Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one or to watch my one hour CLE seminar video go to:
http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

Can Breaching a Contract Be Computer Fraud?

Court in ticket resale case says 'yes,' if it results in unauthorized access, an essential element of the crime.

The U.S. Department of Justice has brought a Computer Fraud and Abuse Act (CFAA) prosecution in New Jersey against the owners and operators of Wiseguy Tickets Inc., an online ticket seller for concerts and sports events. A critical element in proving most violations of the CFAA, the federal computer crime statute, is that the defendant's access to the computer (interpreted broadly to include a Web site) that is the object of the criminal activity was "without authorization or exceeds authorized access." 18 U.S.C. 1030. The defendants are charged with unauthorized access to the Web sites of online ticket vendors (OTVs) such as Ticketmaster and Telecharge for violating the OTVs' Web site terms of service that prohibit the purchasing of tickets in large amounts for resale to the public.

The district court hearing the case recently denied the defendants' motion to dismiss the indictment on the ground that it seeks "to criminalize what otherwise would be a breach of contract action for violating the terms of service for ticket sales on" these OTVs. *U.S. v. Lowson*, No. 10-114 (D.N.J. Oct. 12, 2010). The defendants argued that, "under the government's theory, a teenager hypothetically could be prosecuted under the CFAA for violating the age requirement restrictions in the terms of service when using a search engine like Google." *Id*., slip op. at 10.

The notion that this prosecution is seeking to criminalize a breach of contract will be examined in light of established court decisions interpreting the CFAA and its implications for Web site owners whose legal remedy is not limited to reporting violations to the authorities for criminal prosecution. Web site owners are also entitled under the statute to bring a civil action for damages and injunctive relief. 18 U.S.C.1030 (g).

The contract upon which the defendants premised their motion to dismiss was the requirement on the OTVs' Web sites that all Internet customers had "to accept" the rules in the terms of service "before buying Event tickets." Indictment ¶ 1(f). These terms of service were designed "[t]o ensure fair access to Event tickets" to the general public. Thus, the OTVs "generally limited the number of seats that an online purchaser could obtain per event" and "prohibited the purchase of Event tickets on their website for commercial re-sale (i.e. purchase by ticket brokers)." *Id*.

The OTVs also "specifically prohibited computer programs that purchased tickets automatically, such as 'bots,' 'worms,' 'spiders,' and 'crawlers' from accessing their sites." Id. "To enforce

these restrictions and to protect their webpages from automated ticket purchasing software," the OTVs "used computer code and software that was designed to detect and prohibit automated programs from accessing...[their] computer servers." *Id*. ¶ 1(k).

In denying the Wiseguy defendants' motion to dismiss, the court recognized that, as "the indictment makes clear, the unauthorized access charges at the heart of this indictment involve allegations of breaches of both contract- and code-based restrictions." *Lowson*, slip op. at 10. As to the code-based restrictions, the defendants, assisted by "contract hackers," are charged with employing sophisticated means to circumvent the OTVs' computer code through "automated software," "optical character recognition to defeat...difficult" security measures and " 'hacks' and 'backdoors' to enable automated programs to purchase tickets" and make it appear that the tickets were bought by individual members of the public. *Id*. at 9. From 2002 through 2008, the defendants procured more than 1.5 mil- lion tickets by hacking into the OTVs and generated profits for themselves of n early $30 million by selling event tickets at prices more than the face value to the public. Indictment ¶¶ 52-55.

Based on these facts, the U.S. courts of appeals for the 2d and 5th circuits would readily conclude that the defendants' efforts to defeat the code-based restrictions on the Web sites were sufficient standing alone to prove the CFAA's critical element of "unauthorized access." In *U.S. v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991), the defendant Robert Morris, a student in Cornell University's computer science doctorate program, disseminated through e-mail "a computer program known as a 'worm' that spread and multiplied, eventually causing computers at various educational institutions and military sites to 'crash' or cease functioning." In affirming his conviction, the court concluded that "Morris's conduct here falls well within the area of unauthorized access" because he did "not use...[two standard computer programs] in any way related to their intended function," but "instead he found holes in both programs that permitted him a special and unauthorized access route into other computers." *Id*. at 510. That is precisely what the Wiseguy Tickets defendants are charged with -- circumventing through sophisticated hacks the intended function of the OTV Web sites to prevent mass purchases by ticket sellers.

U.S. v. Phillips, 477 F.3d 215 (5th Cir. 2007), followed Morris' intended-use test in upholding the conviction of Christopher Phillips, a student in the computer sciences department at the University of Texas who hacked into UT's secure server, which only allowed access to an authorized user through the user's Social Security number. Phillips launched what is known as a "brute-force attack" program, which automatically transmitted to the server as many as six random Social Security numbers per second. During the course of 14 months, Phillips gained "access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni." *Id*. at 218. Phillips had also signed a UT acceptable use computer policy in which he agreed not to perform certain scans on his university computer account that would permit him to search for vulnerabilities to hack into and attack the network. The court found that Phillips' brute-force attack program not only was unauthorized by his agreement with UT, but that it "was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computerized data

that he was not permitted to view or use." *Id*. at 220.

Similarly, other courts have emphasized the importance of employment contracts and policies to define unauthorized access. In *EF Cultural Travel B.V. v. Explorica Inc*., 274 F.3d 577, 580-84 (1st Cir. 2001), the court, in affirming a preliminary injunction in a civil action brought under the CFAA, relied upon the defendants' signed confidentiality agreement to find that the defendants' access to EF's Web site was unauthorized because they had used a scraper that had been built from their confidential knowledge about the topology of EF's Web site for the purpose of automatically and accurately downloading EF's 154,293 tour prices from the site.

U.S. v. John, 597 F.3d 263, 269, 272 (5th Cir. 2010), upheld the CFAA conviction of Citigroup account manager Dimetriace Eva- Lavon John, who accessed Citigroup's internal computer system to provide her brother with customer account information that he used to perpetrate fraudulent charges. The court found that John had exceeded authorized access based on "Citigroup's official policy, which was reiterated in training programs that John attended, [that] prohibited misuse of the company's internal computer systems and confidential customer information." *Id*. at 272.

As the above court decisions reflect, "authorization" is a "word...of common usage, without any technical or ambiguous meaning," and is a question of fact to be decided by a jury based on all of the circumstances. *Morris*, 928 F.2d at 511. Criminal (or civil) liability for the CFAA only attaches if there is proof of the other essential elements of the crime, such as the theft or destruction of data. Thus, the risk raised by the Wiseguy defendants that a teenager would be prosecuted for a violation of the CFAA for simply lying about his age on Google is as well founded as a teenager being prosecuted for mail fraud for lying in a letter to his parents.

Given the Wiseguy Tickets prosecution and the case law underpinning it, there are several proactive steps every company can take to enhance the likelihood that violators of its Web site can be criminally prosecuted or sued in a civil action. This is because the "CFAA...is primarily a statute imposing limits on access and enhancing control by information providers." *EF Cultural Travel B.V. v. Zefer Corp*., 318 F.3d 58, 63 (1st Cir. 2003). Thus, a company "can easily spell out explicitly what is forbidden," through employee agreements, policies and access- limiting technology.