NOTICE: Summary decisions issued by the Appeals Court pursuant to M.A.C. Rule 23.0, as appearing in 97 Mass. App. Ct. 1017 (2020) (formerly known as rule 1:28, as amended by 73 Mass. App. Ct. 1001 [2009]), are primarily directed to the parties and, therefore, may not fully address the facts of the case or the panel's decisional rationale. Moreover, such decisions are not circulated to the entire court and, therefore, represent only the views of the panel that decided the case. A summary decision pursuant to rule 23.0 or rule 1:28 issued after February 25, 2008, may be cited for its persuasive value but, because of the limitations noted above, not as binding precedent. See Chace v. Curran, 71 Mass. App. Ct. 258, 260 n.4 (2008).

COMMONWEALTH OF MASSACHUSETTS

APPEALS COURT

25-P-990

RAMON CRUCETA

vs.

J.C. CANNISTRARO LLC.

MEMORANDUM AND ORDER PURSUANT TO RULE 23.0

In February of 2023, Ramon Cruceta (plaintiff) filed an action against the defendant, J.C. Cannistraro LLC (JCC), in the Superior Court, seeking damages for emotional distress after a data breach at JCC allegedly caused the plaintiff's personal information to be released onto the "dark web." A Superior Court judge allowed JCC's motion for summary judgment in May of 2025 based on the plaintiff's inability to prove the claims or damages identified in his complaint. On appeal, the plaintiff argues that the judge erred by allowing JCC's motion for summary judgment because the case contained genuine disputes of material fact. Because the plaintiff failed to allege, or demonstrate, that he has suffered a nonspeculative, direct injury as a result

of the alleged data breach, we affirm the judge's grant of summary judgment.

Background. "We briefly summarize the basic facts in their light most favorable to [the plaintiff], the nonmoving party, reserving additional facts for later discussion." Sullivan v. Liberty Mut. Ins. Co., 444 Mass. 34, 35 (2005). The plaintiff worked as a pipefitter at JCC between 2015 and June 30, 2020. In or about October of 2020, JCC's information technology manager discovered unusual activity within the company's computer network systems. After an investigation, the company found that its network had been encrypted by ransomware. JCC's firewall vendor, Fortinet, had warned JCC before October 2020 about the possibility of a data breach. Fortinet had already recognized this vulnerability, upgraded its software, and encouraged its customers to install the upgrade for maximum security.

JCC notified its employees of the ransomware attack and potential data breach via e-mail message and posting notice on the company's intranet on October 7, 2020. Because the plaintiff's last day of work at JCC was June 30, 2020, he did not receive that e-mail message, nor did he have access to JCC's intranet. The plaintiff received notice of a potential data

breach in December of 2020, when an Experian[1] alert warned that his social security number had been detected on the dark web.[2]

The plaintiff filed a complaint alleging that JCC's negligence in failing to maintain and consistently update its firewall software caused the data breach, the theft of his social security number, and its publication on the dark web. The plaintiff also alleged that this publication constituted an invasion of privacy under G. L. c. 214, § 1B, and fraud. The plaintiff alleged that the publication of his social security number on the dark web caused him to suffer emotional distress, anxiety, and constant daily fear of potential for identity theft, privacy loss, and other financial harm. The plaintiff did not allege that the publication of his social security number on the dark web caused him any specific monetary damage or loss.

JCC filed a motion for summary judgment in March of 2025. After a hearing, a judge of the Superior Court allowed JCC's motion, finding that the plaintiff lacked any proof of

---

[1] Experian is a credit reporting service.

[2] The term "dark web" refers to encrypted online content that is not indexed by conventional search engines, providing increased anonymity for potential threat actors. See Bloomenthal, Investopedia, Understanding the Dark Web: Privacy, Security, and Legal Concerns, https://www.investopedia.com/terms/d/dark-web.asp.

liability, causation, or damages. The judge also found that the plaintiff lacked standing to bring his claims because he failed to allege any nonspeculative injury. The plaintiff timely appealed.

Discussion. We review the judge's grant of summary judgment de novo. See Galenski v. Erving, 471 Mass. 305, 307 (2015). While we view the evidence in the light most favorable to the opposing party, "the opposing party cannot rest on his or her pleadings and mere assertions of disputed facts to defeat the motion for summary judgment." LaLonde v. Eissner, 405 Mass. 207, 209 (1989).

Here, the plaintiff has alleged negligence that caused him emotional distress. The plaintiff's alleged injury is the fact that his social security number appeared on the dark web. He alleges that this caused him severe distress because his private information is accessible to threat actors. While we are sympathetic to the impact of data breaches, this is inadequate to state a claim.

"To prevail on a claim of negligence, 'a plaintiff must prove that the defendant owed the plaintiff a duty of reasonable care, that the defendant breached this duty, that damage resulted, and that there was a causal relation between the breach of the duty and the damage'" (citation omitted). Lev v. Beverly Enters.-Mass., Inc., 457 Mass. 234, 239-240 (2010). A

claim for negligent infliction of emotional distress requires "objective corroboration of the emotional distress alleged." Sullivan v. Boston Gas Co., 414 Mass. 129, 137 (1993), quoting Payton v. Abbott Labs, 386 Mass. 540, 547 (1982). The possibility of future injury, though real, is not enough.

To the extent the plaintiff is alleging negligent infliction of emotional distress, the plaintiff has not presented any "objective corroboration of the emotional distress alleged," such as evidence of physical manifestation of his emotional distress. To the extent that the plaintiff is alleging simple negligence, he has not alleged any cognizable damage, such as monetary loss.

The plaintiff does not mention his claims for invasion of privacy and fraud in his appellate brief. Therefore, he has waived any challenge to summary judgment on these claims.[3]

[3] To the extent that the plaintiff raised challenges to summary judgment on these claims in his reply brief, his arguments "come[] too late." See Boxford v. Massachusetts Highway Dep't, 458 Mass. 596, 605 n.21 (2010) (claim deemed waived when raised for first time in reply brief). Were we to reach the merits, the plaintiff failed to allege that the defendant intended to disseminate his social security number or intended to deceive anyone. See Masingill v. EMC Corp., 449 Mass. 532, 540 (2007) ("To recover for fraudulent misrepresentation, a plaintiff must allege and prove that the defendant made a false representation of a material fact with knowledge of its falsity for the purpose of inducing the plaintiff to act thereon, and that the plaintiff relied upon the representation as true and acted upon it to [her] damage" [quotation and citation omitted]); Hayes v. Mirrick, 378 F. Supp. 3d 109, 116-117 (D. Mass. 2019) (to state claim for

Moreover, viewing the evidence in the light most favorable to the plaintiff, he has not demonstrated that he can prove an essential element of his negligence claim. Accordingly, the judge did not err in granting summary judgment to JCC.[4,5]

Judgment affirmed.

By the Court (Rubin, Henry & Wood, JJ.[6]),

Clerk

Entered: June 4, 2026.

---

statutory invasion of privacy, plaintiff must demonstrate that defendant gathered and disseminated facts of private nature).

[4] Because we resolve the plaintiff's appeal on this ground, we do not reach his other arguments.

[5] JCC's request for appellate attorney's fees is denied.

[6] The panelists are listed in order of seniority.