Update on "Authorized Access" under the Computer Fraud and Abuse Act

July 27, 2022

In as remote and hybrid work arrangements became common during the Covid pandemic, company files became more widely accessible through remote access.

The Computer Fraud and Abuse Act (CFAA), a federal statute, protects against unauthorized computer access, such as someone hacking into a company's computer network. But what happens when an employee has authorized access to digital information but plans to use it for an improper purpose or with improper motives? Will the CFAA still provide protection?

The United States Supreme Court, in Van Buren v. United States, No. 19-783 (June 3, 2021), ruled that an individual does not "exceed authorized access" under the CFAA when accessing the information on a computer normally available, even if it is accessed with improper motive or for an improper purpose.

In Van Buren v. United States, Nathan Van Buren, a sergeant with the Police Department in Cumming, Georgia, ran a license-plate search in a law enforcement computer database, not in the course of his work, but for a personal reason in exchange for money. His conduct violated department policy. A federal grand jury convicted him of one count of felony computer fraud in violation of the CFAA, 18 U.S.C. § 1030(a)(2). The Eleventh Circuit upheld his conviction. However, the U.S. Supreme Court reversed and held that his conduct did not "exceed authorized access" as defined in the CFAA.

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). This provision initially applied to accessing financial information but has since been expanded to cover any information from any computer "used in or affecting interstate or foreign commerce or communication" (18 U.S.C. § 1030(e)(2)(B)) and now includes all computers that connect to the internet. The

statute defines the term “exceeds authorized access” to mean “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter.” 18 U.S.C. § 1030(e)(6). Violations of the statute include penalties such as fines and sentences of imprisonment for up to 10 years. 18 U.S.C. § 1030(c)(2). The CFAA permits a private a right of action for persons who have suffered damage or loss from a CFAA violation. 18 U.S.C. § 1030(g).

The Court performed a close textual analysis of the statute and considered the legislative history. It expressed concern that the statute could criminalize a wide variety of unintended conduct, including, for example, an employee using a work computer to send a personal email or read the news or use a website beyond its terms of service. The Court hesitated to extend criminal liability to those various circumstances.

The Court held that an individual will “exceed authorized access” under the CFAA when he or she accesses a computer without authorization and obtains information located in particular areas of the computer, such as files or databases, that are off-limits to him. Because Van Buren had access to the license plate information he accessed, the Court reversed the Eleventh Circuit’s opinion. Thus, employers should carefully review employees’ computer access, as access for improper purpose may be permitted under the CFAA.

Click here to read the entire Spring 2022 Litigation Quarterly Advisor now

For more information, contact:
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com
Robyn Lym | 973.403.3124 | rlym@bracheichler.com

Authors

The following attorneys contributed to this insight.

Keith J. Roberts

Member
Litigation, Healthcare Law

973.364.5201 · 973.618.5585 Fax

kroberts@bracheichler.com

Robyn K. Lym

Associate
Litigation

973.403.3124 · 973.618.5941 Fax

rlym@bracheichler.com