The Supreme Court Upholds a Cyber Trespass Conviction

By: Jay Shapiro
Cyber Law and Data Protection Alert
1.26.16

Businesses thrive from competition, but in some instances the motivation to out-perform a rival manifests itself in unfair or even illegal practices. The theft of proprietary information is one method used by those bent on obtaining an edge at all costs. Because this type of information is often kept on a corporation's computer system, state and federal prosecutors employ specialized statutes directed at this misconduct. One tool available to federal law enforcement is the Computer Fraud and Abuse Act, 18 U.S.C. 1030, which addresses illegal conduct directed at computer systems. The statute covers such criminal activity as accessing a computer to commit espionage, cyberattacks and computer trespass.

The Computer Fraud and Abuse Act was used by federal prosecutors in *United States v. Musacchio,* a case decided by the Supreme Court on January 25, 2016. The Court upheld the conviction of the former president of a logistics company in Texas for illegally accessing information from the computer systems of that company. Although the Court's decision focused upon issues concerning jury instructions and the statute of limitations, the facts underlying the conviction present a cautionary tale for businesses.

Michael Musacchio had been the president of Exel Transportation Services (ETS), a shipping-logistics company that had offices in Texas and other states. The federal indictment recounted a deliberate plan to use ETS' proprietary information for a new company that Musacchio and others intended to form. In the fall of 2004, Musacchio resigned from Exel. However, Musacchio enlisted the head of information technology at ETS to provide Musacchio with access to ETS' computers even after he separated from the corporation.

The indictment charged that, over the course of time, Musacchio obtained access to ETS' business plan for the upcoming year and other proprietary information. One of Musacchio's co-defendants, Roy Brown, the IT chief who had remained at ETS, on numerous occasions accessed employees' emails to obtain other information related to ETS' business plans. A year after Musacchio left ETS, he formed Total Transportation Services (TTS), a rival business. Brown left ETS to work with Musacchio at TTS, but he continued to infiltrate ETS' systems and even provided Musacchio with his own password to access ETS' electronic information.

The breach was not discovered until the end of the first quarter of 2006. Ultimately, ETS sued TTS, Musacchio, Brown and others, and that lawsuit was settled for $10 million. Then, in 2010, Musacchio, Brown and another accomplice were indicted in the Northern District of Texas (the indictment was superseded two years later). Although the other defendants pleaded guilty, Musacchio elected to go to trial. He was tried in 2013, convicted and sentenced to 60 months in prison.

It is beyond dispute that corporations are vulnerable to computer breaches from outsiders intent on criminal activity ranging from disruption of business to theft of valuable information. An important lesson from *United States v. Musacchio* is that sound business practice requires companies to take steps to protect against unauthorized access that may be perpetrated by those inside as well, including:

- Adopt comprehensive policies concerning access to network systems. These should be published throughout the company and adhered to in order to minimize these significant risks;
- Obtain legal advice concerning the best ways to warn employees about the repercussions of unauthorized disclosure and use of proprietary information; and

- Consult outside counsel to address the company's control over portable devices that could be used to access network systems.

While recent reports have demonstrated that breaches have become a fact of life, these precautions can certainly act as a deterrent to those holding nefarious ambitions.

For more information, please contact Jay Shapiro (212.714.3063; shapiroj@whiteandwilliams.com) or another member of our Cyber Law and Data Protection Group.