## 648 F.3d 295 United States Court of Appeals, Sixth Circuit.

PULTE HOMES, INC., a Michigan Corporation, Plaintiff-Appellant,

V.

LABORERS' INTERNATIONAL UNION OF NORTH AMERICA; Terence M. O'Sullivan; Randy Mayhew, Defendants—Appellees.

Nos. 09–2245, 10–1673. | Argued: Dec. 9, 2010. | Decided and Filed: Aug. 2, 2011.

\* \* \*

## COOK, Circuit Judge.

Plaintiff, an active and successful home builder, sued a national labor union and two of its officers for orchestrating an onslaught on the company's phone and e-mail systems. Plaintiff appeals two orders in this combined appeal: (1) the order denying its motion for a preliminary injunction and (2) the order granting Defendants' motion to dismiss. We affirm in part and reverse in part.

I.

Pulte Homes, Inc.'s (Pulte['s]) complaint stems from an employment dispute. Pulte alleges that in September 2009 it fired a construction crew member, Roberto Baltierra, for misconduct and poor performance. Shortly thereafter, the Laborers' International Union of North America (LIUNA) began mounting a national corporate campaign against Pulte—using both legal and allegedly illegal tactics—in order to damage Pulte's goodwill and relationships with its employees, customers, and vendors.

Just days after Pulte dismissed Baltierra, LIUNA filed an unfair-labor-practice charge with the National Labor Relations Board (NLRB). LIUNA claimed that Pulte actually fired Baltierra because he wore a LIUNA t-shirt to work, and that Pulte also terminated seven other crew members in retaliation for their supporting the union. Pulte maintains that it never terminated any of these seven additional employees.

\*299 Not content with its NLRB charge, LIUNA also began using an allegedly illegal strategy: it bombarded Pulte's sales offices and three of its executives with thousands of phone calls and e-mails. To generate a high volume of calls, LIUNA both hired an autodialing service and requested its members to call Pulte. It also encouraged its members, through postings on its website, to "fight back" by using LIUNA'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.

Yet 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.

Four days after LIUNA started its phone and e-mail blitz, Pulte's general counsel contacted LIUNA. He requested, among other things, that LIUNA stop the attack because it prevented Pulte's employees from doing their jobs. When the calls and e-mails continued, Pulte filed this suit alleging several state-law torts and violations of the Federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, a statute that both criminalizes certain computer-fraud crimes and creates a civil cause of action.

\* \* \*

II.

\* \* \*

1.

To state a transmission claim, a plaintiff must allege that the defendant "knowingly cause[d] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[d] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). We assume, because it is not disputed, that LIUNA's communications constitute "transmissions," *see id.*, and that Pulte's phone and e-mail systems qualify as "protected computers," *see id.* § 1030(e)(2). According to LIUNA and the district court, however, Pulte fails to allege that LIUNA "intentionally caused damage." We address damages and intent—in that order—and conclude that Pulte properly alleges both.

[The court discusses the damage and intent elements of (a)(5)(A) at length. It concludes that impairing a system is sufficient for damage, and that the record supports a finding of intent.]

\* \* \*

2.

Though Pulte's transmission claim passes Rule 12(b)(6), we agree with the district court that its access claim does not

\* \* \*

Because Congress left the interpretation of "without authorization" to the courts, we again start with ordinary usage. The plain \*304 meaning of "authorization" is "[t]he conferment of legality; ... sanction." 1 OED, *supra*, at 798. Commonly understood, then, a defendant who accesses a computer "without authorization" does so without sanction or permission. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132–33 (9th Cir.2009).

In addition, comparing the phrase "without authorization" to another, somewhat similar phrase in the CFAA further informs the proper interpretation. The CFAA criminalizes both accessing a computer "without authorization" and "exceeding authorized access" to a computer. *E.g.*, 18 U.S.C. § 1030(a)(1). Despite some similarities in phrasing, we must, if possible, give meaning to both prohibitions. *See Daniel v. Cantrell*, 375 F.3d 377, 383 (6th Cir.2004) ("We avoid interpretations of a statute which would render portions of it superfluous."); *cf. Int'l Airport Ctrs.*, *L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir.2006) (observing that "[t]he difference ... is paper thin"). We can.

Unlike the phrase "without authorization," the CFAA helpfully defines "exceeds authorized access" as "access[ing] a computer with authorization and ... us [ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Under this definition, "an individual who is authorized to use a computer for certain purposes *but goes beyond those limitations* ... has 'exceed[ed] authorized access.' " *LVRC Holdings LLC*, 581 F.3d at 1133 (second alteration in original) (emphasis added). In contrast, "a person who uses a computer 'without authorization' *has no rights, limited or otherwise*, to access the computer in question." *Id.* (emphasis added); *accord Lockheed Martin Corp. v. Speed*, No. 6:05–CV1580–ORL–31, 2006 WL 2683058, at \*5 (M.D.Fla. Aug. 1, 2006) (observing that individuals "without authorization" have "no permission to access whatsoever").

We ask, then, whether LIUNA had *any* right to call Pulte's offices and e-mail its executives. It did—and LIUNA's methods of communication demonstrate why.

LIUNA used unprotected public communications systems, which defeats Pulte's allegation that LIUNA accessed its computers "without authorization." Pulte allows all members of the public to contact its offices and executives: it does not allege, for example, that LIUNA, or anyone else, needs a password or code to call or e-mail its business. Rather, like an unprotected website, Pulte's phone and e-mail systems "[were] open to the public, so [LIUNA] was authorized to use [them]." *See Citrin*, 440 F.3d at 420. And though Pulte complains of the number, frequency, and content of the communications, it does not even allege that one or several calls or e-mails would have

been unauthorized. Its complaint thus amounts—at most—to an allegation that LIUNA exceeded its authorized access.

Because Pulte does not allege that LIUNA possessed *no* right to contact Pulte's offices and its executives, it fails to satisfy one of the elements—access "without authorization"—of its claim. *See* 18 U.S.C. § 1030(a)(5)(B), (C).

\* \* \*

## III.

For these reasons, we affirm in part and reverse in part the order dismissing Pulte's complaint, affirm the denial of the preliminary injunction, and remand for proceedings consistent with this opinion.