Protecting Trade Secrets From Theft By Ex-Employees

Insights
3.02.16

In late 2015, Atlantic Marine Construction Company, a Virginia Beach construction company, filed a lawsuit against a former Vice President of Construction and his new employer, alleging various causes of action arising out of the VP's trade-secret theft.At first glance, this lawsuit reflects a familiar scenario: a departing employee steals proprietary data on his way out and later provides it to a competitor.This case includes an interesting twist, however.Atlantic Marine alleges that the VP stole the trade secrets at issue **after** he was terminated, using a software tool to access his former employer's network.

The former VP allegedly stole the information at issue using Google Chrome Remote Desktop, a program that allows users to remotely access and control one computer from another over the Internet.Atlantic Marine alleges that the VP installed the program on a work computer during his employment without authorization.Then, after his termination, the VP logged on to the software with his personal Gmail address and accessed Atlantic Marine's computer network at least 16 times to view, copy, and download various trade secrets, including proposal sheets with contract details, formulas used for calculating costs, and other valuable confidential data.The complaint, filed in federal court in the Eastern District of Virginia, alleges violations of the federal Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, and the Virginia Uniform Trade Secret Act, in addition to a state law claim for trespass to chattels.

Notably, the alleged trade-secret theft at issue in the *Atlantic Marine* case could likely have been avoided by simply wiping the hard drive of the VP's work computer upon termination, although this step could be at odds with an employer's desire to preserve evidence in the event of future litigation. A different, safer step would have been to remove and preserve the VP's hard drive, which would both keep the hard drive for future purposes and also prevent it from being used for removal of data.

The case serves as a valuable reminder for employers to think through their specific policies and procedures for exiting employees.Specifically, employers can minimize the risk of post-termination trade-secret theft by taking a few precautionary measures:

- Collect any company-issued mobile devices and laptops, in addition to keys, access cards, and other related items;
- Examine the employee's device and laptop to determine if the employee has accessed or copied sensitive information in recent months, and consider saving a forensic copy of the device or hard

drive;

- Employers with Bring-Your-Own-Device ("BYOD") policies should take advantage of "mobile device management" ("MDM") software, which enables employers to override personal passwords and wipe the device remotely;
- Remove the employee's name from email group lists, distribution lists, the company website, and the building directory;
- Deactivate all email and user accounts and passwords of the terminated employee, and remove all access privileges; and
- Remind all terminated employees in their exit interview of their obligations to maintain the confidentiality of information and the consequences of violating the obligation.

These issues arise repeatedly in trade secret matters, regardless of the level of employee who leaves or even the manner used by the departing employee to take materials.

Related People

John W. Stapleton
Partner
404.240.5843
Email