Litigation Alert: The Computer Fraud and Abuse Act: Does it Protect Against the Improper Use of Electronically Stored Information?

August 10, 2020

The COVID-19 pandemic has perpetuated far-reaching changes in the business community and how we work, travel, and participate in society as individuals. Many industries have rapidly transitioned to having their employees work from home. Other industries have suffered layoffs and furloughs, creating uncertainty for many companies and their employees. Now more than ever, employers are searching for top talent and will not hesitate to go to a competitor to find it. All the while, employees have greater access to proprietary or protected information, remotely, from the privacy of their home offices.

Your employees' access to your company's proprietary and confidential information is authorized. But what if the authorized access to your company's proprietary information turns into an unauthorized use? The Computer Fraud and Abuse Act (CFAA), a federal statute, protects against unauthorized access, such as someone hacking into your computer network. But how does it protect against instances of authorized access, but unauthorized use? How do courts treat an employee's unauthorized access to information? What protections have the courts given a company whose employee diverted electronically stored confidential or proprietary information? How have courts addressed a company's attempts to enforce its rights to protect its confidential or proprietary information?

Recently, the United States Supreme Court, in *Van Buren v. United States*, No. 19-783 (U.S.), granted a petition for certification to consider whether a person who is authorized to access information on a computer for certain purposes violates the CFAA if he or she accesses the same information for an improper purpose. The decision is important to determine whether the statute applies to protect not only against hackers, but against unauthorized use, by authorized users, such as an employee, who has access to confidential information, but uses that information for an improper or unlawful purpose such as to unfairly compete.

The case arises from a criminal investigation of Nathan Van Buren, a sergeant with a Police Department in Cumming, Georgia. Van Buren asked an individual, Andrew Albo, for a loan. As part of a sting operation, Albo asked Van Buren to look into whether a particular woman was an undercover police officer. Van Buren ran a search on the woman in the government database. A federal grand jury convicted Van Buren of one count of felony computer fraud, in violation of the CFAA, 18 U.S.C. § 1030(a)(2), and one count of honest-services wire fraud, in violation of 18 U.S.C. §§ 1343 and 1346. On appeal, Van Buren argued that accessing information in the database did not "exceed authorized access," as defined in the CFAA. The Eleventh Circuit upheld his conviction.

Under the CFAA, an individual may be subject to criminal penalties or civil liability if he or she "intentionally accesses a computer without authorization or exceeds authorized access." 18 U.S.C. § 1030(a)(2). There is currently a circuit split to interpret the "exceeds authorized access" prong of the statute. The First, Fifth, and Seventh Circuits have held that accessing a computer for an unauthorized purpose violates the statute, even if the person was otherwise authorized to access the information. *See United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). The Second, Fourth, and Ninth Circuits have held that a person violates the statute if a person accesses information on a computer that he or she is prohibited from accessing. *See United States v. Valle*, 807 F.3d 508 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). Thus, by granting the petition for certification, the U.S. Supreme Court will provide clarity on the definition of "exceeds authorized access" and whether authorized users can violate the CFAA.

The Van Buren decision demonstrates the severity of violations of the CFAA. A violation of Section 1030(a)(2) of the CFAA is a misdemeanor, punishable by a fine or imprisonment of one year, or both. 18 U.S.C. § 1030(c)(2)(A). That misdemeanor becomes

a felony publishable by imprisonment for up to five years, "if the offense was committed for purposes of commercial advantage or private financial gain." 18 U.S.C. § 1030(c)(2)(B)(i). A company damaged by the actions of another that violate the statute may bring a civil claim and obtain money damages and injunctive or other equitable relief. 18 U.S.C. § 1030(g). Van Buren was also charged with wire fraud. Thus, depending on the circumstances, the penalties for violating the CFAA are severe and can even result in criminal prosecution. While a company may have redress under state and federal trade secret statutes and under the common law, this decision will be instrumental in determining the extent to which the CFAA protects a company in instances when an employee or other authorized user diverts its electronically stored confidential and protected proprietary information.

The need for this added protection is particularly relevant today, as the COVID-19 pandemic has substantially increased remote access to a company's computer network, in the privacy of an employee's home. A company seeking to protect its proprietary information at this time when access to company information by employees has become easier than ever, should carefully review the CFAA, its accompanying case law, and any recent developments, including the Supreme Court's analysis on this issue.

Litigation may be necessary to protect your company's interests. If you have any questions about this alert, please contact:

Rose A. Suriano, Esq., Member and Co-Chair, Litigation Practice, at rsuriano@bracheichler.com or 973-403-3129
Robyn K. Lym, Esq., Associate, Litigation Practice, at rlym@bracheichler.com or 973-403-3124