THE
NATIONAL LAW REVIEW

SEC Brings First Major Cyber Insider Trading Case Against International Hacking Ring

Article By
Sigal P. Mandelker
Boris Zeldin
Proskauer Rose LLP
Corporate Defense and Disputes

- Communications, Media & Internet
- Criminal Law / Business Crimes
- Financial Institutions & Banking
- Securities & SEC

- All Federal

Tuesday, August 25, 2015

In an action that emphasizes the agency's commitment to *cybersecurity*, the ***SEC*** recently charged 32 defendants with violations of the federal antifraud laws and corresponding SEC rules, stemming from an alleged $100 million conspiracy to steal and trade on material non-public information contained in corporate earnings announcements that were obtained by hacking into the computer networks of three newswire services.

According to the SEC, over the past five years two Ukrainian men, Ivan Turchynov and Oleksandr Ieremenko, masterminded "one of the most intricate and sophisticated" insider trading schemes ever seen. The men allegedly used several methods, including brute force attacks and utilizing proxy servers to pose as employees and customers of the newswire services, in order to gain access to the newswire services' internal computer systems and obtain over 100,000 corporate earnings announcements before they were released to the public. Turchynov and Ieremenko would then transmit this information to U.S. based traders in Georgia, New York, and Pennsylvania, and international traders in Russia, Ukraine, Malta, Cyprus, and France, who, the SEC claims, utilized the data to place illicit trades. The complaint alleges that, in certain instances, the traders would also direct the

hackers to target specific announcements.

Although the window to trade was often quite narrow – in one instance only 36 minutes separated the hack and the public announcement – it is believed that the traders were able to use the stolen data to reap over $100 million dollars in profits. A portion of these proceeds were sent to Turchynov and Ieremenko as payment for the stolen information. The complaint alleges that the traders sought to conceal the funds sent to the hackers by characterizing the transfers as payments for construction equipment.

SEC Chair Mary Jo White described this scheme as "unprecedented in terms of the scope of the hacking, the number of traders, the number of securities traded and profits generated." The SEC noted that it was able to identify and unwind the conspiracy by using "innovative analytical tools to find suspicious trading patterns and expose misconduct." The agency has frozen the defendants' assets and is seeking a judgment ordering penalties, restitution with pre-judgment interest, and permanent injunctions against future violations.

The U.S. Attorney's Offices for the District of New Jersey and the Eastern District of New York also announced parallel criminal actions against Turchynov and Ieremenko, as well as several of the trader defendants charged by the SEC.

This complaint, and the sophistication of the alleged scheme, underscores the significance of cybersecurity in today's increasingly technology-reliant market. Security measures used by vendors to protect confidential information can represent a significant potential data vulnerability, which companies should carefully evaluate. We expect to see continued regulatory activity in this space. As we previously wrote here, government authorities have already identified cybersecurity, especially targeted at vendors with access to sensitive data, as an area ripe for regulation. These events will no doubt strengthen that emphasis and may be cited as evidence of the need for greater government oversight.