Information that does not constitute a trade secret, for three (3) years after termination or expiration of this Agreement; and (ii) with respect to Confidential Information that constitutes a trade secret under applicable law, for so long as such trade secret status is maintained."

[4] *See*, *Allen Brothers, Inc. v. Abacus Direct Corp.*, 2005 U.S. Dist. LEXIS 8444 (N.D. Ill. 2005) (court enforced contractual limitation of liability provision to limit plaintiff's damages for claims under Colorado's version of the UTSA to $1.00 in nominal damages and $2.00 in exemplary damages).

© 2025 Neal, Gerber & Eisenberg LLP.

National Law Review, Volume II, Number 138

Source URL:https://natlawreview.com/article/software-code-theft-are-you-protected-0