OBER | KALER
ATTORNEYS AT LAW

IP Watch™
Intellectual Property Law Alerts from Ober|Kaler's IP Group

Intellectual Property Group

E. Scott Johnson, Chair
Royal W. Craig
Jonathan M. Holda
Anthony F. Vittoria
James B. Wieland
Cynthia Blake Sanders
Christopher F. Lonegro
Jed R. Spencer
Kyle E. Conklin

Carlyle C. Ring, Jr. (Counsel)

MAY 22, 2009

Trade Secrets in the Video Game Industry

Kyle E. Conklin
410-347-7360
keconklin@ober.com

There has always been significant migration among video game industry employees, but this is especially true in today's economic climate. Unfortunately, this trend heightens the risk that a company's trade secrets will be misappropriated. This risk is exemplified by a recently-filed lawsuit involving a well-known video game company.

In April, Genius Products and Numark Industries filed suit against Activision and 7 Studios, claiming that the defendants misappropriated trade secrets involving an interactive disc-jockey video game, *Scratch: The Ultimate DJ*. Under a development agreement, 7 Studios was developing the game for Genius, but when Activision, which was also producing its own disc-jockey game, acquired 7 Studios, 7 Studios demanded new terms to the agreement. Genius refused to accept the new terms and terminated the agreement. Subsequently, Genius filed suit alleging that Activision and 7 Studios misappropriated its trade secrets, including "computer source code, generic code, object code, the 'game engine,' graphic materials, art work, story lines, music, sound effects, documentation, and user manuals."

As this lawsuit suggests, trade secret protection is important to commercial success, and to fully protect a company's trade secrets, one must first know what can be a trade secret and the different mechanisms of protecting these secrets. This article discusses trade secrets and how they relate to the software and video game industry.

What is a trade secret?

The legal definition of a trade secret varies by jurisdiction, but it is generally defined as any information that has economic value from not being known to the public, industry, or others who could realize economic value. This information must also be the subject of reasonable efforts to maintain its secrecy. If information qualifies as a trade secret, the trade secret owner may prevent anyone who improperly discovers the information from disclosing or using it.

A variety of information may qualify as a trade secret, including a formula, pattern, compilation of data, device, method, technique, or process. And in the gaming industry, trade secrets commonly comprise software, including firmware, software

tools, encoded file formats, story and character ideas and the code itself—source code, object code, and machine code.[1]

Software Must Be a Secret and Subject to Reasonable Security Measures

For software to qualify as a trade secret it must be a legitimate secret—the software cannot be disclosed to anyone not having a duty of confidentiality. And in some jurisdictions, the software must be novel—it cannot be common industry knowledge.[2] This novelty requirement, however, has a low threshold requiring some degree of change over what is already known. Software is typically also protectable under copyright law; these two forms of protection are not mutually exclusive.

If the software has been disclosed to a party not having a duty of confidentiality, the software is no longer considered a secret, and trade secret protection is lost. Thus, in the gaming industry, it is important to examine disclosures to employees, hired contractors, joint venturers, licensees, and end users.

The circumstances determine what necessary measures must be taken to ensure secrecy. Requiring all employees to sign a non-disclosure agreement is a common measure. An employee handbook or a written policy notifying the employee of the confidential nature of the employment relationship is another security measure that helps maintain secrecy, as well as restricting dissemination and access to the source code. And when disclosing confidential information to third parties such as independent contractors and joint venturers, a nondisclosure agreement should be signed by the recipient before making the disclosure.

With licensees and end users of widely distributed software, it is important that the license or EULA contain a provision that prohibits "reverse engineering" because of the ease software can be reverse engineered. Further, the trade secret owner should only distribute the software in object code, not source code, and always provide notice that the software is proprietary.

Software Must Provide Competitive Advantage and Value

For software to qualify as a trade secret, the owner must derive some advantage over competitors who do not have the software.[3] Commercial advantage may comprise the mere time and effort it took to develop the software, or the fact that the software is unknown to competitors.[4] The competitive advantage must also result in some value to the trade secret owner.

Proving Misappropriation of a Software Trade Secret

For a trade secret owner to prove misappropriation, the owner must prove that the defendant (1) is using the trade secret and (2) wrongfully obtained it.[5] With software, these requirements are generally satisfied by showing that the defendant's code is substantially similar to the trade secret or contains some unique identifying characteristics, such as unique syntax errors or algorithms. To show that the defendant wrongfully obtained the software, the owner can show, among others things, that the defendant (1) illegally gained access to the owner's computer and communication systems, (2) used misrepresentations or fraud to procure the trade secret, (3) bribed the owner's employee to gain information, or (4) hired the owner's former employees for the purpose of obtaining the trade secret.[6]

Conclusion

Virtually any type of software can be trade secret as long as it is a legitimate secret, provides a competitive advantage and value, and is subject to reasonably security measures.

Because of the increased mobility and competition in the industry, it's now more important than ever to ensure you have procedures in place to identify and secure trade secrets.

NOTES

[1]International Game Developers Association, Intellectual Property and the Video Game Industry (2003), available at **http://www.igda.org/ipr/IGDA_IPRights_WhitePaper.pdf.**

[2]L.J. Kutten, Computer Software Protection: Liability; Law; Forms § 4:27 (2009).

[3]L.J. Kutten, Computer Software Protection: Liability; Law; Forms § 4:29 (2009).

[4]*Id.* § 4:30.

[5]*Id.* § 4:26.

[6]*Id.*