

Rel: November 15, 2024

Notice: This opinion is subject to formal revision before publication in the advance sheets of **Southern Reporter**. Readers are requested to notify the **Reporter of Decisions**, Alabama Appellate Courts, 300 Dexter Avenue, Montgomery, Alabama 36104-3741 ((334) 229-0650), of any typographical or other errors, in order that corrections may be made before the opinion is printed in **Southern Reporter**.

SUPREME COURT OF ALABAMA

OCTOBER TERM, 2024-2025

SC-2023-0784

Shymikka Griggs

v.

NHS Management, LLC

Appeal from Jefferson Circuit Court
(CV-23-902261)

PARKER, Chief Justice.

This appeal arises from the Jefferson Circuit Court's dismissal of Shymikka Griggs's data-breach action against NHS Management, LLC ("NHS"), a consulting firm that provides management services for

nursing homes and physical-rehabilitation facilities. Because Griggs fails to demonstrate that she sufficiently pleaded her claims, we affirm the circuit court's judgment.

I. Facts

The relevant facts are set forth in Griggs's complaint. NHS provides administrative services for nursing homes and physical-rehabilitation facilities in Alabama, Arkansas, Florida, and Missouri. In providing those services, NHS collects sensitive personal-identification information and personal-health information from employees, patients, and vendors at each of the facilities that it services. The information that NHS collects includes the following:

- Name, address, phone number, and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Driver's license number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Health information;

- Information concerning a patient/resident's doctor, nurse, or other medical providers;
- Photo identification;
- Employer information;
- Payment information; and
- Similar information for patient/residents' family members or guardians.

In May 2021, NHS discovered what it described as a "sophisticated cyberattack" on its computer network (hereinafter "the data breach"). An investigation revealed that cybercriminals had had unfettered access to NHS's network for 80 days between February and May 2021. In October 2021, NHS notified the United States Department of Health and Human Services of the data breach.

In March 2022, NHS notified the individuals whose data was potentially accessed of the data breach, including Griggs, a former employee of NHS. In its notice, NHS notified the potential victims that the breached information included their names, dates of birth, Social Security numbers, medical information, and health-insurance information.

It appears that Griggs initially filed a class-action complaint against NHS in the United States District Court for the Northern District of Alabama, but she later voluntarily dismissed her complaint. In June 2023, Griggs filed a class-action complaint in the Jefferson Circuit Court. In her complaint, Griggs alleged that, after she received NHS's letter notifying her of the data breach, she was notified by Credit Karma, a credit-monitoring service, that her personal-identification information would be found on many different sites on the "dark web." She also alleged that she spent considerable time working with Credit Karma to freeze her credit and to correct errors on her credit report. She further alleged that, since the data breach, she has been receiving a high number of spam emails, calls, and texts and that she often received more than three spam calls or texts in the same day. Griggs alleged that she received several calls from the fraud department at Apple, Inc., asking whether she had made certain Apple product purchases worth about \$3,000 that she had not made. She has also received harassing phone calls and emails stating that she owes money for "payday loans" that she does not owe. She alleged that those payday loans had resulted from the sale of her personal information on the "dark web" after the data breach.

Griggs also alleged that she spends about 15 minutes every day monitoring her financial accounts and that she anticipated spending more time and money to mitigate harm caused by the data breach. She further alleged that all persons whose personal-identification and health information had been compromised in the data breach have suffered and will continue to suffer similar damage.

In her class-action complaint, Griggs asserted claims of negligence, negligence per se, breach of contract, invasion of privacy, unjust enrichment, breach of confidence, breach of fiduciary duty, and violation of the Alabama Deceptive Trade Practices Act, § 8-19-1 et seq., Ala. Code 1975. Griggs requested various forms of equitable relief, compensatory damages, attorneys' fees and costs, and pre- and postjudgment interest.

In August 2023, NHS moved to dismiss Griggs's complaint. In its motion, NHS argued that Griggs could not establish "standing" because the injuries she alleged were not injuries in fact. NHS also argued that Griggs had failed to state a claim on which relief could be granted. On October 10, 2023, the circuit court dismissed Griggs's complaint "pursuant to Rule 12(b)," Ala. R. Civ. P., with prejudice. Griggs appeals.

II. Standard of Review

In NHS's motion to dismiss, it argued that Griggs's claims were due to be dismissed under Rule 12(b)(1), Ala. R. Civ. P., for lack of subject-matter jurisdiction because, it said, Griggs had failed to allege an injury in fact. NHS also argued that Griggs's claims were due to be dismissed under Rule 12(b)(6) for failure to state a claim upon which relief can be granted. In its order dismissing Griggs's claims, the circuit court stated that it was doing so "pursuant to Rule 12(b)."

Although the circuit court did not expressly indicate which of the grounds for dismissal listed in Rule 12(b) was applicable, it dismissed Griggs's claims with prejudice. Griggs conceded at oral argument before this Court that the circuit court's dismissal of her claims with prejudice means that it dismissed her claims on the merits, because dismissal for lack of subject-matter jurisdiction is generally regarded as being without prejudice. See Ex parte Capstone Dev. Corp., 779 So. 2d 1216 (Ala. 2000) (holding that a dismissal for lack of subject-matter jurisdiction is treated as a dismissal without prejudice). Accordingly, we address only whether Griggs sufficiently pleaded her claims under Rule 12(b)(6).

When reviewing an order of dismissal under Rule 12(b)(6), this Court applies the following standard of review:

"On appeal, a dismissal is not entitled to a presumption of correctness. Jones v. Lee County Commission, 394 So. 2d 928, 930 (Ala. 1981); Allen v. Johnny Baker Hauling, Inc., 545 So. 2d 771, 772 (Ala. Civ. App. 1989). The appropriate standard of review under Rule 12(b)(6) is whether, when the allegations of the complaint are viewed most strongly in the pleader's favor, it appears that the pleader could prove any set of circumstances that would entitle her to relief. Raley v. Citibanc of Alabama/Andalusia, 474 So. 2d 640, 641 (Ala. 1985); Hill v. Falletta, 589 So. 2d 746 (Ala. Civ. App. 1991). In making this determination, this Court does not consider whether the plaintiff will ultimately prevail, but only whether she may possibly prevail. Fontenot v. Bramlett, 470 So. 2d 669, 671 (Ala. 1985); Rice v. United Ins. Co. of America, 465 So. 2d 1100, 1101 (Ala. 1984). We note that a Rule 12(b)(6) dismissal is proper only when it appears beyond doubt that the plaintiff can prove no set of facts in support of the claim that would entitle the plaintiff to relief. Garrett v. Hadden, 495 So. 2d 616, 617 (Ala. 1986); Hill v. Kraft, Inc., 496 So. 2d 768, 769 (Ala. 1986)."

Nance v. Matthews, 622 So. 2d 297, 299 (Ala. 1993).

III. Analysis

Griggs contends that she sufficiently pleaded each of her claims. As noted above, Griggs asserted claims of negligence, negligence per se, breach of contract, invasion of privacy, unjust enrichment, breach of confidence, breach of fiduciary duty, and violation of the Alabama Deceptive Trade Practices Act. In her response to NHS's motion to dismiss, Griggs conceded that her claim alleging violation of the Alabama

Deceptive Trade Practices Act was due to be dismissed. Griggs also appears to have abandoned her breach-of-contract claim because she did not address that claim in her brief on appeal. Ex parte Riley, 464 So. 2d 92, 94 (Ala. 1985) ("[I]t has long been the law in Alabama that failure to argue an issue in brief to an appellate court is tantamount to the waiver of that issue on appeal."). Thus, those claims are not before us.

A. Negligence

To sufficiently plead a negligence claim, Griggs had to allege (1) that NHS owed her a duty, (2) that NHS breached that duty, (3) that NHS's breach of duty caused her damage, and (4) that she incurred damages. See Prill v. Marrone, 23 So. 3d 1, 6 (Ala. 2009) ("The elements of a negligence claim are a duty, a breach of that duty, causation, and damage." (citation omitted)).

First, Griggs contends that she sufficiently alleged that NHS owed her a duty. She points to the following allegations in her complaint:

- "[NHS] had clearly-defined and mandatory obligations created by HIPAA, [i.e., the Health Insurance Portability and Accountability Act] contract, industry standards, common law, and representations made to [Griggs] and Class Members, to keep their

Personal Information confidential and to protect it from unauthorized access and disclosure."

- "[NHS] has obligations created by HIPAA, industry standards[,] and common law to keep Class Members' Personal Information confidential and to protect it from unauthorized access and disclosure."
- "NHS is a business associate of a 'covered entity' under HIPAA. Business associates of covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of [Personal Health Information]. Safeguards must include physical, technical and administrative components."
- "NHS's duty included a responsibility to implement processes by which [it] could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a cyberattack."
- "[NHS's] duty of care to use reasonable security measures arose due to the special relationship that existed between it and the Class, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. [NHS] was in a position

to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a cyberattack and data breach."

Griggs fails to demonstrate that those allegations were sufficient to allege that NHS owed her a duty under Alabama law. The only authority that Griggs cites in this section of her principal brief is Martin v. Arnold, 643 So. 2d 564 (Ala. 1994), which she cites for the elements of a negligence claim. However, as this Court has repeatedly held, citing authority merely for the elements of a cause of action is generally not sufficient to argue in an appellate brief that the allegations in a complaint met the pleading standard regarding each element. See Davis v. Sterne, Agee & Leach, Inc., 965 So. 2d 1076 (Ala. 2007), and S.B. v. Saint James Sch., 959 So. 2d 72 (Ala. 2006) (overruled on other grounds, as recognized in Flickinger v. King, 385 So. 3d 504, 517 (Ala. 2023)). In Davis, a widow sued her sons and the family's financial-management firm, asserting claims of negligence, wantonness, and conspiracy (among other claims), after the sons allegedly stole the funds from their deceased father's IRA and the firm failed to prevent the theft. The trial court entered a summary judgment for the defendants. On appeal, the widow

argued that she had presented substantial evidence of negligence and wantonness. However, the only legal authority that the widow cited to support her negligence claim was the traditional four-element test of negligence. Brief of the widow, p. 45, in Davis, supra.¹ This Court held that a "citation to a statute and a general principle of law, along with a conclusory statement that [the widow had] presented substantial evidence to support her [negligence and wantonness] claims" did not satisfy Rule 28(a)(10), Ala. R. App. P. Davis, 965 So. 2d at 1092-93. Likewise, as to her conspiracy claim, her brief "quote[d] a general proposition of the law of conspiracy" from a previous decision, followed by a conclusory assertion that the defendants had conspired to take the action that was the basis of her claim. Davis, 965 So. 2d at 1092.

Similarly, in S.B., this Court reviewed a summary judgment in favor of a private school and its administrator on certain negligence claims asserted against them by the parents of certain students. In particular, the plaintiffs claimed that the school was negligent in failing to prevent students from uploading pornographic images onto the

¹"[T]his court takes judicial knowledge of its own records." Austill v. Prescott, 293 So. 3d 333, 339 n.6 (Ala. 2019) (citation omitted).

computers in the school's computer lab. In their brief on appeal challenging the summary judgment, the plaintiffs cited "a single case" that "merely sets forth the general duty a school owes to its students." S.B., 959 So. 2d at 89. "Aside from the single case cited, the [plaintiffs did] not discuss or cite any authority relative to their negligence claims." Id. Instead, the argument in their brief "consist[ed] primarily of a series of factual statements and conclusory statements of liability on the part of [the school and its administrator], with no real explanation as to how or why [the school and its administrator were] liable." Id. Accordingly, we concluded that the plaintiffs' argument failed to comply with Rule 28(a)(10).

Like the appellants' arguments in Davis and S.B., Griggs's argument before this Court is deficient. Davis and S.B., like this case, presented legal theories in which the existence of a duty was not necessarily obvious. Under such circumstances, citation to the traditional negligence test alone constitutes citation to only a general proposition of law. Aside from her lone citation to Martin, Griggs merely quotes the allegations in her complaint. Griggs's argument that NHS owed her a duty to safeguard her personal information or to timely notify her after

it discovered the data breach fails to comply with Rule 28(a)(10). Horn v. Fadal Machining Ctrs., LLC, 972 So. 2d 63, 80 (Ala. 2007) (holding that authority supporting only general propositions of law is not sufficient to satisfy Rule 28(a)(10) and that, when no authority is cited, the effect is the same as if no argument had been made).²

²In her reply brief, Griggs cited the Alabama Data Breach Notification Act ("the ADBNA"), § 8-38-1 et seq., Ala. Code 1975, in support of her argument that NHS owed her a duty to safeguard her personal information. That statute provides that entities such as NHS "shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security." § 8-38-3(a), Ala. Code 1975.

However, as NHS points out in its motion to strike portions of Griggs's reply brief, Griggs did not rely on that statute in her response to NHS's motion to dismiss or in her opening brief on appeal. Although Griggs cited the ADBNA once in a footnote in the facts section of her opening brief, she did so only to note that NHS's notice of the data breach was untimely. Because Griggs cited the ADBNA in support of her duty argument for the first time in her reply brief, Griggs has waived the issue whether the ADBNA imposed a duty on NHS.

In her response to the motion to strike, Griggs contends that she merely cited the ADBNA as additional authority to refute NHS's arguments, which she says opened the door to her to cite statutes that impose a duty on NHS to safeguard personal information. That argument might be plausible if Griggs had cited some authority in her opening brief. But without any authority cited in the first place, any authority cited in the reply brief cannot be additional. Authority cited for the first time in a reply brief cannot cure a complete failure to cite authority in

Because Griggs fails to demonstrate that she sufficiently pleaded an essential element of her negligence claim, we need not consider that claim any further. Nevertheless, we note that Griggs's arguments that she sufficiently alleged the elements of breach and causation fail for the same reason -- she cited no authority demonstrating that her allegations regarding those elements were sufficient. Again, she simply restates the allegations of her complaint and baldly asserts that those allegations were sufficient.

Although we recognize that the issue of the sufficiency of pleadings alleging negligence in the specific context of a data breach is a question of first impression in Alabama, that fact alone does not relieve an appellant from his obligation to cite some authority in support of his

the opening brief. Steele v. Rosenfeld, LLC, 936 So. 2d 488, 493 (Ala. 2005) (observing that when authority is cited for the first time in an appellant's reply brief, the effect is the same as if the argument was made for the first time in a reply brief).

Griggs also relied on the ADBNA at oral argument, but because Griggs, in effect, failed to timely cite the ADBNA in her briefs, her reliance on the ADBNA at oral argument was the equivalent of raising the issue for the first time at oral argument. But an issue cannot be raised for the first time at oral argument. Hutchins v. Shepard, 370 So. 2d 275, 276-77 (Ala. 1979) (refusing to consider an argument raised for the first time during oral argument).

argument, even if it is from another jurisdiction that has considered the issue or if it addresses an analogous situation. As noted by one commentator, "[a] critical part of an appellate lawyer's job is to compare and contrast his case to previous judicial opinions to persuade a court to rule his way." Ed R. Haden, Alabama Appellate Practice § 12.12[2] (2023). Griggs does not attempt to compare or contrast her allegations here with prior decisions addressing the sufficiency of allegations of duty, breach, or causation in cases involving at least analogous, if not identical, facts.

For these reasons, we conclude that Griggs fails to demonstrate that the circuit court erred in dismissing her negligence claim as insufficiently pleaded.

B. Negligence Per Se

Next, Griggs contends that she sufficiently alleged the elements of her claim of negligence per se. Griggs contends that, in that claim, she sufficiently alleged the elements of duty and breach by alleging that NHS violated various provisions of the Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996),

SC-2023-0784

and the Federal Trade Commission Act ("the FTCA"), see 15 U.S.C. §§ 41-58.

Although Griggs recognizes that neither of those statutes creates a private right of action, she contends that even a statute that creates no private right of action can serve as the basis for a negligence per se claim. In support of that argument, Griggs relies on Allen v. Delchamps, Inc., 624 So. 2d 1065 (Ala. 1993), in which this Court allowed a negligence per se claim to proceed under the Food, Drug, and Cosmetic Act ("the FDCA"), 21 U.S.C. § 301 et seq., even though the FDCA did not provide for a private cause of action for civil damages. But regardless of whether a violation of HIPAA or the FTCA will support a negligence per se claim, an allegation that NHS violated those statutes is not sufficient to plead a claim for negligence per se. This Court has held that "negligence per se does not arise by the mere violation of a statute or regulation. The element of proximate cause is also required." Elder v. E.I. DuPont De Nemours & Co., 479 So. 2d 1243, 1248 (Ala. 1985).

Here, Griggs contends only that she alleged that "HIPAA and the FTCA established a duty or standard of care in support of her negligence per se claim." She makes no argument that she pleaded that NHS's

alleged violations of HIPAA and the FTCA were the proximate cause of her alleged damages. To the extent that Griggs falls back on her argument that she sufficiently alleged proximate causation regarding her negligence claim, as noted above, she failed to cite any authority in support of that argument. For this reason, Griggs fails to demonstrate that she sufficiently pleaded her negligence per se claim.

C. Invasion of Privacy

Next, Griggs contends that she sufficiently pleaded her invasion-of-privacy claim because the personal information that was accessed -- Social Security numbers, names, and birth dates -- was highly sensitive and because failure to secure such information would be highly offensive to a reasonable person. Griggs relies on federal cases for the proposition that a third party's procurement of personal data can give rise to a claim of invasion of privacy.

"This Court defines the tort of invasion of privacy as the intentional wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.'" Rosen v. Montgomery Surgical Ctr.,

825 So. 2d 735, 737 (Ala. 2001) (emphasis added; citation omitted).

Further, in Alabama,

"invasion of privacy consists of four limited and distinct wrongs: (1) intruding into the plaintiff's physical solitude or seclusion; (2) giving publicity to private information about the plaintiff that violates ordinary decency; (3) putting the plaintiff in a false, but not necessarily defamatory, position in the public eye; or (4) appropriating some element of the plaintiff's personality for a commercial use."

Johnston v. Fuller, 706 So. 2d 700, 701 (Ala. 1997). Regardless of the type of invasion of privacy Griggs alleges occurred as a result of the data breach, Griggs makes no effort to demonstrate that she alleged that NHS's conduct was intentional. This omission is fatal to her claim.

D. Unjust Enrichment

Next, Griggs contends that she sufficiently pleaded her unjust-enrichment claim by alleging that she conferred a benefit on NHS. Specifically, Griggs points to her allegation that "[p]art of the wages or pay terms that these Class Members negotiated with ["NHS"] was intended to be used by ["NHS"] to fund adequate security of ["NHS's"] computer property and [Griggs's] and Class Members' Personal Information." She also points to her allegation that NHS "retained the benefits of its unlawful conduct including the amounts received for data

and cybersecurity practices that it did not provide." In support of her argument, Griggs relies on Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012), in which the United States Court of Appeals for the Eleventh Circuit held:

"To establish a cause of action for unjust enrichment/restitution, a Plaintiff must show that '1) the plaintiff has conferred a benefit on the defendant; 2) the defendant has knowledge of the benefit; 3) the defendant has accepted or retained the benefit conferred; and 4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it.'"

693 F.3d at 1328 (quoting Della Ratta v. Della Ratta, 927 So. 2d 1055, 1059 (Fla. Dist. Ct. App. 2006)).

Griggs's allegation that she somehow conferred a benefit on NHS in exchange for data protection is insufficient. As the United States District Court for the Central District of Illinois noted when dismissing an unjust-enrichment claim in a data-breach action, the plaintiff "paid for food products. She did not pay for a side order of data security and protection." Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016). Further, as NHS notes, Resnick is distinguishable because there the plaintiffs alleged that they had paid a monthly

premium to the defendant for data security. For these reasons, Griggs fails to demonstrate that she sufficiently pleaded her unjust-enrichment claim.

E. Breach of Confidence

Next, Griggs contends that she sufficiently pleaded her claim of breach of confidence. In support, Griggs relies on Muransky v. Godiva Chocolatier, Inc., 979 F.3d 917 (11th Cir. 2020), for the proposition that "[a] breach of confidence 'is rooted in the concept that the law should recognize some relationships as confidential to encourage uninhibited discussions between the parties involved.'" 979 F.3d at 932 (quoting Young v. United States Department of Justice, 882 F.2d 633, 640 (2d Cir. 1989)). Griggs further cites Muransky for the proposition that "[a] breach of confidence ... involves 'the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship.'" Id. (quoting Alan B. Vickery, Note, Breach of Confidence: An Emerging Tort, 82 Colum. L. Rev. 1426, 1455 (1982)). Based on that authority, Griggs contends that she sufficiently alleged a breach-of-confidence claim by alleging that she provided NHS her personal information with the expectation and understanding that

SC-2023-0784

NHS would protect it from unauthorized access and disclosure, but that NHS breached that confidence by failing to secure her personal information.

However, Griggs does not identify any Alabama authority recognizing breach of confidence as a cause of action under Alabama law. Further, as NHS points out, even if breach of confidence were a cognizable claim under Alabama law, Griggs does not demonstrate that she alleged that NHS affirmatively disclosed her information. Affirmative disclosure is a necessary element of breach of confidence; theft by a third party is not sufficient. Purvis v. Aveanna Healthcare, LLC, 563 F. Supp. 3d 1360, 1378 (N.D. Ga. 2021) (holding that plaintiffs failed to plead breach-of-confidence claim because they did not allege facts suggesting that the defendants had disclosed the plaintiffs' information; they alleged only that their information had been stolen by third parties). For these reasons, Griggs fails to demonstrate that breach of confidence is a recognized cause of action in Alabama, let alone that she sufficiently pleaded it.

F. Breach of Fiduciary Duty

Finally, Griggs contends that she sufficiently pleaded her breach-of-fiduciary-duty claim. She cites various cases from this Court holding that, under Alabama law, a fiduciary relationship exists when one person has influence or dominion over another person. She also contends that Alabama does not have a rule that there can never be a fiduciary relationship between employees and employers. She contends that a fiduciary relationship can be inferred from her allegations that NHS collects and stores sensitive personal information as a precondition to employment. She contends that, as a result, NHS has influence and dominion over her and the class members and that NHS has obligations to keep that information confidential.

Griggs alleged that she was an employee of NHS. Generally, in Alabama, "'a principal or employer is not the fiduciary of the agent or employee.'" Miller v. SCI Sys., Inc., 479 So. 2d 718, 720 (Ala. 1985) (quoting and adopting the trial court's order). Griggs seeks to undermine that rule by arguing that "Alabama does not have a hard and fast rule that there can never be a fiduciary relationship between employees and employers." The only case that Griggs cites for that proposition is Lanfear v. Home Depot, Inc., 536 F.3d 1217, 1224 (11th Cir. 2008). Griggs also

relies on the same portion of Lanfear for the proposition that courts must inquire regarding whether the nature of the relationship between the parties is that of a fiduciary relationship. But that portion of Lanfear does not contain any language supporting either proposition. Rather, that portion of Lanfear addressed the issue whether an employee must exhaust administrative remedies. The language that Griggs purports to quote from Lanfear regarding the nature of the relationship between the parties appears nowhere in that decision. Although NHS observes in its brief that Lanfear does not support Griggs's argument, Griggs does not address Lanfear further in her reply brief or attempt to explain its relevance.

In short, Griggs cites no authority supporting her contention that the relationship between her and NHS was an exception to Miller's general rule that an employer is not a fiduciary of an employee, and she does not respond to NHS's reliance on Miller in her reply brief. Griggs contends that she alleged that there is a fiduciary relationship between her and NHS because NHS voluntarily collected and stored her personal information, thereby exercising influence and dominion over her. Griggs contends that, as a result, NHS had a duty to keep her personal

information confidential and that it breached that duty by failing to keep her information safe and confidential. But she cites no authority supporting those contentions. Accordingly, Griggs's argument fails to comply with Rule 28(a)(10).

IV. Conclusion

Based on the foregoing, Griggs fails to demonstrate that she sufficiently pleaded her claims against NHS. Accordingly, Griggs does not demonstrate that the circuit court erred in dismissing her claims under Rule 12(b)(6). Therefore, we affirm the circuit court's judgment dismissing Griggs's claims.

AFFIRMED.

Wise, Bryan, Sellers, Mendheim, and Mitchell, JJ., concur.

Cook, J., concurs specially, with opinion.

Shaw, J., concurs in the result, with opinion.

Stewart, J., concurs in the result.

COOK, Justice (concurring specially).

I concur with our Court's decision to affirm the Jefferson Circuit Court's dismissal of Shymikka Griggs's data-breach action against NHS Management, LLC ("NHS"). However, because data-breach actions are likely to become more frequent in the future, I write specially to provide additional guidance to the bench and bar on the types of claims that may be alleged in such actions and to note issues that counsel may wish to address in a future appropriate case.

I. Initial Observations

I start with a few initial observations about what this case concerns and what it does not concern. First, although this is a class action, the only claims before this Court today are the claims raised by the named class representative -- Griggs -- against her former employer, NHS, a consulting firm that provides management services for nursing homes and physical-rehabilitation facilities in Alabama, Arkansas, Florida, and Missouri.³ In other words, at this point, this is a case involving the theft

³See, e.g., Smith v. Bayer Corp., 564 U.S. 299, 313 (2011) (quoting Devlin v. Scardelletti, 536 U.S. 1, 16 n.1 (2002) (Scalia, J., dissenting)) ("[A] nonnamed class member is [not] a party to the class-action

of a single employee's personal information from her employer's network; it is not a case involving the theft of the health-care records of a medical patient. Had such a claim been alleged, the outcome here might (or might not) have been different.

Second, this is a case in which no express contract governing the protection or use of the data at issue exists. Again, if there were such a contract, the outcome here might (or might not) have been different.

Third, the parties agree that Alabama law controls in this case. If Griggs were attempting to state a claim under the law of a different state

litigation before the class is certified."); In re Checking Account Overdraft Litigation, 780 F.3d 1031, 1037 (11th Cir. 2015) ("Absent class certification, there is no justifiable controversy between [the defendant] and the unnamed putative class members. Furthermore, because the unnamed putative class members are not yet before the court, any claims that they might have against [the defendant] necessarily exist only by hypothesis."); and Molock v. Whole Foods Mkt. Grp., Inc., 952 F.3d 293, 301-02 (D.D.C. 2020) (Silberman, J., dissenting) ("Putative class members are not 'parties' to the action for any purpose, so the reasoning goes, thus before class certification there are no parties (other than those named) for a district court to dismiss."). See also Supreme Court of Alabama, Supreme Court O/A Jacksonville Alabama, YouTube (Sept. 19, 2024, 19:51-20:01) (at the time this decision was issued, this oral-argument session could be located at: <https://www.youtube.com/watch?v=jMUTOkd1tYk>) ([in which counsel for Griggs concedes that the only claims before our Court were claims brought by Griggs against NHS](#)).

or even under federal law, the outcome here might (or might not) have been different.

Although Griggs raised several claims in her complaint below,⁴ I believe that, at its core, this is a negligence case because the bulk of Griggs's claims against NHS rest on a duty that she contends it owed her to keep her personal information safe from a cyberattack. While I agree with the main opinion that Griggs failed to sufficiently argue that she had adequately pleaded this element of both her negligence and negligence per se claims, this does not mean that there will never be a situation in which a defendant may owe a duty to a plaintiff to safeguard such data from a criminal engaging in a cyberattack. And, even when such a duty does exist, as I also explain below, a plaintiff may still have to sufficiently allege that he or she has been damaged as a result of the breach of that duty.

II. To Recover for Negligence, a Plaintiff Must Establish That a Legal Duty Exists to Protect Personal Information from a Cyberattack by Criminals

As explained in the main opinion, a negligence claim under

⁴I concur fully with the main opinion's analyses of Griggs's arguments concerning those remaining claims.

Alabama law includes several elements. Among those elements is that the defendant must owe a duty to the plaintiff. The question whether a duty exists is a question of law for the trial court to consider. See, e.g., Rosenthal v. JRHBW Realty, Inc., 303 So. 3d 1172, 1182 (Ala. 2020) (quoting Taylor v. Smith, 892 So. 2d 887, 891 (Ala. 2004)) ("In Alabama, the existence of a duty is a strictly legal question to be determined by the court.").

In her brief on appeal, Griggs argues, among other things, that she sufficiently alleged in her complaint that NHS owed her a duty to protect her personal information from a cyberattack. Specifically, she notes that, in her complaint, she alleged (1) that NHS had "'clearly-defined and mandatory obligations created by HIPAA [i.e., the Health Insurance Portability and Accountability Act], contract, industry standards, common law, and representations made to [her] and class members, to keep their Personal Information confidential and to protect it from unauthorized access and disclosure,'" Griggs's brief at 43, and (2) that "NHS had obligations created by HIPAA, contract, industry standards, common law and representations made to class members, to keep class members' [personal information] confidential and to protect it from

unauthorized access and disclosure," Griggs's brief at 56.

A. Griggs's Failure to Comply with Rule 28(a)(10), Ala. R. App. P.

In making these assertions in her brief, however, Griggs fails to cite any relevant legal authority -- from this State or from another jurisdiction -- that supports her assertion that her employer, NHS, had a duty to prevent a third-party criminal from stealing her personal information off of its network. See Griggs's brief at 43-47. Our Court has repeatedly stated that

"Rule 28(a)(10), Ala. R. App. P., requires that arguments in an appellant's brief contain 'citations to the cases, statutes, other authorities, and parts of the record relied on.' Further, 'it is well settled that a failure to comply with the requirements of Rule 28(a)(10) requiring citation of authority in support of the arguments presented provides this Court with a basis for disregarding those arguments.' State Farm Mut. Auto. Ins. Co. v. Motley, 909 So. 2d 806, 822 (Ala. 2005)(citing Ex parte Showers, 812 So. 2d 277, 281 (Ala. 2001)). This is so, because "'it is not the function of this Court to do a party's legal research or to make and address legal arguments for a party based on undelineated general propositions not supported by sufficient authority or argument.'" Butler v. Town of Argo, 871 So. 2d 1, 20 (Ala. 2003) (quoting Dykes v. Lane Trucking, Inc., 652 So. 2d 248, 251 (Ala. 1994))."

Jimmy Day Plumbing & Heating, Inc. v. Smith, 964 So. 2d 1, 9 (Ala. 2007).

As the main opinion correctly notes, Griggs "presented legal theories in which the existence of a duty was not necessarily obvious," and, "[u]nder such circumstances, citation to the traditional negligence test alone constitutes citation to only a general proposition of law," which does not meet the requirements of Rule 28(a)(10). ____ So. 3d at ____.

Given that this lawsuit concerns claims arising out of an area of the law that our Court has not yet had a chance to address -- a data breach involving the alleged theft of an employee's personal information -- I agree with the main opinion that Griggs's failure to provide such legal authority is fatal to the question of whether a duty exists here and therefore whether a negligence claim can be maintained in this case.

B. Under Alabama Law, Does an Employer Have a Legal Duty to Protect an Employee from Third-Party Criminal Activity?

In the event that we were to reach this question in a future appropriate case, I note that the general rule in Alabama is that "an employer is not liable to its employees for criminal acts committed by third persons against an employee." Carroll v. Shoney's, Inc., 775 So. 2d 753, 755 (Ala. 2000). However, our Court has recognized that an exception to that general rule exists "when a special relationship or

special circumstances create a duty to protect ... an employee from the criminal acts of a third party." Id. Specifically, our Court has explained that this "'singular exception'" to the general rule "'arises when 'the particular criminal conduct was foreseeable.'" Id. at 756 (quoting Moye v. A.G. Gaston Motels, Inc., 499 So. 2d 1368, 1371 (Ala. 1986), quoting in turn Henley v. Pizitz Realty Co., 456 So. 2d 272, 276 (Ala. 1984)) (emphasis added). In other words, our Court has stated that this exception applies to employers only in the most "'extraordinary and highly unusual circumstances,'" including when the employer had "'specialized knowledge'" that criminal conduct was a "probability" such that the "criminal conduct [was] foreseeable." Carroll, 775 So. 2d at 756 (citations omitted).⁵

In her complaint, Griggs pleaded that she had been an employee of NHS and that it was this relationship that created a duty for NHS to protect her data from the cyberattack at issue here. However, other than generally alleging that NHS had a duty to protect her against a general

⁵In its response brief, NHS made all of these arguments about the limited duty to protect employees from third-party criminal activity. However, in her reply brief, Griggs simply ignores NHS's argument and the caselaw it cited.

threat of data breaches, Griggs did not allege in her complaint (1) that the cyberattack on NHS's network was foreseeable, (2) that NHS had "specialized knowledge" of the criminal activity, and (3) that the cyberattack at issue was a probability, as our caselaw discussed above appears to require.

Given that our caselaw discussed above has not been overruled and given that it would clearly apply to Griggs's allegation concerning the duty that she believes NHS owed to her, it was essential for Griggs to plead facts demonstrating that those circumstances existed here.

In making this observation, however, I do not wish to be understood as reaching or deciding what should be pleaded or what is necessary to prove the duty element for a negligence claim in a future data-breach case concerning a nonemployee in a sensitive context or when a special relationship exists or sensitive data is involved.⁶

⁶See, generally, Buckley v. Santander Consumer USA, Inc. (Case No. C17-5813 BHS, Mar. 29, 2018) (W.D. Wash. 2018) (not reported in the Federal Supplement) (declining to find a "common law legal duty" that could support plaintiff's negligence claim when the plaintiff alleged "failure to maintain adequate security" but then failed to allege negligent affirmative acts or a special relationship with defendant); Parker v. Carilion Clinic, 296 Va. 319, 347, 819 S.E.2d 809, 825 (2018) (explaining

C. The Alabama Data Breach Notification Act Does Not Establish a Legal Duty Actionable by a Private Plaintiff

Rather than addressing the caselaw discussed above, Griggs instead argues on appeal that NHS -- regardless of its status as her employer -- owed her a duty under the Alabama Data Breach Notification Act of 2018, ("the ADBNA"), § 8-38-1 et seq., Ala. Code 1975. According to Griggs, the ADBNA "firmly establishes NHS's duty to safeguard data," Griggs's brief at 23, which, she says, includes, among other things, providing "'notice within 45 days of the covered entity's ... determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates,'" Griggs's reply brief at 24 (quoting § 8-38-5(b), Ala. Code 1975) (emphasis omitted).

This argument is mistaken, at least as to private litigants. Section 8-38-9(a)(1), Ala. Code 1975, expressly states that the ADBNA cannot be

that "[n]one of our precedents has ever imposed a tort duty on a healthcare provider" to safeguard personal health information from unauthorized access); and McConnell v. Department of Lab., 345 Ga. App. 669, 677, 814 S.E.2d 790, 798 (2018) (finding no "general duty to safeguard personal information" under the Georgia Personal Identity Protection Act, Ga. Code Ann. §§ 10-1-910 through 10-1-915), aff'd, 305 Ga. 812, 828 S.E.2d 352 (2019).

used to manufacture a duty for a common-law claim, like negligence, because it cannot be used to alter a common-law claim: "Nothing in [the ADBNA] may otherwise be construed to affect any right a person may have at common law, by statute, or otherwise." (Emphasis added.)

Further, the Alabama Legislature has made absolutely clear that any alleged violation of the ADBNA is not actionable by a private citizen. See § 8-38-9(a)(1) ("A violation of [the ADBNA] does not establish a private cause of action under Section 8-19-10."). In fact, § 8-38-9(b)(2) states that the "Attorney General shall have the exclusive authority to bring an action for damages in a representative capacity on behalf of any named individual or individuals." (Emphasis added.)

By recently passing the ADBNA in 2018, the Legislature made clear that it was concerned with cybersecurity and cybercrime. In doing so, the Legislature made an important policy choice -- expressed in the text of the statute -- that the State of Alabama through the Attorney General's office has the authority and discretion regarding when and how

to apply this statute.⁷

D. Is There an Actionable Legal Duty Requiring Timely Notification of a Data Breach?

In addition to arguing that she sufficiently pleaded that NHS had breached its duty to her by failing to prevent the cyberattack in this case, Griggs also contends that she sufficiently plead that NHS had breached its duty by failing to timely notify her of the data breach itself. It appears undisputed by the parties that NHS did not notify Griggs as well as others impacted by the data breach until 10 months after it discovered that the breach had occurred. This 10-month period is troubling to me.

In my view, it might be possible to argue that a duty exists once an employer like NHS becomes aware of the data breach. In other words,

⁷In addition to the issues I have identified above, there are multiple procedural problems with this argument also. First, Griggs admits in her brief on appeal that the ADBNA "was not cited in the complaint." Griggs's brief at 7 n.3 (emphasis added). In fact, based on my review of the record, it does not appear that she alleged in any of her filings with the trial court that the ADBNA applied in her case, much less that it established a duty for NHS. Second, Griggs raises this argument for the first time in her reply brief on appeal. It is well settled that our Court will not consider completely new arguments that are raised for the first time in a reply brief. See Sverdrup Tech., Inc. v. Robinson, 36 So. 3d 34, 46-47 (Ala. 2009) (noting that "this Court will not consider arguments raised for the first time in a reply brief").

perhaps Griggs could have argued that NHS had "'specialized knowledge'" that criminal conduct was a "probability" and, thus, was "foreseeable" once it had actual knowledge of the data breach. Carroll, 775 So. 2d at 756. However, this is far from clear and might depend upon the exact knowledge NHS had acquired and the type of data involved. In any event, Griggs did not make this argument on appeal, and I see no reason to address it any further here.⁸

III. Does an Alleged Violation of Federal Regulations Create a Legal Duty for a Negligence Per Se Claim?

Griggs also argues on appeal that she sufficiently alleged the elements of her negligence per se claim. However, as the main opinion correctly notes, Griggs contends only that she alleged that the Health

⁸Even if Griggs had made such an argument, as explained below, she would still need to argue that she experienced damage resulting from this delayed notification. See In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (recognizing that unreported California cases and courts in other jurisdictions analyzing statutes mirroring California's Database Breach Act have held that "a plaintiff must allege actual damages flowing from the unreasonable delay," not simply damages from "the intrusion itself," in order to recover actual damages). I cannot find any explanation in Griggs's brief that she suffered any form of damage as a result of the delay in notification (as opposed to the data breach itself).

Insurance Portability and Accountability Act (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) ("HIPAA"),⁹ and the Federal Trade Commission Act ("the FTCA"), see 15 U.S.C. §§ 41-58, each "established a duty or standard of care in support of her negligence per se claim." Griggs's brief at 47. She made no argument that she had pleaded that NHS's alleged violations of those federal laws were the proximate cause of her alleged damages. As was the case with Griggs's negligence claim, I agree with the main opinion that this failure is fatal to whether such a claim can be maintained in this case. See Rule 28(a)(10), Ala. R. App. P.

However, in the event that we were to reach this question in a future appropriate case, I note that in Allen v. Delchamps, Inc., 624 So. 2d 1065, 1067 (Ala. 1993) (quoting Fox v. Bartholf, 374 So. 2d 294, 295-96 (Ala. 1979)), our Court explained that a plaintiff must allege the following in order to establish a claim of negligence per se:

"(1) The statute must have been 'enacted to protect a class of persons which includes the litigant seeking to assert the statute';

"(2) The injury complained of must be 'of a type contemplated by the statute';

⁹HIPAA, as amended, is codified in various sections of Titles 18, 26, 29, and 42 of the United States Code.

"(3) 'The party charged with negligent conduct must have violated the statute'; and

"(4) 'The jury must find [that] the statutory violation proximately caused the injury.'"

(Emphasis added.)

Here, although Griggs relies on Delchamps in support of her assertions related to her negligence per se claim, she does not point to a violation of any specific statutory provisions in either HIPAA or the FTCA in arguing that those statutes created a duty for her employer, NHS. Instead, all of her allegations in her complaint concern HIPAA violations based upon violations of HIPAA regulations.¹⁰

¹⁰While Delchamps spoke about only violations of a "statute" providing a basis for a negligence per se claim, it also discussed alleged regulatory violations. Regardless, we are bound by the words quoted above -- words that have been repeated in other decisions. See, generally, Fox v. Bartholf, 374 So. 2d 294, 295-96 (Ala. 1979) (articulating the elements necessary for a negligence per se cause of action based on "the amalgam of Alabama case law," which are all based on statutory violations).

Moreover, I would be especially concerned with extending the words of Delchamps when a broader rule would cause significant constitutional and prudential concerns. For instance, allowing regulations issued by an agency (not a legislature) to create private legal liability would cause serious separation-of-powers concerns. These concerns are heightened because the legislative branch made a deliberate decision to vest

Further, Griggs makes no effort to explain how any of the other elements quoted in Delchamps have been met here. For instance, Delchamps requires that the "statute must have been 'enacted to protect a class of persons which includes the litigant seeking to assert the statute.'" 624 So. 2d at 1067 (emphasis added; citation omitted). Here,

enforcement powers in only a regulatory agency and not in private parties.

Such an extension would also create federalism concerns. These regulations were issued by an entirely different sovereign -- the federal government. Because of this federalism concern, there would be other practical problems that such an expansion of liability standards would bring. Defendants in future cases could (and I am sure would) attack such regulations as improper under federal law -- that is, as being inconsistent with the federal legislation authorizing the regulation or otherwise arbitrary and capricious. Courts in our State would then need to determine the validity of federal regulations under federal law. See Loper Bright Enters. v. Raimondo, 603 U.S. ___, 144 S. Ct. 2244 (2024) (explaining that courts should not defer to agency interpretation of an ambiguity in a law that the agency enforces). In sum, if Alabama wishes to subcontract its decision to create tort claims to federal agencies, our Legislature rather than our Court needs to make such a significant decision.

Finally, the text of the Delchamps decision is ambiguous as to whether it is ruling on the "duty" question or the "standard of care" question. Delchamps, 624 So. 2d at 1068. The question before our Court today is a question of duty, and I do not reach the question whether a federal regulation might (or might not) constitute evidence of a standard of care for a state-law tort claim in particular situations.

SC-2023-0784

Griggs is an employee, not a medical patient, yet she seeks application of the data provisions found in HIPAA with no explanation for why she is in the "class of persons" protected by HIPAA.

The only other case that Griggs cites on this point is Smith v. Triad of Alabama LLC (Case No. 1:14-CV-324-WKW, Sept. 29, 2015) (M.D. Ala. 2015) (not reported in Federal Supplement). Smith was a medical-data-breach case that involved allegations invoking HIPAA. In that case, the United States District Court for the Middle District of Alabama cited our Court's decision in Delchamps for its negligence per se analysis, and it is therefore distinguishable for the same reasons that Delchamps is distinguishable. Smith is also distinguishable because the plaintiffs in that case were medical patients. In other words, unlike in this case, in Smith there were allegations showing that the plaintiffs were part of the "class of persons" protected by HIPAA.

Additionally, Griggs's argument that NHS owed her a duty under the FTCA is even weaker. In support of this assertion, Griggs, in her complaint, relied on (1) a nonbinding "publication" (Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016)), and (2) an administrative decision (citing In the Matter of LabMD, Inc.,

2016-2 Trade Cas. (CCH), ¶ 79708 (July 28, 2016)). I find neither of these sources to be compelling or persuasive on this point because (1) Griggs cites no caselaw in which a court has found negligence per se based upon such a "publication" and (2) the administrative decision has been vacated (something that Griggs fails to mention). See LabMD, Inc. v. Federal Trade Commission, 894 F.3d 1221 (11th Cir. 2018). Moreover, neither of these sources indicate that the FTCA creates a duty for an employer to protect an employee's personal information from a cyberattack.

If a plaintiff in a future data-breach case were to raise a negligence per se claim similar to the one that Griggs alleges here, he or she would have to plead (at least) that he or she was part of the actual "class of persons" that the statute he or she is relying on was enacted to protect and that the injury complained of -- the theft of personal information as a result of a cyberattack -- was "contemplated by the statute." He or she would also have to plead (at least) that the defendant not only violated the statute but that the injury complained of proximately caused the injury. Without such allegations, a plaintiff may not be able to proceed with his or her negligence per se claim.

IV. Even If a Duty Exists in a Data-Breach Case, a Plaintiff Must

Still Plead That He or She Suffered Damages As a Result of Any Alleged Breach of a Duty to Protect Personal Information

Finally, even if we were to assume that a duty can arise in the circumstances alleged by Griggs here for either her negligence or negligence per se claims, a plaintiff in a future case would still need to show that he or she suffered damage as a result of the data breach.¹¹ Current Alabama law makes clear that the risk of damage is not enough to recover. Instead, Alabama law requires the existence of "a manifest, present injury before a plaintiff may recover in tort." Southern Bakeries, Inc. v. Knipp, 852 So. 2d 712, 716 (Ala. 2002) (citing Hinton ex rel. Hinton v. Monsanto Co., 813 So. 2d 827, 829 (Ala. 2001) (plurality opinion); DeArman v. Liberty Nat'l Ins. Co., 786 So. 2d 1090 (Ala. 2000); Stringfellow v. State Farm Life Ins. Co., 743 So. 2d 439 (Ala. 1999); Williamson v. Indianapolis Life Ins. Co., 741 So. 2d 1057 (Ala. 1999); and

¹¹To be clear, I am not referring to standing here, and I therefore am not opining on whether standing applies to private-law negligence claims. Instead, I mean that the fact of damage is an element of a negligence claim. See, e.g., Hilyer v. Fortier, 227 So. 3d 13, 22 (Ala. 2017) (noting that, "[t]o establish negligence, the plaintiff must prove: (1) a duty to a foreseeable plaintiff; (2) a breach of that duty; (3) proximate causation; and (4) damage or injury" (quoting Lemley v. Wilson, 178 So. 3d 834, 841 (Ala. 2015), quoting in turn Martin v. Arnold, 643 So. 2d 564, 567 (Ala. 1994))).

Pfizer, Inc. v. Farsian, 682 So. 2d 405 (Ala. 1996)).

Counsel for Griggs was asked twice at oral argument whether Griggs had incurred actual out-of-pocket damages as a result of the data breach in this case. In both instances, counsel for Griggs could not provide a specific answer to that question. See Supreme Court of Alabama, Supreme Court O/A Jacksonville Alabama, YouTube (Sept. 19, 2024, 27:08-27:26; 27:26-27:33; 28:09-28:37; 28:37-31:05) (at the time this decision was issued, this oral-argument session could be located at: <https://www.youtube.com/watch?v=jMUTOkd1tYk>). In my view, given this concession and the examples of damages pleaded in the complaint, it is not plausible that Griggs can establish a "manifest, present injury." Counsel for NHS similarly argued that it was not plausible that such a proximately caused actual damage existed today.

With all of this said, this case is at the pleading stage and not yet at the summary-judgment stage. Alabama is a notice-pleading state. Extensive caselaw (including cases that I have authored) states that a dismissal on the pleadings is not allowed if ""it appears that the pleader could prove any set of circumstances that would entitle her to relief."" Flickinger v. King, 385 So. 3d 504, 511 (Ala. 2023) (emphasis altered;

citations omitted). Further, our caselaw makes clear that, at the pleading stage, the question is not "" whether the plaintiff will ultimately prevail, but only whether she may possibly prevail."" Id. (citations omitted).

At oral argument, counsel for NHS could not deny that there were "any set of circumstances" that would constitute damage. Thus, the problem with my conclusion and the acknowledgement by NHS's counsel during oral argument is that plausibility is not the pleading standard today in Alabama. Because of this, I cannot rely upon the lack of actual damages to affirm the dismissal on the pleadings and must instead base my concurrence on the other issues discussed above.

In contrast to Alabama's pleading standard, I note that federal courts do consider whether a plausible claim has been pleaded. See, generally, Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007), and Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009) (requiring that the complaint state a "plausible claim"). Notably, the substance of the relevant Alabama rules of civil procedure are identical to the relevant federal rules of civil procedure. Compare Rules 8 and 12, Ala. R. Civ. P., with Rules 8 and 12, Fed. R. Civ. P.

I have previously noted this inconsistency between the Alabama

and the federal pleading standards in a special writing and have invited parties to raise this question in an appropriate case. See Ex parte McKesson Corp., [Ms. SC-2023-0289, Dec. 22, 2023] ___ So. 3d ___, ___ n.6 (Ala. 2023) (Cook, J., concurring in the result) ("I make this observation in the hope that future litigants may consider raising this issue in an appropriate case for our Court to fully consider after input from members of the public wishing to file amicus briefs (including whether the heightened standard might be appropriate in all cases or only in a subset of cases).").

Yet, NHS has not asked us to reconsider our current pleading standard and adopt the federal pleading standard as discussed in Iqbal and Twombly, supra. Absent extraordinary circumstances, our Court will not reach out and overrule past precedent without an express request to do so. See, e.g., American Bankers Ins. Co. of Florida v. Tellis, 192 So. 3d 386, 392 n.3 (Ala. 2015) (noting that the Court follows "'controlling precedent'" unless "'invited to'" overrule it (citation omitted)). However, I raise this issue here to once again invite parties in a future appropriate case to argue whether we should reconsider our pleading standard in light of the federal pleading standard.

V. Conclusion

It is for all of these reasons that I agree that the circuit court's dismissal of Griggs's data-breach action against NHS is due to be affirmed.

SHAW, Justice (concurring in the result)

I concur in the result. Additionally, I note the following.

I agree that the plaintiff below, Shymikka Griggs, has not demonstrated on appeal that the dismissal of her negligence claim is due to be reversed. In its motion to dismiss, the defendant below, NHS Management, LLC ("NHS"), acknowledged the elements of a negligence action, which, generally stated, require a plaintiff to show a duty, a breach of that duty, causation, and damages. But NHS argued that no legal duty existed in this case. Specifically, NHS cited caselaw and provided a discussion of the various factors and considerations used to determine when the law imposes a duty and argued that, under that authority and analysis, no duty existed in this case. See, e.g., DiBiasi v. Joe Wheeler Elec. Membership Corp., 988 So. 2d 454, 461-63 (Ala. 2008) (discussing "a number of factors [used] to determine whether a duty exists" and noting that the foreseeability of a risk of harm alone can be insufficient to create such a duty), and New Addition Club, Inc. v. Vaughn, 903 So. 2d 68, 73-76 (Ala. 2004) (discussing when one has a duty to protect another from the criminal acts of a third person). Whether a duty exists is a question of law. Bryan v. Alabama Power Co., 20 So. 3d

SC-2023-0784

108, 116 (Ala. 2009). It can be a complicated issue. See DiBiasi and New Addition Club, supra. The trial court, which did not specify the reasons for its dismissal, could have accepted NHS's argument.

Thus, it was incumbent upon Griggs, in her initial brief on appeal, to present a legal argument as to whether the law imposes a duty in this case, or the issue is deemed waived. Soutullo v. Mobile Cnty., 58 So. 3d 733, 739 (Ala. 2010), and Fogarty v. Southworth, 953 So. 2d 1225, 1232 (Ala. 2006). While Griggs argues on appeal that her complaint alleged that a duty existed and alleged that there was a foreseeable risk, this does not address the issue, presented to the trial court, that, despite those allegations, no duty existed. Although I am not wholly convinced that, in a case like this, the law will not impose a duty for purposes of a negligence action, the issue has been waived.