One Indispensible Lesson Every Company Should Learn From the Goldman Sachs Computer Theft Trial

Insights
12.01.10

Opening arguments began yesterday in the trial of Sergey Aleynikov, a former Goldman Sachs computer programmer accused of stealing the computer code underlying Goldman's high-frequency trading programs. When Aleynikov was taken into custody by the FBI, he reportedly said he did not intend to take any proprietary code. Rather, he intended to take only open source code.

What's the difference? Open source code is computer code that is publicly available on the internet for use by anyone. Overlooked initially by most analysts, this "open source" defense featured prominently in opening arguments by Aleynikov's attorneys. Depending upon how much of what he took was open source code, Aleynikov's defense is a little like saying that although he took the Coke formula, he only intended to take sugar and water. Whether his defense will fly is likely dependant upon how much of what he took was open source code, and how much was not. It will also likely matter how the open source code was used by Goldman Sachs, and what restrictions were placed on the use of this code by the parties who made it available on the internet.

Typically, in order to copy open source code from the internet, a party must agree to the terms of a "click" or similar pop-up license. Although there are hundreds of different open source code licenses, many require that the user of the code must make publicly available any subsequent use of the code. In other words, if Goldman's high-frequency trading programs were built on the back of open source code, it will be more difficult for Goldman to claim trade secrecy for such programs.

Indispensible Lesson

Whether Aleynikov's defense prevails, this case presents an unmistakable and imperative lesson for companies that derive appreciable revenue from computer programs. Such companies should immediately assemble key personnel from management, business, information technology and inside and outside counsel with one agenda item:

- identify the top five most productive computer-based, proprietary assets and determine whether any of these assets have open source code embedded in their digital architecture. If the answer is yes, then the company needs to identify the different types of open source code that are involved, analyze the licensing requirements associated with each such code, assess the use and application of the code, and determine the exposure based on these factors.

To the extent there is a risk that the proprietary status and trade secret protections are diluted or compromised, then companies need to work with counsel to identify a cure. Otherwise, companies could find themselves answering what might come to be known as the Aleynikov defense.

Brent Cossrow is a member of Fisher Phillips' Employee Defection & Trade Secrets Practice Group. Mr. Cossrow's practice focuses on e-discovery and other electronically stored information issues. As always, please feel free to share your thoughts and questions in the comment space below. Mr. Cossrow's recent interviews with the media regarding the Goldman Sachs trial can be found here and here.

Related People

Brent A. Cossrow
Partner
610.230.2135
Email