KLEINBERG KAPLAN

Legal Update

Analyst Indicted for Stealing Hedge Fund Trading Data

March 2014

The New York County District Attorney's Office recently announced the indictment of a former analyst with a New York City hedge fund alleging that the analyst illegally accessed and duplicated proprietary and highly confidential information relating to the firm's trading methods. The analyst is charged with multiple counts of Unlawful Use of Secret Scientific Material, Unlawful Duplication of Computer Related Materials in the First Degree, and Criminal Possession of Computer Related Material.

The prosecution alleges that, over a nearly five-month period, the analyst gained unauthorized access to, and emailed to his personal email account, confidential documents describing the hedge fund's trading models, including information relating to quantitative trading strategies, a marketing presentation, and a scientific white paper. The analyst's former employer reported his actions to the District Attorney's Office after independently monitoring and investigating the analyst's conduct.

The New York County prosecutor appears to be aggressively prosecuting cases involving the theft of sensitive commercial data. For example, late last year, charges were brought against an individual whose federal conviction based on the very same conduct had been overturned by the United States Court of Appeals for the Second Circuit in *United States v. Aleynikov*, 676 F.3d 71 (2012), which precluded federal criminal enforcement under the National Stolen Property Act or Section 1832 of the Economic Espionage for the theft of computer code. The federal district court had convicted the defendant of stealing computer code from his former employer, a well-known investment banking firm. The Second Circuit reversed, finding the indictment to be legally insufficient. The Second Circuit held that the source code that Aleynikov stole did not constitute "goods," "wares," or "merchandise" within the meaning of the National Stolen Property Act and that Aleynikov's theft therefore did not violate that statute. The Second Circuit also held that the computer system Aleynikov stole was not 'produced for' or 'placed in' interstate or foreign commerce within the meaning of Section 1832 of the Economic Espionage Act because Goldman Sachs did not intend to sell or license it to anyone. The appellate court concluded, therefore, that the theft did not violate that section. Following the Second Circuit's dismissal of charges against Aleynikov, the New York County prosecutor charged Aleynikov under New York State laws for his use of his employer's confidential information.

Notwithstanding the Second Circuit's decision in *Aleynikov*, in light of the New York County prosecutor's actions, the threat of criminal prosecution should deter employees who might otherwise co-opt an employer's confidential data.

Redress for improper use of confidential information may also be sought through a civil suit. An employer uncovering evidence of the theft of confidential information by an employee can file a civil action both to enjoin future theft and use of any stolen materials and to recover monetary damages. Causes of action in a civil suit could include, for example, breach of contract, including confidentiality, non-disclosure, or non-competition agreements, breach of fiduciary duties, misappropriation of trade secrets, and claims based on the New York faithless servant doctrine. Federal copyright law or other specialized legislation such as the Federal Computer Fraud and Abuse Act may also afford relief under certain circumstances.

To discuss further, please contact your primary Kleinberg Kaplan attorney or:

Marc R. Rosen
212.880.9897
mrosen@kkwc.com

David Parker
212.880.9880
dparker@kkwc.com

Norris D. Wolff
212.880.9860
nwolff@kkwc.com

David M. Levy
212.880.9894
dlevy@kkwc.com

Netra Sreeprakash
212.880.9876
nsreeprakash@kkwc.com

This Legal Update provides general information only and is not intended as legal advice.