CASE NO. SC-23-0784

THE SUPREME COURT OF ALABAMA

SHYMIKKA GRIGGS,

on behalf of herself and all others similarly situated,

Appellant

vs.

NHS MANAGEMENT, LLC

Appellee

On Appeal from the Circuit Court
Of Jefferson County, Alabama
(Circuit Court No.: CV-23-902261)

BRIEF OF APPELLANT

Taylor C. Bartlett, Esq.
HENINGER GARRISON & DAVIS, LLC
2224 1ST Avenue North
Birmingham, Alabama 35203
T: 205.326.3336
F: 205.380.8085
Email: taylor@hgdlawfirm.com

STATEMENT REGARDING ORAL ARGUMENT

Plaintiff-Appellant contends that the facts and law of this case are simple and capable of review and disposition upon written briefs. However, because the subject matter of this action (a massive data breach of highly sensitive personal information) is one of first impression before this Court, Appellant requests oral argument to aid the decisional process with argument from the parties.

TABLE OF CONTENTS

Page

STATEMENT OF JURISDICTION

The Supreme Court of Alabama has exclusive jurisdiction over all Alabama lower court appeals where the amount in controversy exceeds fifty thousand dollars ($50,000). Here, Plaintiff-Appellant Shymikka Griggs, on behalf of herself and a putative class of similarly situated individuals, brought this action against Defendant-Appellee NHS Management, LLC for its failure to protect the highly sensitive personal information of thousands of individuals. At the trial court, Plaintiff sought monetary relief exceeding fifty thousand dollars and equitable relief.

A final appealable judgment was entered by the Circuit Court of Jefferson County, Alabama, Birmingham Division, on October 10, 2023. There are no other claims remaining before the Circuit Court, and no other motions or orders have been filed since the entry of final judgment on October 10, 2023. *See, e.g.*, *Hinson v. Hinson*, 745 So. 2d 280, 281 (Ala. Civ. App. 1999) (citing *Taylor v. Taylor*, 398 So. 2d 267, 269 (Ala. 1981)).

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

STATEMENT OF THE CASE

This data breach class action was filed by Plaintiff-Appellant Griggs in the Circuit Court of Jefferson County on June 30, 2023. (C. 8–76). On August 5, 2023, NHS moved to dismiss Plaintiff-Appellant's suit pursuant to Alabama Rule of Civil Procedure 12(b)(1), claiming the Circuit Court did not have subject matter jurisdiction based on lack of standing, and pursuant to Rule 12(b)(6) for failure to state a claim upon which relief could be granted. (C. 81–117). Plaintiff opposed NHS's motion to dismiss (C. 147–81), seeking leave to amend should any portion of the motion be granted. (C. 180). NHS's filed a reply in support of its motion (C. 182–202), after which the parties participated in oral arguments.

On October 10, 2023, the Circuit Court entered an order granting NHS's Motion to Dismiss with prejudice, simply stating that the Defendant's motion was due to be granted. (C. 203, "Order"). Yet the Circuit Court provided no further explanation and gave Plaintiff no leave to amend. (*Id.*).

The Circuit Court's Order resolved all pending issues. Plaintiff-Appellant filed a timely Notice of Appeal with security for costs on October 26, 2023. (C. 204–07).

STATEMENT OF THE ISSUES

1. Whether the Circuit Court erred in dismissing Plaintiff-Appellant Griggs' complaint with prejudice where Plaintiff alleged that she is a real party in interest, who has stated causes of actions and injuries-in-fact related to her legally protected privacy rights, for which she could be "entitled to a remedy." *Jakeman v. Lawrence Grp. Mgmt. Co., LLC*, 151 So. 3d 1083, 1087–88 (Ala. 2014) (quoting *Ex parte BAC Home Loans Servicing, LP,* 159 So. 3d 31, 44–45 (Ala. 2013)).

2. Whether the Circuit Court erred in dismissing Plaintiff-Appellant Griggs' complaint with prejudice and without explanation, when the allegations of the complaint are to be viewed "most strongly in the pleader's favor," and a matter should be dismissed "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." *Young Ams. for Liberty v. Finis St. John IV*, No. 1210309, -- So. 3d --, 2022 WL 17073690, at *2, *4 (Ala. Nov. 18, 2022) (reversing dismissal and remanding to circuit court) (quoting *Nance ex rel. Nance v. Matthews,* 622 So. 2d 297, 299 (Ala. 1993)).

STATEMENT OF THE FACTS

I. Procedural History

On May 4, 2022, Plaintiff[1] Griggs brought this matter as a class action in the United States District Court for the Northern District of Alabama (Case No. 2:22-cv-00565-RDP, "N.D. Ala. Case"), citing minimal diversity under the Class Action Fairness Act ("CAFA"). After the parties fully briefed NHS's motion to dismiss (ECF Nos. 14, 17, 18), the federal court *sua sponte* questioned whether it had subject matter jurisdiction, and even if minimal diversity existed, whether the "local controversy" exception applied; and whether it had the discretion to decline jurisdiction under the discretionary exception of CAFA (N.D. Ala. Case, *id.* at ECF No. 25). Both parties provided supplemental briefing, based on NHS's admission that approximately 100,000 Data Breach Notices were sent to NHS Data Breach victims in all 50 states, with the majority (75,783) being sent to Alabama addresses (*id.* at ECF Nos. 26–27). The parties agreed that: 1) minimal diversity under CAFA was met; 2) that the "local controversy" does not apply; and 3) that the Court should not

[1] Plaintiff-Appellant Shymikka Griggs will be referred to as "Plaintiff" and Defendant-Appellee NHS Management, LLC will be referred to as "NHS" throughout this brief.

exercise its discretion to decline CAFA jurisdiction. Nevertheless, the federal court ordered that Plaintiff must refile an amended complaint, "appropriately address[ing] the citizenship of putative class members." (*Id.* at ECF No. 29, entered on June 26, 2023). Importantly, the federal court never entered a substantive order regarding the merits of Plaintiff's case or NHS's motion to dismiss.

Given the near impossible task of accurately addressing the citizenship (not residency) of approximately 100,000 putative class members whose identities are unknown except to NHS, Plaintiff voluntarily dismissed her federal complaint without prejudice. (*Id.* at ECF Nos. 30–31).

On June 30, 2023, Plaintiff refiled her complaint in the Circuit Court of Jefferson County, Alabama. (C. 8–76).[2] NHS moved to dismiss the complaint on August 5, 2023. (C. 81). and the parties fully briefed that motion and response. (Mot., C. 81–117; Opp., C. 147–81; Reply, C. 182–202). On October 2, 2023, the Circuit Judge heard oral arguments in the matter. (*See* Order (setting hearing date and time), C. 118).

[2] The only record on appeal is the Clerk's Record, for which all page numbers are referenced as C. [page number] pursuant to Rule 28(g).

On October 10, 2023, the court entered its Order dismissing the case, simply stating that the Defendant's motion is due to be granted under Rule 12(b), without further detail. (C. 203). Like the federal court, the Circuit Court never entered a substantive order regarding the merits of Plaintiff's case, nor provided any detailed bases for granting NHS's motion to dismiss. (*Id.*).

II. Statement of Facts

A. NHS's failures related to its "Sophisticated Cyberattack."

This data breach and privacy class action arose out of what NHS describes as a "sophisticated cyberattack" (the "Data Breach") on its computer network that NHS first discovered about May 16, 2021. (C. 17; s*ee also* C. 73–76, Plaintiff's "Notice Letter" attached as Exhibit A to Complaint). Upon investigation, NHS realized that cybercriminals gained unfettered access to its network between February 25, 2021 and May 16, 2021, an *eighty day period* of time before its discovery. (C. 17 ¶ 28).

When a healthcare related company, like NHS, experiences a data breach that affects more than 500 individuals, as NHS did here, the regulations of the U.S. Department of Health and Human Services

("HHS") require that the company notify HSS "without unreasonable delay and in no case later than 60 days following a breach." (C. 18 ¶ 31). Yet, NHS delayed over five months after discovering its Data Breach, first notifying NHS on October 29, 2021. (*Id.*). And NHS did not begin notifying the Data Breach victims (*i.e.*, putative class members) until about March 31, 2022, *over a year* after the Data Breach began and *ten and one-half months* after it first learned of the Data Breach. (C. 18–19, ¶ 32). NHS's extremely delayed notice to victims, including Plaintiff, violates HIPAA's Breach Notification Rules, which require that "individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach." (*Id.*[3]). Likewise, NHS's delay in identifying and reporting the Data Breach caused additional injuries to Plaintiff and the Class. (C. 47 ¶ 133). In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. (*Id.*) Early notification helps data breach victims mitigate their own injuries, and in the converse, delayed notification causes more harm and increases their risk of identity theft. (*Id.*).

[3] Note: the Alabama Data Breach Notification Act of 2018 requires notification within 45 days, but this Act was not cited in the complaint.

NHS Management provides administrative services for skilled nursing and physical rehabilitation centers located in four states: Alabama, Arkansas, Florida, and Missouri. (C. 14–15 ¶¶ 21–22). Its services include operational expertise, financial analysis, clinical expertise, business office support including accounts payable, purchasing, marketing, technology, human resource systems such as payroll, and strategic planning. (*Id.*). In the course of its business, NHS collects both highly sensitive personally identifiable information[4] and HIPAA protected health information.[5] (C. 10–11). Furthermore, its voluminous cache of personal data is collected from its own current and former employees and vendors, as well as from the patients and residents of the facilities that NHS serves, their family members, and guardians. (C. 15 ¶ 23; *see also* C. 73–76). If an individual refused to provide the required information, NHS would be unlikely to employ the individual or

[4] Personally identifiable information, called "PII," includes names, dates of birth, Social Security numbers, and contact information. (C. 10–11 ¶ 4).

[5] Health care-specific data, as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), is referred to as protected health information "PHI." (C. 10 ¶ 4).

vendor, or the related nursing facility would be unlikely to admit the patient/resident. (C. 15 ¶ 23).

According to the March 31, 2022, Notice Letter that NHS sent to Plaintiff (C. 73–76), who is a former employee of NHS (C. 41 ¶ 104), as well as the undated notice NHS posted on its website (*see* C. 17 n.6), NHS "determined that an unauthorized actor accessed certain NHS systems and information stored therein between February 25, 2021 and May 16, 2021." (*Id.*) On NHS's website notice, it admitted that the breached information included individual's names; addresses; contact information; Social Security numbers; dates of birth; driver's license numbers; medical history; treatment or diagnosis information; and health insurance information. (C. 17 n.6). In other words, the data breached was the highly sensitive and immutable data used by criminals when using another person's identity for fraudulent purposes, *i.e.*, name, contact information, date of birth, and Social Security number. (C. 11–12 ¶¶ 9–10). It also explained that "[d]etails on what information may have been impacted per individual will be provided via written notice to those for whom we have valid mailing addresses." (C. 17 n.6). Thereafter, Plaintiff Griggs learned directly from NHS that her "name, date of birth, Social Security

number, medical information, and health insurance information" were among the data breached. (C. 74).

B. NHS had a duty and ability to protect data.

This Data Breach never should have happened. The data that NHS collects and stores on its computer network is subject to the protection of the FTC Act, HIPAA, common law, and statutory law. (C. 19 ¶ 35; C. 29–31 ¶¶ 63–68; C. 32 ¶¶ 74–75; C. 33–34 ¶¶ 77–81). A breach of this sort is a failure by NHS to recognize that it has legal responsibilities that arise from the moment it collects and stores highly sensitive data; a failure by NHS to adequately protect its computer network; and especially a failure by NHS to sufficiently monitor its computer network so that if a breach does occur, it is able to mitigate damages quickly. (*E.g.*, C. 16 ¶ 25; C. 20–22 ¶¶ 38(a)–(m)). As Plaintiff's Complaint explains in great detail, the risks of experiencing a criminal cyberattack are well known, especially for entities that collect and store a wealth of PII and PHI. (*E.g.*, C. 19 ¶ 37; C. 25–29). NHS's failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII and PHI of its employees and vendors, as well as the patients/residents and their family members and guardians constitutes an unfair act or practice prohibited

by Section 5 of the FTC Act, 15 U.S.C. § 45. (*e.g.*, C. 31 ¶ 70). Moreover, NHS is a business associate of a "covered entity" under HIPAA and it must implement safeguards to ensure the confidentiality, integrity, and availability of PHI, including physical, technical and administrative components. (C. 33 ¶ 78). It did not.

Several best practices have been identified that at a minimum should be implemented by healthcare management companies like NHS, including but not limited to implementing: training for all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and restrictions on which employees can access sensitive data. (C. 31 ¶ 73). NHS failed to follow these industry best practices, including a failure to implement multi-factor authentication. (*Id.*) Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protecting against any possible

communication breach; and training staff regarding critical points. (C. 32 ¶ 74). NHS failed to follow these cybersecurity best practices, including failure to train staff. (*Id.*). Its admitted failure to notice the Data Breach for a period of 80 days, alone, evidences its failure to monitor for breaches. (C. 17 ¶ 28).

Although cybercriminals have become more sophisticated, businesses like NHS that collect and store the PII and PHI of individuals *still* have a duty to protect that data, and they must also become more sophisticated and diligent with their data security and network monitoring. (C. 19 ¶¶ 35–37). NHS recognizes this duty when it admits in its Notice Letters that, after the Data Breach, it began "reviewing and enhancing its existing policies and procedures to reduce the likelihood of a similar future event." (C. 73–76).

C. Plaintiff and putative class members suffered injuries.

Plaintiff and other similarly situated individuals have suffered injuries due to NHS's failure to protect their Private Information as it has a legal duty to do.

Plaintiff has already suffered identity theft from NHS's Data Breach. Since NHS's Data Breach, Plaintiff has been notified by Credit

Karma that her PII was found on many different sites on the "dark web," requiring her to spend time freezing her credit and correcting errors on her credit reports. (C. 41 ¶ 108). She has received a high number of spam emails, calls, and texts each day, which are both annoying and time-consuming. (C. 41 ¶ 109). She was contacted by Apple's fraud department regarding approximately $3,000 in Apple product purchases fraudulently made in her name. (C. 42 ¶ 110). Plaintiff has received harassing phone calls and emails stating that she owes money for "payday loans," which she believes resulted from the sale of her PII on the dark web after the NHS Data Breach. (C. 42 ¶ 111). In addition, she is required to—upon the advice of NHS in her Notice Letter (*see* C. 75)—spend time closely monitoring her financial accounts, trying to mitigate her own injuries, efforts which are likely to continue for years to come. (C. 42 ¶¶ 112–16).

In addition to these specific instances of harm experienced by Plaintiff, she and all putative class members face an ongoing and imminent risk of identity fraud, have already experienced fraud, and suffer fear, anxiety and stress over the breach of their PII and PHI. (C. 45–46 ¶¶ 128–30). Plaintiff and class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, credit

card fraud, tax return fraud, medical services billed in their names, utility bills opened in their names, and similar identity theft. (C. 44 ¶ 122).

Plaintiff and class members suffered a loss of value of their Personal Information when it was acquired by cyber thieves in the Data Breach. (C. 44 ¶ 125). Plaintiff and class members were also damaged in losing the benefit-of-the-bargain between themselves and Defendant. (C. 44 ¶¶ 126–27). In addition, Plaintiff's complaint is replete with the injuries she and putative class members have or will imminently suffer from NHS's Data Breach. (*See, e.g.*, C. 12 ¶¶ 10 (heightened risk of fraud), 11 (out-of-pocket costs), 12 (lost time); *see also* C. 43–47).

D. NHS's limited relief is insufficient.

Through its notice letters, NHS offered just one year of credit monitoring services and "identity theft restoration" through Kroll, a tacit admission that its failure to protect their PII and PHI has harmed Plaintiff and putative class members. (C. 43 ¶ 117; *see also* C. 75). This one-year limitation is inadequate when victims are likely to face many years of identity theft, especially when Social Security numbers are breached. (C. 43–44 ¶¶ 116–20). Here, hackers misappropriated Social

Security numbers, personally identifiable information, protected health information alongside basic contact information—this is everything a fraudster needs to take over a person's identity, open fraudulent loans, commit credit card fraud, bill medical services in their names, tax return fraud, and so on. (*E.g.*, C. 37–38; C. 44 ¶¶ 121–24). Clearly, such information does not lose its usefulness to hackers after just one year. (C. 43 ¶ 117).

E. Plaintiff sought relief through this action.

Through her complaint filed on June 30, 2023, Plaintiff seeks relief on behalf of herself and a class of similarly situated individuals to address NHS's inadequate safeguarding of their PHI and PII, and for its failure to provide adequate and timely notice to these individuals of the Data Breach. (C. 11 ¶ 5). Plaintiff seeks remedies including but not limited to compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, and adequate credit monitoring services. (C. 13 ¶ 15). Plaintiff asserted claims for negligence, negligence *per se*, breach of implied contract, invasion of privacy, unjust enrichment, breach of confidence, and breach of fiduciary duty. (C. 13 ¶ 16).

On August 5, 2023, NHS moved to dismiss Plaintiff's suit. (C. 81–117). Plaintiff opposed NHS's motion to dismiss (C. 147–81) and sought leave to amend should any portion of the motion be granted. (C. 180). NHS filed a reply in support of its motion. (C. 182–202). On October 10, 2023, the Circuit Court dismissed the entire case with prejudice. (C. 203). Plaintiff filed a timely notice of appeal on October 26, 2023. (C. 204–07).

STATEMENT OF THE STANDARD OF REVIEW

The Alabama Supreme Court's review of a circuit court's judgment of dismissal is *de novo*, "regardless of whether the judgment was entered under Rule 12(b)(1), Ala. R. Civ. P., for lack of subject-matter jurisdiction, or under Rule 12(b)(6), Ala. R. Civ. P., for failure to state a claim." *Johnson v. Ala. Sec'y of Lab. Fitzgerald Washington*, No. SC-2022-0897, 2023 WL 4281620, at *2 (Ala. June 30, 2023), *cert. granted sub nom. Williams v. Washington, AL Sec. of Lab.*, No. 23-191, 2024 WL 133549 (U.S. Jan. 12, 2024) (citing *DuBose v. Weaver*, 68 So. 3d 814, 821 (Ala. 2011); and *Bay Lines, Inc. v. Stoughton Trailers, Inc.*, 838 So. 2d 1013, 1017–18 (Ala. 2002)).

On appeal, no presumption of correctness is given to dismissal in the trial court. "'We review de novo whether the trial court had subject-matter jurisdiction.'" *Hudson v. Ivey*, No. SC-2022-0836, __ So. 3d __, 2023 WL 2620607, at *2 (Ala. Mar. 24, 2023) (citing *Taylor v. Paradise Missionary Baptist Church*, 242 So. 3d 979, 986 (Ala. 2017) (quoting *Solomon v. Liberty Nat'l Life Ins. Co.*, 953 So. 2d 1211, 1218 (Ala. 2006))).

Similarly, "'[w]here a [Rule] 12(b)(6)[, Ala. R. Civ. P.,] motion has been granted and this Court is called upon to review the dismissal of the

complaint, we must examine the allegations contained therein and construe them so as to resolve all doubts concerning the sufficiency of the complaint in favor of the plaintiff. . . . In so doing, this Court does not consider whether the plaintiff will ultimately prevail, only whether he has stated a claim under which he may possibly prevail.'" *Roberson v. Balch & Bingham, LLP*, 358 So. 3d 1118, 1126 (Ala. 2022) (quoting *Pearce v. Schrimsher*, 583 So. 2d 253, 253–54 (Ala. 1991)) (additional internal citations omitted).

SUMMARY OF THE ARGUMENT

The Circuit Court erred when it dismissed Plaintiff's complaint on the pleadings pursuant to Ala. R. Civ. P. 12(b) with prejudice, and without leave to amend. Notably, the Circuit Court neither explained its dismissal, nor identified whether the dismissal was pursuant to NHS's Rule 12(b)(1) "standing" argument or pursuant to its Rule 12(b)(6) failure to state a claim argument. However, both paths lead to the same conclusion: the Circuit Court erred when it dismissed Plaintiff's case.

A. The Circuit Court erred dismissing under Ala. R. Civ. P. 12(b)(1).

In its motion to dismiss, NHS's Rule 12(b)(1) "standing" argument (C. 94–102) conflated Article III standing with this Court's precedent under the Alabama Constitution and this Court's recent caselaw. NHS then doubled down on its analytical error in its reply in support of the motion (C. 188–94), factually attacking Plaintiff's injury allegations rather than addressing whether Plaintiff is a proper party to bring this action.

This Court has long explained that "the concept of standing under the Alabama Constitution is different than it is under the United States Constitution." *Milton v. Haywood*, No. SC-2023-0382, -- So. 3d --, 2023

WL 8855663, at *5 (Ala. Dec. 22, 2023) (Parker, C.J., concurring). "Under the Alabama Constitution, '[t]o say that a person has standing is to say that that person is the proper party to bring the action. To be a proper party, the person must have a real, tangible legal interest in the subject matter of the lawsuit.'" *Id.* (quoting *Town of Cedar Bluff v. Citizens Caring for Children*, 904 So. 2d 1253, 1256 (Ala. 2004) (quoting *Doremus v. Bus. Council of Ala. Workers' Comp. Self-Insurer's Fund*, 686 So. 2d 252, 253 (Ala. 1996)) (emphasis in *Milton* concurrence).

Here, Plaintiff has sufficiently alleged that she is a proper party to bring this action. In other words, she is a "real party in interest" as a former employee of NHS who was notified by NHS that her "name, date of birth, Social Security number, medical information, and health insurance information" were among the data accessed during what NHS calls a "sophisticated cyberattack" on its computer network. She provided extensive factual support regarding the preventability, risks, harm caused by NHS's failure to adequately protect and monitor its computer network as required by the FTC Act, HIPAA, common law, and statutes, as well as its failure to timely notify the victims whose data was breached. Her causes of action for negligence, negligence *per se*, breach

of implied contract, invasion of privacy, unjust enrichment, breach of confidence, and breach of fiduciary duty each arise from NHS's failure to adequately protect and monitor its computer network. And she alleged that has suffered injuries-in-fact (including but not limited to fraudulent loans, identity theft, lost time, and a substantial and imminent risk of future risks) related to her legally protected privacy rights, and for which she could be "entitled to a remedy." *Jakeman*, 151 So. 3d at 1088. These allegations are sufficient for Plaintiff to thwart an Ala. R. Civ. P. 12(b)(1) dismissal.

B. The Circuit Court erred dismissing under Ala. R. Civ. P. 12(b)(6).

The Circuit Court also erred when it did not consider the allegations of Plaintiff's complaint "most strongly in the pleader's favor." It is well-settled precedent in Alabama that a matter should be dismissed only if there is "no set of facts in support of the claim that would entitle the plaintiff to relief." *Nance,* 622 So. 2d at 299 (citing *Raley v. Citibanc of Ala./Andalusia*, 474 So. 2d 640, 641 (Ala. 1985); *Hill v. Falletta*, 589 So. 2d 746 (Ala. Civ. App. 1991)). "Dismissals under Rule 12(b)(6) should be granted sparingly, and such a dismissal is proper only when it appears beyond doubt that the plaintiff can prove no set of facts in support of the

claim which would entitle him or her to relief." *Garrett v. Hadden*, 495 So. 2d 616, 617 (Ala. 1986) (citing Committee Comments to Rule 8, Ala. R. Civ. P.; *Roberts v. Meeks,* 397 So. 2d 111 (Ala. 1981)).

For each of her causes of action, Plaintiff's allegations, when considered most strongly in her favor, support that she is entitled to relief on behalf of herself and a class of similarly situated individuals whose PII and PHI was breached on NHS's insufficiently protected and monitored computer network. Furthermore, NHS's failure to protect the PII and PHI that it collected and stored, as well as its excessive delay reporting the breach to both the HHS and individual victims, violated its duties under HIPAA, the FTC Act, common law, and statutes.

Plaintiff's allegations, when considered in light of NHS's duties and its public admissions, are sufficient to withstand dismissal under Rule 12(b)(6). The Circuit Court erred in dismissing her case for failure to state a claim for relief.

ARGUMENT

I. The Circuit Court erred in dismissing Plaintiff's complaint as a real party in interest, who has stated causes of actions and injuries-in-fact related to legally protected privacy rights, for which she could be "entitled to a remedy."

The Circuit Court erred in dismissing Plaintiff's complaint with prejudice where Plaintiff sufficiently alleged that: 1) she is a real party in interest, 2) who has stated causes of actions and injuries-in-fact related to legally protected privacy rights, and 3) for which she could be "entitled to a remedy." *Jakeman*, 151 So. 3d at 1088.

In its motion to dismiss, NHS's "standing" argument (C. 94–102) conflated Article III standing from the federal courts with standing as it is interpreted by this Court under the Alabama Constitution. *See, e.g.*, *Ex parte BAC Home Loans Servicing, LP,* 159 So.3d at 44 ("the concept of standing was developed by the United States Supreme Court for 'public law' cases."). Then, in its reply brief, rather than acknowledging this Court's precedent and addressing misdirection, NHS doubled down on its own belief that *BAC Home Loans* needs to be revaluated based on U.S. Supreme Court precedent (C. 188 (citing *Key v. Warren Averett, LLC*, 372 So. 3d 1132, 1142 (Ala. 2022) (Mitchell, J., concurring)). However, what NHS failed altogether to address in its motion to dismiss (C. 93–102) and

in its reply brief (C. 188–94) was whether Plaintiff Griggs is a proper party to bring this action.

This Court has long explained that "the concept of standing under the Alabama Constitution is different than it is under the United States Constitution." *Milton*, -- So. 3d --, 2023 WL 8855663, at *5 (Ala. Dec. 22, 2023) (Parker, C.J., concurring). "Under the Alabama Constitution, '[t]o say that a person has standing is to say that that person is the proper party to bring the action. To be a proper party, the person must have a real, tangible legal interest in the subject matter of the lawsuit.'" *Id.* (quoting *Town of Cedar Bluff*, 904 So. 2d at 1256 (quoting *Doremus*, 686 So. 2d at 253) (emphasis original in *Milton* concurrence).

The Alabama Supreme Court, in *Ex parte BAC Home Loans Servicing, LP*, 159 So. 3d at 31, "examined the concept of standing and cautioned that the concept is generally relevant only in public-law cases." 159 So. 3d at 44–45. In *BAC Home Loans*, the Court quoted Professor Hoffman, "a professor with a more intimate awareness of Alabama cases [than Wright and Miller] and the invocation therein of the doctrine of standing":

> '[T]he word "standing" unnecessarily invoked in the proposition can be erroneously equated with "real party in

> interest" or "failure to state a claim." This simple, though doctrinally unjustified, extension could swallow up Rule 12(b)(6), Rule 17[, Ala. R. Civ. P.,] and the whole law of amendments.'

159 So. 3d at 46 (quoting Hoffman, *The Malignant Mystique of "Standing"*, 73 Ala. Law. 360, 362 (2012)). As this Court explained, in private-law actions in Alabama, "if the elements are met, the plaintiff is entitled to judicial intervention; if they are not met, then the plaintiff is not entitled to judicial intervention. Everything necessary to justify judicial intervention, by definition, inheres in those elements that we say constitute a 'cause of action' in and by our courts." 159 So. 3d at 44. "If in the end the facts do not support the plaintiff[], or the law does not do so, so be it—but this does not mean the plaintiff[] cannot come into court and allege, and attempt to prove, otherwise." *Id.* at 46. If a plaintiff fails to prove the elements of her claim, it is not that she has a "standing" problem, but instead, she may have a "failure to prove one's cause of action" problem. *Id.* (paraphrasing the Court's conclusion).

Here, Plaintiff has sufficiently alleged that she is a proper party to bring this action. In other words, she is a "real party in interest" as a former employee of NHS (C. 41 ¶ 104) who was notified by NHS that her "name, date of birth, Social Security number, medical information, and

health insurance information" were among the data accessed (C. 41 ¶ 106) during what NHS calls a "sophisticated cyberattack" on its computer network. (C. 9 ¶ 1). She provided extensive factual support regarding the preventability, risks, harm caused by NHS's failure to adequately protect and monitor its computer network as required by the FTC Act, HIPAA, common law, and statutes (*e.g.*, C. 19–22), as well as its failure to timely notify the victims whose data was breached (C. 18 ¶ 32). Her causes of action for negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, breach of confidence, and breach of fiduciary duty each arise from NHS's failure to adequately protect and monitor its computer network. (C. 53–69). And she alleged that she has suffered injuries-in-fact (including but not limited to fraudulent loans, identity theft, lost time, and a substantial and imminent risk of future risks) related to her legally protected privacy rights (C. 41–42), and for which she could be "entitled to a remedy." (Prayer for Relief, C. 70–71).

These allegations are sufficient to show that Plaintiff is a proper party to bring the action on behalf of herself and similarly situated individuals. The Circuit Court erred in dismissing this action pursuant to Ala. R. Civ. P. 12(b)(1).

II. The Circuit Court erred when it did not consider the allegations in Plaintiff's complaint most strongly in her favor and failed to determine whether she could prove no set of facts in support of her claims that would entitle her to relief.

In the matter before this Court, the Circuit Court dismissed Plaintiff's original complaint with prejudice, with no explanation other than "Defendant's motion is due to be granted." (C. 203). However, under Ala. R. Civ. P. 12(b)(6), the allegations of the complaint must be viewed most strongly in the pleader's favor. *Nance*, 622 So. 2d at 299. The Circuit Court's silence as to why this matter was dismissed provides the parties and this Court mere speculation for its reasoning and the basis for such a speedy and harsh result, closing the doors to the Plaintiff and putative class for all relief sought.

A. Dismissals should be sparingly granted.

The courts of Alabama "exist for the very purpose of performing such tasks as sorting out what constitutes a cognizable cause of action, what are the elements of a cause of action, and whether the allegations of a given complaint meet those elements. Such tasks lie at the core of the judicial function." *Wyeth, Inc. v. Blue Cross & Blue Shield of Ala.*, 42

So. 3d 1216, 1220–21 (Ala. 2010) (citing generally Ala. Const. art. VI, § 139(a) (1901); Ala. Const. art. VI, § 142 (1901)).

Alabama precedent for dismissal under Rule (12)(b)(6) is well-settled: a matter should be dismissed only where there is "no set of facts in support of the claim that would entitle the plaintiff to relief." *Young Ams. for Liberty v. Finis St. John IV*, 2022 WL 17073690, at *2 (quoting *Nance,* 622 So. 2d at 299); *see also Raley v. Citibanc of Ala./Andalusia*, 474 So. 2d 640, 641 (Ala. 1985); *Hill*, 589 So. 2d at 746. "Dismissals under Rule 12(b)(6) should be granted sparingly, and such a dismissal is proper only when it appears beyond doubt that the plaintiff can prove no set of facts in support of the claim which would entitle him or her to relief." *Garrett*, 495 So. 2d at 617 (citing Committee Comments to Rule 8, Ala. R. Civ. P.; *Roberts,* 397 So. 2d at 111); *see also Snider v. Morgan*, 113 So. 3d 643, 652 (Ala. 2012) (reversing dismissal in part); *Radenhausen v. Doss*, 819 So. 2d 616, 619 (Ala. 2001) (denying motion to dismiss; reversing and remanding).

Reversal of a dismissal on appeal is appropriate if "'it appears that the pleader could prove any set of circumstances that would entitle her to relief.'" *Flickinger v. King*, No. SC-2022-0721, -- So. 3d --, 2023 WL

3029709, at *4–5 (Ala. Apr. 21, 2023) (reversing dismissal in part, affirming in part) (emphasis in original; citations omitted). The question is not "whether the plaintiff will ultimately prevail, but only whether she may possibly prevail." *Id.* 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.'" *Id.* (emphasis in original; citations omitted).

Where this Court is called upon to review a Rule 12(b)(6) dismissal of the complaint, it "'must examine the allegations contained [in the complaint] and construe them so as to resolve all doubts concerning the sufficiency of the complaint in favor of the plaintiff.'" *Radenhausen v. Doss*, 819 So. 2d 616, 619–20 (Ala. 2001) (quoting *Boswell v. Liberty Nat'l Life Ins. Co.,* 643 So. 2d 580, 581 (Ala. 1994) (quoting *Grant v. Butler*, 590 So. 2d 254, 255 (Ala. 1991) (quoting in turn *Green Cnty. Bd. of Educ. v. Bailey,* 586 So. 2d 893, 897–98 (Ala. 1991))).

For each of her causes of action, Plaintiff's allegations, considered most strongly in her favor, support that she is entitled to relief on behalf of herself and a class of similarly situated individuals whose PII and PHI was breached on NHS's insufficiently protected and monitored computer

network. Furthermore, NHS's failure to protect the PII and PHI that it collected and stored, as well as its excessive delay reporting the breach to both the HHS and individual victims, violated its duties under HIPAA, the FTC Act, statutes and common law. In short, NHS had—and was aware that it had—specific legal duties to protect the highly sensitive PII and PHI that it stored on its computer network, yet it failed to meet those duties. Plaintiff's allegations, when considered in light of NHS's duties and its public admissions and the injuries she and putative class members have suffered and will continue to suffer, are sufficient to withstand dismissal under Rule 12(b)(6).

B. Plaintiff alleges injuries-in-fact.

In her complaint, Plaintiff alleges injuries-in-fact that have resulted from 1) a substantial and present risk of identity theft, as well as other injuries, including 2) the misuse of her personal information, including but not limited to her Social Security number, 3) lost time and expense spent trying to mitigate the harm caused by Data Breach; 4) loss of value of her property rights of her personal information; and 5) an invasion of her privacy. Each provides an independent basis to satisfy the injury-in-fact requirements of each claim.

1. Increased risk of identity theft is a cognizable injury-in-fact.

An increased risk of identity theft in a data breach case is a cognizable injury-in-fact, yet Plaintiff is not required to demonstrate with certainty that "the harms [she] identif[ies] will come about." *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 414 n.5 (2013).[6] The Eleventh Circuit addressed this specific issue in a case in which extremely sensitive data was stolen in an Equifax data breach. "Given the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data, we have no hesitation in holding that Plaintiffs adequately alleged that they face a 'material' and 'substantial' risk of identity theft that satisfies the concreteness and actual-or-imminent elements." *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir.), *cert. denied sub nom*. Here, NHS notified Plaintiff of a similarly "colossal amount of sensitive data stolen, *including Social Security*

[6] Federal caselaw is persuasive authority when interpreting the Alabama Rules of Civil Procedure, especially when the corresponding federal rule is nearly identical to the Alabama Rule of Civil Procedure being considered. Federal authorities are not binding on this Court. *E.g.*, *First Baptist Church of Citronelle v. Citronelle–Mobile Gathering, Inc.*, 409 So. 2d 727, 729 (Ala. 1981). As this Court has not yet addressed many of the issues here, Plaintiff must rely heavily on the federal appellate courts.

numbers, names, and dates of birth" (*see* Plaintiff's Notice Letter, C. 74) that was accessed in its Data Breach, which the Eleventh Circuit had "no hesitation in holding that Plaintiff[] adequately alleged that they face a 'material' and 'substantial' risk of identity theft that satisfies the concreteness and actual-or-imminent elements" in *Equifax*. 999 F.3d at 1262 (emphasis added).

Common factors that courts commonly emphasize when addressing whether increased risk of identity theft is a cognizable injury are, first, whether a plaintiff alleges that hackers intentionally targeted personal information (a cognizable injury), or conversely, whether the loss of data was inadvertent (like the theft of electronics that happened to include stored personal data, which may not be a cognizable injury). *See id.*; *see also Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) (intentional hackers' primary incentive is to "sooner or later[] to make fraudulent charges or assume those consumers' identities[.]"); *cf. Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (no evidence that the data on the stolen laptop was accessed or misused, nor that theft of laptop was with intent to steal private data). "Where a data breach targets personal information, a reasonable inference can be drawn that

the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 640 (3d Cir. 2017) (unauthorized dissemination of plaintiffs' private information is a de facto injury satisfying concrete injury requirements).

Next, courts focus on the type of data that cybercriminals access in a data breach. Courts make "a distinction between easily changeable or replaceable information, such as credit and debit card information, and personally identifiable information, such as [S]ocial [S]ecurity numbers, birth dates, or driver's license numbers, which is more static." *In re 21st Century Oncology Customer Data Sec. Breach Litig.,* 380 F. Supp. 3d 1243, 1252–53 (M.D. Fla. 2019). Social security numbers paired with names and birth dates, in particular, are stolen information that circuit courts regularly find an injury-in-fact because such information can be used for identity theft. *In re Equifax*, 999 F.3d at 1262; *see also Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017) (defendant did not dispute plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were stolen, and "drawing on

'experience and common sense" and the court agreed). Thus, breaches that involve highly sensitive information, like Social Security numbers, support a finding of an injury-in-fact for an increased risk of identity theft.

Finally, courts find "an increased risk of identity theft is more likely to constitute an injury in fact where there is evidence that a third-party has accessed the sensitive information and/or already used the compromised data fraudulently." *In re 21st Century Oncology,* 380 F. Supp. 3d at 1254 (collecting cases). In *Attias*, an unauthorized party admittedly accessed personally identifying data on a defendant's servers, such that the court found it plausible "to infer that this party has both the intent and the ability to use that data for ill." 865 F.3d at 628. Similarly, the Seventh Circuit held that a concrete injury occurred where a defendant did not contest that the data breach took place, then offered one year of credit monitoring to all affected customers. *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (a defendant unlikely that provided a year of identity theft protection because the risk is so ephemeral that it can safely be disregarded."). The Third Circuit held that "Congress's decision to protect personal information from

disclosure . . . 'elevates to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.'" *In re Horizon*, 846 F.3d at 639 n.19 (3d Cir. 2017) (quoting *Lujan*, 504 U.S. at 578). In *In re Horizon*, where one plaintiff had already been a victim of identity theft as a result of the breach, it gives legitimacy to other plaintiffs' "argument that they face an increased risk of future injury." *Id.* But, as the Eleventh Circuit reinforced recently, "actual identity theft is by no means required when there is a sufficient risk of identity theft." *In re Equifax*, 999 F.3d at 1262.

Where all three factors occur, *i.e.,* 1) personal data is intentionally targeted and stolen by cyber criminals; 2) the data actually stolen, like Social Security numbers, is highly personal and can be used to steal a person's identity; and 3) plaintiff has plausibly alleged that the data was already accessed and/or used by the cyber criminals, the federal circuit courts regularly find an injury-in-fact based upon an increased risk of identity theft.

Here, Plaintiff's allegations—many of which are based on NHS's own public admissions about the data breach—are ample to support a finding of injury-in-fact. First, NHS admitted that its computer files were

accessed in "a sophisticated cyberattack" for an 80-day period from February 25, 2021, to May 16, 2021. (C. 17 ¶¶ 26, 28; C. 74). By February 4, 2022, NHS knew highly sensitive personal information was accessed including, *inter alia*, full names; contact information; Social Security numbers; dates of birth; driver's licenses; medical history, treatment and diagnosis information; and health and health insurance information. (C. 17 ¶ 29). The Personal Information accessed included that of current and former employees, vendors, and patients/residents of the facilities NHS serves as well as their family members and guardians. (C. 18 ¶ 30). Acknowledging the risks that the data breach caused, NHS offered victims of the attack "12 months of identity theft services through Kroll. These services include 12 months of monitoring, fraud consultation, and identity theft restoration." (C. 23 ¶ 41). Plaintiff received a letter from NHS stating that the information breached included her "name, date of birth, Social Security number, medical information, and health insurance information." (C. 41 ¶ 106; C. 74). In addition, Plaintiff alleged multiple recent experiences supporting her private information has been accessed and misused. (C. 41–42 ¶¶ 108–11). Since NHS's Data Breach, Credit Karma informed her that her information was found on many different

sites on the "dark web." (C. 41 ¶ 108). Apple's fraud department contacted her about $3000 of suspicious product purchases made in her name with her personal information. (C. 42 ¶ 110). These allegations, paired with NHS's acknowledgement that Plaintiff's Social Security and other highly sensitive private information was accessed in its Data Breach (and "the unequivocal damage that can be done with this type of data"), are sufficient to find that "substantial" or "certainly impending" risk of identity theft. *In re Equifax*, 999 F.3d at 1262.

Plaintiff has sufficiently alleged all factors used in data breach cases to find an "injury-in-fact" based on an increased risk of identity theft, including that: 1) cybercriminals intentionally targeted and stole private information stored on NHS's network; 2) the data accessed was highly sensitive, included names, Social Security numbers, dates of birth, and other types of PII used to steal a person's identity; and 3) the stolen data was accessed and already misused by the cybercriminals. These are sufficient allegations to find an injury-in-fact based an increased risk of identity theft.

2. Lost time is an injury-in-fact.

Plaintiff's allegations, which include both past and future time associated with monitoring financial and medical accounts, are likewise sufficient to support an injury-in-fact. Both past and future lost time are cognizable injuries in fact under specific circumstances, which are present in this matter.

In *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020), the Eleventh Circuit outlines several factors that this Court should consider when deciding whether lost time is an injury-in-fact. First, a complaint must include "specific time allegation[s]" that relate to this data breach. 979 F.3d at 930–31 (citing *Salcedo v. Hanna*, 936 F.3d 1162, 1168 (11th Cir. 2019) (allegation of time wasted is generally insufficient)). Second, a "management-of-risk" lost time claim is "bound up" with the actual risk. *Id*. (*e.g.*, if a receipt is not an advantage to identity thieves, a plaintiff cannot claim injury for time spent keeping the receipt out of thieves' hands). *Id*. To measure the gravity of the risk, the Eleventh Circuit considers whether the stolen data would subject a plaintiff to a "substantial risk" of identity theft in the future. *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1342–43 (11th Cir. 2021). Social Security numbers, birth dates, and driver's license numbers

would create a substantial risk; credit card numbers, standing alone, do not result in a substantial risk of identity theft. *Id.* In addition, allegations related to "at least some evidence of actual misuse" support that "the threatened harm of future identity theft [i]s 'certainly impending.'" *Id.* at 1344. And finally, a plaintiff cannot "conjure standing" by taking steps "to avoid an insubstantial, non-imminent risk of identity theft," *id.* at 1345, as in situations where only credit card numbers (which are readily changeable) are breached.

Here, Plaintiff alleges her already-lost time with specificity. (C. 42 ¶ 112 ("She spends about 15 minutes per day" monitoring her financial accounts.)). The types of data stolen from Plaintiff, *i.e.*, her name, date of birth, Social Security number, medical information, and health insurance information (C. 41 ¶ 106) subject her to a "substantial risk" of future identity theft. And she pleaded evidence of actual misuse, supporting that future identity theft is "certainly impending," warranting past and future time mitigating her risks. (*E.g.*, C. 41 ¶ 108 (Since NHS's Data Breach, Plaintiff was "notified by Credit Karma that her PII was found on many different sites on the 'dark web.' She spent considerable time working with Credit Karma to freeze her credit and correct errors on her

credit reports."); C. 41 ¶ 109 (She "has been receiving a high number of spam emails, calls, and texts, often receiving over 3 spam calls or texts in a given day."); C. 42 ¶ 110 (She "has received several calls from the Apple fraud department asking whether she made certain Apple product purchases worth about $3000." She had not.); and C. 42 ¶ 111 ("Since the NHS Data Breach, Plaintiff Griggs has been receiving harassing phone calls and emails stating that she owes money for 'payday loans.' This is incorrect because she does not owe any payday loans.")). Each of these allegations supports an injury-in-fact for lost time reasonably expended due to the Data Breach.

In addition, Plaintiff Griggs alleges that she "anticipates spending time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach" (C. 42 ¶ 115), which is an allegation of future lost time, reasonably related to a substantial and imminent risk of identity theft and, therefore, another injury-in-fact. Plaintiff has alleged that she is aware that her personal information "could be abused months or even years after the NHS Data Breach." (C. 42 ¶ 113). Her claims are neither speculative nor self-inflicted.

3. Data misuse and unwanted spam are injuries-in-fact.

Plaintiff's claims of having already suffered data misuse and excessive spam communications related to NHS's Data Breach are likewise allegations of injury-in-fact. Admittedly, if each incident (finding her information on the dark web, the Apple charges, and spam communications) were standing alone (which it is not), it might not constitute an injury-in-fact. However, these allegations cannot be considered in a vacuum. They must be considered within the context all allegations in the four-corners of her complaint.

As discussed above, the Eleventh Circuit recently held that when the data accessed or stolen in a data breach includes "Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data, [it has] no hesitation in holding that [p]laintiffs adequately alleged that they face a "material' and 'substantial" risk of identity theft that satisfies the concreteness and actual-or-imminent elements." *In re Equifax*, 999 F.3d at 1262. With certain private information along with a Social Security number, an identity thief can open new loans, credit accounts, and commit tax fraud. *Id*. at 1263; *Tsao*, 986 F.3d at 1343. The *Equifax* list of sensitive data sufficient for a "material' and 'substantial" risk of identity theft (*i.e.*,

name, date of birth, and Social Security number) matches Plaintiff's data that NHS admitted was accessed in its Data Breach here. (C. 41 ¶ 106). As emphasized in *Equifax*, which is based on a comparable stolen data, "Plaintiff[] ha[s] easily shown an injury in fact." *In re Equifax*, 999 F.3d at 1263. Furthermore, an allegation of "actual identity theft is by no means required when there is a sufficient risk of identity theft." *Id.* at 1262.

Similarly, in recent caselaw from the Fourth Circuit, a plaintiff "began experiencing an uptick in spam text and telephone calls that he attributes to this Data Breach." *Holmes v. Elephant Ins. Co.*, No. 3:22CV487, 2023 WL 4183380, at *5 (E.D. Va. June 26, 2023) (citing *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921 (4th Cir. 2022)). In *Garey*, the Fourth Circuit determined that receiving unsolicited mail closely paralleled the tort of loss of privacy and recognized it as an injury-in-fact. *Id.* (citing *Garey*, 35 F.4th at 922). "Spam texts and calls invade an individual's privacy as much or perhaps even more than unsolicited mail." *Holmes*, 2023 WL 4183380, at *5.

Plaintiff's allegations of injury-in-fact are sufficiently pleaded throughout her complaint.

C. Each of Plaintiff's claims is sufficiently pleaded.

1. Plaintiff alleges all elements of negligence.

For Plaintiff to support her negligence claim, she must plausibly allege that: 1) NHS has a duty to her, as a foreseeable plaintiff, 2) NHS breached that duty, 3) proximate causation, and 4) the breach resulted in damage or injury. *Martin v. Arnold*, 643 So. 2d 564, 567 (Ala. 1994). She has sufficiently—and undeniably—alleged each of these factors.

First, Plaintiff alleged that NHS has a duty to "a foreseeable plaintiff" (including herself and class members): "[NHS] had clearly-defined and mandatory obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and class members, to keep their Personal Information confidential and to protect it from unauthorized access and disclosure." (C. 24 ¶ 46; *also* C. 19 ¶ 35 and C. 3, ¶ 78 (similar); C. 53 ¶ 149 (NHS's "duty included a responsibility to implement processes by which they 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."), and C. 54 ¶ 151 (NHS could have "ensure[d] that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a cyberattack

and data breach.")).

Second, NHS admits in its Notice Letters that it was not able to protect Plaintiff's and class member's PII and PHI on its insecure computer systems during "a sophisticated cyberattack" resulting in "an unauthorized actor accessed certain NHS systems and information stored therein" for an 80-day period. (C. 74; *see also* C. 16–17 ¶¶ 26–34 (collecting details about the breach as reported by NHS); C. 20 ¶ 38 (list of acts and omissions of how NHS breached its duty). Moreover, Plaintiff alleges that NHS breached its duty to discover, to report to governmental authorities, and to notify Plaintiff and class members of the cyberattack in a timely manner. (*E.g.*, C. 17 ¶ 28 (its system was at risk for 80-day period); C. 18 ¶ 31 ("NHS notified the U.S. Department of Health and Human Services ("HHS") on October 29, 2021, over ***5 months after*** discovering the Data Breach, that *at least* 501 individuals were affected when its computer network was hacked. If a breach affects 500 or more individuals, covered entities, including NHS, must notify HHS 'without unreasonable delay and *in no case later than 60 days following a breach*.'") (emphases in Compl.); C. 18 ¶ 32 ("NHS did not begin notifying the Data Breach victims (i.e., Class Members) until on or about March

31, 2022, over a year after the Data Breach began and ***ten and one-half months*** after it first learned of the Data Breach.") (emphasis in Compl.). NHS clearly breached many duties, including, *inter alia*: 1) to protect highly sensitive Personal Information entrusted with it, 2) to monitor its systems for breaches, and 3) to promptly and fully report the data breach to authorities and victims. (C. 20 ¶ 38).

Third, Plaintiff adequately alleges proximate causation, pleading NHS "failed to properly maintain and safeguard its computer systems and the data," then enumerating specific acts and omissions it committed to support proximate causation. (C. 20–22 ¶ 38 (*e.g.*, subparts (a) to (o)). Plaintiff pleaded that as "a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft." (C. 44 ¶ 121; *see also* C. 12–13 ¶¶ 10, 14 (similar)). "Due to Defendant's insufficient security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with the risk the misuse of their Personal Information for years." (C. 23 ¶ 44). These allegations are sufficient allegations for proximate causation.

Fourth and finally, Plaintiff's allegations of injury and damages satisfy the last element, that the breach resulted in damage or injury. Plaintiff and Class "suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information." (C. 10 ¶ 2). The injuries are specific and enumerated. (*E.g.*, C. 46–47 ¶ 131 (a)–(k)). And Plaintiff describes her own injuries-in-fact in great detail. *See supra,* Argument, Section II(B) (regarding Plaintiff's allegations of injuries-in-fact, with supporting caselaw). Plaintiff's allegations of damages and injuries are sufficient for the last element of negligence.

2. HIPAA and the FTCA buttress a negligence per se claim.

Although there is "no private right of action under either HIPAA or the FTCA, both can serve as a basis for a negligence *per se* claim under Alabama law. No directly on-point, binding precedent in Alabama holds that HIPAA and the FTCA *cannot* serve as the basis of a negligence *per se* claim. *E.g., Smith v. Triad of Ala., LLC*, No. 1:14–CV–324, 2015 WL 5793318, at *12 (M.D. Ala. Sept. 29, 2015). But after searching Alabama

and Eleventh Circuit caselaw, the Middle District of Alabama relied on *Allen v. Delchamps, Inc.*, 624 So. 2d 1065, 1067–68 (Ala. 1993) to hold that "even where a private right of action is not contemplated by a statute, the statute can still serve as the basis of a negligence per se claim." 2015 WL 5793318, at *11. In *Allen*, this Court acknowledged that no private cause of action existed under the federal statute in question, but it allowed the negligence *per se* claim to proceed. 624 So. 2d at 1067–68. It explained: "the plaintiffs in this case are not suing directly under the FDCA or its accompanying regulations. Rather, they are relying on the regulations to establish a duty or standard of care." *Id.*

Here, Plaintiff alleges that HIPAA and the FTCA established a duty or standard of care in support of her negligence per se claim. (*See, e.g.*, C. 57 ¶ 162 ("Pursuant to the HIPAA (42 U.S.C. §§ 1302d, *et seq.*) and the FTCA, [Defendant] was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.")).

3. The Invasion of Privacy claim is sufficiently pleaded.

NHS's failure to secure and monitor its computers would be considered "highly offensive" by a reasonable person, therefore supporting Plaintiff's invasion of privacy claim.

Not all stolen data is equal. As discussed in *In re Equifax*, "*some of the most sensitive personal information possible* [includes]: all nine digits of Americans' Social Security numbers, coupled with their names, dates of birth, and addresses[.]" 999 F.3d at 1257 (emphasis added). The theft of this "most sensitive information" results in unique risks, including "'a pervasive, substantial and imminent risk of identity theft and fraud, a risk that will continue so long as Social Security numbers have such a critical role in consumers' financial lives.'" *Id*. at 1247. "Using this information, identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness." *Id*.

The Supreme Court of the United States has long recognized that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *U.S. Dep't. of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763–64 (1989). Courts have recognized that a third-

party's procurement of personal data can give rise to an actionable privacy tort. *See Nayab v. Capital One Bank (USA), N.A.*, 942 F.3d 480, 491 (9th Cir. 2019) (release of highly personal information—a consumer credit report—to a third-party). As the court in *Nayab* explained "the consumer is harmed because he or she is deprived of the right to keep private the sensitive information about his or her person. This harm is highly offensive and is not trivial . . .." *Id.* at 492 (reversing a dismissal).

Like the class members in the *Equifax* case, and according to its Notice Letters, NHS's failure to protect and monitor its computer systems left "some of the most sensitive personal information possible" of Plaintiff and class members unprotected. 999 F.3d at 1257. But here, NHS's lack of protection lasted for a period of eighty days. (C. 17 ¶ 28). Even more egregious—and intentional—is NHS's decision to delay notifying proper authorities for more than five months after belatedly discovering the breach (C. 18 ¶ 31), and never revealing the full magnitude of the breach to HHS. *Id.* (only notifying HHS that at least 501 individuals were affected). Although the data breach began about February 25, 2021 (C. 17 ¶ 28), Plaintiff's Notice Letter was dated March 31, 2022, over a year later. (C. 18 ¶ 32; C. 74). NHS was fully aware that

acting promptly was necessary to mitigate harm in a data breach (C. 19 ¶ 27 ("NHS immediately took steps to stop the attack and mitigate the harm.")) but decided not to promptly notify Plaintiff and Class members of the data breach. (*See* C. 74; *compare* C. 17 ¶ 27 to C. 18 ¶ 32). As a result, the actual victims of this data breach could not promptly mitigate their own risks.

Plaintiff's allegations support that it is plausible that NHS's actions would be considered "highly offensive to a reasonable person," even if lacking those "magic words." *Pickett v. Williamson*, No. 5:11-CV-03439-JHE, 2015 WL 2450767, at *3 (N.D. Ala. May 22, 2015) (pleaded facts were sufficient even certain "magic words" are missing from the complaint). And whether NHS's extremely long delay notifying Plaintiff and Class about the Data Breach so that they could mitigate their injuries would be "highly offensive to a reasonable person" is a jury question. *Cunningham v. Dabbs*, 703 So. 2d 979, 982 (Ala. Civ. App. 1997) (A reasonable jury could determine that defendant's actions were severe enough to constitute an invasion of plaintiff's right to privacy.). Being "deprived of the right to keep private [] sensitive information," a harm that "is highly offensive and is not trivial." *Nayab*, 942 F.3d at 492.

Plaintiff has sufficiently pleaded all elements of her invasion of privacy claim.

4. Plaintiff's Unjust Enrichment Claim is viable.

In *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012), a similar data breach case, the Eleventh Circuit held that members of healthcare plan sufficiently pleaded their unjust enrichment claim. The Circuit Court explained, "[t]o 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.'" *Id*. (quoting *Della Ratta v. Della Ratta*, 927 So.2d 1055, 1059 (Fla. Dist. Ct. App. 2006)).

A "benefit conferred" does not have to be monetary. Plaintiff has alleged that "[p]art of the wages or pay terms that [she and other] Class Members negotiated with Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiff's and Class Members' Personal Information." (C. 45 ¶ 127).

This allegation, set within the four corners of the Complaint, is sufficient to establish that 1) Plaintiff conferred a benefit on NHS (her labor for which she negotiated pay), and 2) that a portion of the wage or pay terms was intended for data security. Plaintiff has further alleged that NHS either failed to implement or inadequately implemented policies to secure sensitive information, as can be seen from its data breach. (*See, e.g.*, C. 20 ¶ 38; C. 31 ¶¶ 69, 73).

NHS should not be permitted to "retain the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide." (C. 62 ¶ 181). It failed to implement the data management and security measures that are mandated by industry standards. Plaintiff alleged sufficient facts that this claim should have survived dismissal.

5. Plaintiff's Breach of Confidence is viable.

The Eleventh Circuit recognizes the potential applicability of the common law tort of breach of confidence, particularly in the context of "close professional relationships." *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d at 932. 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." *Id.* (citing *Young v. U.S. Dep't of Justice*, 882 F.2d 633, 640 (2d Cir. 1989)); *see also* David A. Elder, *Privacy Torts* § 5:3 (2019). "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.'" *Muransky*, 979 F.3d at 932 (citing Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 Colum. L. Rev. 1426, 1455 (1982)); *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019); and *Vassiliades v. Garfinckel's*, 492 A.2d 580, 591 (D.C. 1985)).

Plaintiff alleges that she provided to NHS her personal information as required for employment with the reasonable expectation and mutual understanding that NHS would protect it from unauthorized access and disclosure. (C. 25 ¶ 47; C. 63 ¶ 189). NHS's relationship with Plaintiff and class members was governed by terms and expectations that Plaintiff's and class members' PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties. (C. 63 ¶ 186). NHS's failure to adequately protect its computer systems led to the data breach, which in turn resulted in the unconsented, unprivileged disclosure of Plaintiff's and the classes'

nonpublic information to third-party cybercriminals. (C. 63 ¶ 190). And she alleges that her PII and PHI were actually accessed by criminals (which NHS admits, *see* C. 74) and was misused. (C. 41–42, ¶¶ 105–11). These allegations and injuries-in-fact are sufficient to support Plaintiff's breach of confidence claim, which should have survived dismissal under Rule 12(b)(6).

6. The claim for Breach of Fiduciary Duty is sufficient.

Under Alabama law, a fiduciary relationship exists when one person has gained the trust of or inspired confidence in another person that he will act in good faith with the other's interest in mind. *Brown v. Gadsden Reg'l Med. Ctr. LLC*, No. 4:16-CV-01739-KOB, 2019 WL 3501528, at *3 (N.D. Ala. Aug. 1, 2019) (citing *K&C Dev. Corp. v. AmSouth Bank, N.A.*, 597 So.2d 671, 675 (Ala. 1992) ("[The duty] arises in cases in which confidence is reposed and accepted, or influence acquired, and in all the variety of relations in which dominion may be exercised by one person over another.")). Alabama courts have found a fiduciary relationship in cases where persons or entities have exercised "influence" or "dominion" over another. And importantly, Alabama courts have indicated that the existence of a fiduciary relationship is a fact-

based inquiry into the questions of "influence" or "dominion." *See Mitchell v. Harris*, 246 So. 2d 648, 652 (Ala. 1971) (if fiduciary relation existed, it was a question of fact) (citing *Nelson v. Brown (Brown v. Nelson)*, 164 Ala. 397, 51 So. 360 (Ala. 1910)).

Alabama does not have a hard and fast rule that there can never be a fiduciary relationship between employees and employers. *E.g.*, *Lanfear v. Home Depot, Inc.*, 536 F.3d 1217, 1224 (11th Cir. 2008). Instead, courts must engage in an inquiry as to whether or not the "nature of the relationship between the parties" to determine the existence of a fiduciary relationship. *Id*. Alabama courts have used that legal principle as a point of contrast, demonstrating that the existence of certain fiduciary relationships is still an open question. And Alabama courts have recognized the principle that a fiduciary relationship may be voluntarily assumed. *See Dailey v. City of Birmingham*, 378 So. 2d 728, 729 (Ala. 1979) ("Alabama clearly recognizes the doctrine that one who volunteers to act, though under no duty to do so, is thereafter charged with the duty of acting with due care and is liable for negligence in connection therewith."). The upshot of this is that a) as a matter of Alabama law, it is not certain that a fiduciary relationship cannot exist

between NHS and Plaintiff or other putative class members, who include employees, patients/residents, their families and guardians, and even vendors and b) the facts and circumstances can show that a fiduciary relationship may be found to exist.

Here, where all inferences are taken in Plaintiff's favor, the facts and circumstances alleged demonstrate that there is a fiduciary relationship between NHS and the class members, including Plaintiff. NHS voluntarily collects and stores a tremendous amount of sensitive PII and PHI from employees, patients, guardians, and even vendors as a pre-condition to employment, medical services, and even purchasing or services agreements. (C. 15 ¶ 23). NHS thereby exercises both influence and dominion over Plaintiff and class members. *Id*. As a recipient of this sensitive Personal Information, NHS had obligations created by HIPAA, contract, industry standards, common law, and representations made to class members, to keep class members' PII and PHI confidential and to protect it from unauthorized access and disclosure. (C. 24 ¶ 46). NHS voluntarily collected and became guardians of this Personal Information then failed in its duty to keep that highly sensitive information safe and confidential. (C. 65–68 ¶¶ 197–99). All these facts, as alleged by Plaintiff,

create the special fiduciary relationship between NHS and Plaintiff and putative class members, and NHS breached its fiduciary duty. Plaintiff adequately pleaded this claim, which should have survived dismissal.

CONCLUSION

For all the reasons set forth above, this Court should reverse the Circuit Court's grant of NHS's motion to dismiss, whether under Rule 12(b)(1) or 12(b)(6), and should remand the matter to the Circuit Court for further litigation on the merits.

Dated: January 29, 2024

Respectfully submitted,

/s/ Taylor C. Bartlett

Taylor C. Bartlett
(AL Bar # ASB 2365 A51B)
HENINGER GARRISON DAVIS, LLC
2224 1st Avenue N.
Birmingham, AL 35203
Tel.: (205) 326-3336
taylor@hgdlawfirm.com

On behalf of Attorneys for Appellant

CERTIFICATE OF COMPLIANCE

This Brief complies with the font and word limits as required by Rule 32(d) because the Brief has been prepared in 14-point Century Schoolbook font, and this document is **11,206** words long, which is less than the 14,000 allowed by Rule 28(j).

Dated: January 29, 2024 */s/Taylor C. Bartlett*

Taylor C. Bartlett
Attorney for Plaintiff-Appellant

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing by electronically filing the same using the appellate online electronic filing system and by depositing a copy in the U.S. Mail, properly addressed and first-class postage prepaid, on the 29th day of January, 2024.

H. Thomas Wells, III (ASB-4318-H62W)
htw@starneslaw.com
STARNES DAVIS FLORIE LLP
100 Brookwood Place, 7th Floor
Birmingham, AL 35209
Telephone: (205) 868-6000
Fax: (205) 868-6099

Spencer Persson
spencerpersson@dwt.com
Andrew G. Row
andrewrow@dwt.com
DAVIS WRIGHT TREMAINE LLP
865 S. Figueroa Street, Suite 2400
Los Angeles, CA 90017
Telephone: (213) 633-6800
Fax: (213) 633-6899

/s/Taylor C. Bartlett
Taylor C. Bartlett
HENINGER GARRISON DAVIS LLC

Counsel of Record for the Appellant