



Nick Akerman

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

Nick is a partner in the New York office of Dorsey & Whitney. This article was co-authored with Melissa Krasnow, a partner in the Minneapolis office of Dorsey & Whitney

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



Can a Labor Union Be Sued Under the Computer Fraud and Abuse Act for Spamming an Employer’s Voice and Email Systems?

The answer is yes. The Sixth Circuit Court of Appeals last week reversed a district court and reinstated a Computer Fraud and Abuse Act (“CFAA”) claim brought by an employer against a labor union for “bombarding” the computer systems of its sales and executive offices with emails and voicemails making it impossible for the company to communicate with its customers and vendors. *Pulte Homes, Inc v. Laborers’ International Union of North America*, 2011 WL 3274014 (6th Cir. Aug 2, 2011). This case is a good example of how the federal Circuit Courts of Appeal are taking control of the interpretation of the scope of the CFAA away from the district courts and applying it expansively to protect computer technology.

“To generate a high volume of calls, . . . [the Union] both hired an auto-dialing service and requested its members to call Pulte [Homes, a homebuilder]. It also encouraged its members, through postings on its website, to "fight back" by using . . . [the Union’s] server to send e-mails to specific Pulte executives. Most of the calls and e-mails concerned Pulte's purported unfair labor practices, though some communications included threats and obscene language.” *Id.* at *1.

As the court pointed out, “it was the volume of the communications, and not their content, that injured Pulte. The calls clogged access to Pulte's voicemail system, prevented its customers from reaching its sales offices and representatives, and even forced one Pulte employee to turn off her business cell phone. The e-mails wreaked more havoc: they overloaded Pulte's system, which limits the number of e-mails in an inbox; and this, in turn, stalled normal business operations because Pulte's employees could not access business-related e-mails or send e-mails to customers and vendors.” *Id.*

“Four days” into the onslaught, “Pulte's general counsel contacted” the union and requested that they “stop the attack because it prevented Pulte's employees from doing their jobs.” *Id.* When the Union ignored his request, the company filed suit for, among other things, a violation of the CFAA for “knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer.” 18 U.S.C. § 1030(a)(5)(A). The CFAA defines damage as “any impairment to the integrity or availability of data, a program, a system, or information.” *Id.* § 1030(e)(8).

The court, relying on the plain meaning of the terms “impairment,” “integrity,” and “availability,” concluded “that a transmission that weakens a sound computer system--or, similarly, one that diminishes a plaintiff's ability to use data or a system--causes damage.” *Id.* at *4. Here, the court found that the complaint alleged “just that” – “the transmissions diminished Pulte's ability to use its systems and data because they prevented Pulte from receiving at least some calls and accessing or sending at least some e-mails.” *Id.*

The court also found that the complaint alleged that the Union acted with the requisite intent under the statute to intentionally cause damage. The court summed up the allegations in the complaint that showed that the Union acted “with the conscious purpose of causing damage (in a statutory sense) to Pulte’s computer system”:

- (1) The union “instructed its members to send *thousands* of e-mails to three specific Pulte executives; (2) many of these e-mails came from . . . [the union’s] server; (3) . . . [the Union] encouraged its members to "fight back" after Pulte terminated several employees; (4) . . . [the union] used an auto-dialing service to generate a high volume of calls; and (5) some of the messages included threats and obscenity. And although Pulte appears to use an idiosyncratic e-mail system, it is plausible . . . [the union] understood the likely effects of its actions--that sending transmissions at such an incredible volume would slow down Pulte's computer operations. . . . [The Union’s] rhetoric of "fighting back," in particular, suggests that such a slow-down was at least one of its objectives.

Id. at *6.

This case is reflective of the pattern that has emerged over the past few years in the judicial interpretation of the CFAA. The district courts have interpreted the CFAA narrowly, sometimes limiting it only to outside computer hacking, while the appeals courts have continued to interpret the statute broadly as a true federal omnibus computer crime statute outlawing all criminal activity directed at computers and computer systems.