UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN RE: 21st CENTURY ONCOLOGY CUSTOMER DATA SECURITY BREACH LITIGATION

MDL No. 2737

Case No: 8:16-md-2737-MSS-AEP

This Document Relates to ALL CASES

ORDER

THIS CAUSE comes before the Court for consideration of Defendants' Motion to Dismiss Plaintiffs' Consolidated Complaint, (Dkt. 116), Defendants' Notice of Filing Supplemental Authority in Support of Defendants' Motion to Dismiss, (Dkt. 119), Plaintiffs' response in opposition to Defendants' Motion to Dismiss, (Dkts. 142, 146), Plaintiffs' Notice of Supplemental Authority in Support of Plaintiffs' Opposition, (Dkt. 149), Plaintiffs' Supplemental Memorandum in Opposition to Defendants' Motion to Dismiss, (Dkt. 156), Defendants' Response to Plaintiffs' Supplemental Memorandum in Opposition to Defendants' Motion to Dismiss, (Dkt. 157), Defendants' Supplemental Memorandum in Support of Motion to Dismiss Plaintiffs' Consolidated Amended Class Action Complaint, (Dkt. 195), Plaintiffs' Supplemental Memorandum in Opposition to Defendants' Motion to Dismiss, (Dkts. 199, 201), and Plaintiffs' Notice of Supplemental Authorities in Connection

with Plaintiffs' Memoranda in Opposition to Defendants' Motion to Dismiss. (Dkt. 206) The Court heard argument on Defendants' first iteration of the Motion to Dismiss. (Dkts. 154, 167) Upon consideration of all relevant filings, case law, and being otherwise fully advised, the Court **DENIES** Defendants' Motion to Dismiss.

I. BACKGROUND

On March 4, 2016, Defendant 21st Century Oncology Holdings, Inc. announced that on October 3, 2015, an unauthorized third party might have gained access to its database containing patients' personal information ("Data Breach"). As a result of the Data Breach, the information of approximately 2.2 million current and former patients was compromised. The patients brought eighteen (18) separate putative class action suits against 21st Century Oncology Holdings, Inc. and its subsidiaries and affiliates (collectively, "Defendants") alleging, among other things, state statutory claims, negligence, and unjust enrichment stemming from the Data Breach. On October 7, 2016, the Judicial Panel on Multidistrict Litigation transferred the individual actions to this Court for pretrial proceedings. (Dkt. 1)

On January 17, 2017, Plaintiffs Matthew Benzion, Steven Brehio, Judy Cabrera, Valerie Corbel, Veneta Delucchi, Jackie Griffith, Roxanne Haavedt, Kathleen LaBarge, Sharon MacDermid, Timothy Meulenberg, Robert Russell, Carl Schmitt, Stacey Schwartz, and Stephen Wilbur (hereinafter, "Plaintiffs") filed a Consolidated Class Action Complaint merging their individual claims into a singular pleading. (Dkts. 100, 103) On July 30, 2018, Plaintiffs filed an Amended Consolidated Class Action Complaint ("Amended Complaint"), which is the currently operative complaint in this action. (Dkts. 191, 194)

On behalf of a putative nationwide class, Plaintiffs allege the following ten (10) causes of action: Negligence (Count I), Gross Negligence (Count II), Negligent Misrepresentation (Count III), Breach of Express Contracts (Count IV), Breach of Implied Contracts (Count V), Breach of Implied Duty of Good Faith and Fair Dealing (Count VI), Breach of Fiduciary Duty (Count VII), Unjust Enrichment (Count VIII), Invasion of Privacy (Count IX), and Declaratory Judgment (Count X). (Dkt. 194)

Defendants filed their initial Motion to Dismiss as against the original Consolidated Complaint, asserting that some of the Plaintiffs do not have standing in this action for failure to assert an injury in fact and that all Plaintiffs have failed to state a claim as to their asserted causes of action. (Dkt. 116) After the Motion was fully briefed and the Court heard argument on the Motion, Defendants filed a Notice of Petition in Bankruptcy, which prompted a prolonged stay of this case. Through a settlement between the Parties in the bankruptcy action, this action was permitted to proceed.[1] The Parties conducted preliminary fact discovery, and thereafter, Plaintiff filed the Amended Complaint. (Dkts. 191, 194) On August 29, 2018, Defendants filed a Supplemental Motion to Dismiss based on the currently operative Amended Complaint while preserving its previous arguments contained in its initial Motion to Dismiss. (Dkt. 195) Similarly, on September 28, 2018, Plaintiff filed an opposition to the Supplemental Motion to Dismiss that preserves its previous opposition to Defendants' initial Motion to Dismiss. (Dkts. 199, 205) Thus, the Court considers all arguments and responses made by the Parties in the briefings of both the initial Motion to Dismiss and the Supplemental Motion to Dismiss to

1 The Court notes that although the bankruptcy stay was effectively lifted by the Court's permitting the Parties to proceed in this action, the case was never administratively reopened. Thus, the Court will direct that the Clerk reopen this matter.

the extent that such arguments and responses are applicable as against the Amended Complaint.

In the Amended Complaint, Plaintiffs allege that prior to the Data Breach, Defendants acknowledged in a "Notice of Privacy Practices" posted on their website that they are "required by law to maintain the privacy of your protected health information, to provide you with notice of our legal duties and privacy practices with respect to that protected health information, and to notify any affected individuals following a breach of any unsecured protected health information." (Dkt. 194 at ¶ 8) Plaintiffs state that Defendants "failed to maintain reasonable and/or adequate security measures to protect Plaintiffs' and other Class members' [personally identifiable information ("PII") and protected health information ("PHI")] from being released, disclosed, and rendered publicly accessible to unauthorized parties." (Dkt. 194 at ¶ 10)

Plaintiffs allege that on November 6, 2015, the Federal Bureau of Investigation ("FBI") "learned that 'an unauthorized party was attempting to sell compromised 21st Century Oncology data,' which 'was advertised, in Russian, as approximately 10 million patient records from 21st Century Oncology available to purchase for $10,000'" and that the FBI had "obtained a sample of the data from the unauthorized party." (Dkt. 194 at ¶ 114) (quoting the Declaration of FBI Special Agent Joseph Battaglia ("FBI Declaration"), Dkt. 195-1 at ¶ 3) They claim that due to Defendants' insufficient security protocols, Defendants failed to detect the Data Breach until the FBI notified them on or about November 13, 2015. (Dkt. 194 at ¶ 5) Plaintiffs allege that "on November 19, 2015, 21st Century 'confirmed that the sample of data provided by the FBI contained its patients' information,' and the FBI informed 21st Century 'that the unauthorized party listed

additional data beyond the sample for sale.'" (Dkt. 194 at ¶ 119) (quoting FBI Declaration, Dkt. 195-1 at ¶ 6)

Plaintiffs assert that the Data Breach resulted in "the release, disclosure, and publication of private and highly sensitive PII/PHI including: names, Social Security numbers, physicians' names, medical diagnoses, treatment information, and insurance information." (Dkt. 194 at ¶ 6) Plaintiffs allege that the following injuries were suffered and are likely to be suffered as a direct and proximate result of the Data Breach:

> (a) release, disclosure, and publication of their personal and financial information;
>
> (b) loss or delay of tax refunds as a result of fraudulently filed tax returns;
>
> (c) costs associated with the detection and prevention of identity theft and unauthorized use of their PII/PHI with regard to financial, business, banking, and other accounts;
>
> (d) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling credit cards, purchasing credit monitoring and identity theft protection services (beyond the one-year offered by 21st Century), the imposition of withdrawal and purchase limits on compromised accounts, and the time, stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, including phishing emails and phone scams;
>
> (e) the imminent and certain impending injury flowing from fraud and identity theft posed by their PII/PHI being placed in the hands of hackers and being offered for sale on the Dark Web;
>
> (f) damages to and diminution in value of their PII/PHI entrusted to 21st Century for the sole purpose of obtaining healthcare services from 21st Century;
>
> (g) money paid to 21st Century for healthcare services during the period of the Data Breach, because Plaintiffs and Class members would not have obtained healthcare services from 21st Century had it disclosed that it lacked adequate systems and procedures to reasonably safeguard patients' PII/PHI;

> (h) overpayments to 21st Century for healthcare services purchased, in that a portion of the amount paid by Plaintiffs and Class members to 21st Century was for the costs for 21st Century to take reasonable and adequate security measures to protect the Plaintiffs and Class members' PII/PHI, which 21st Century failed to do; and
>
> (i) personal, professional, or financial harms caused as a result of having their PII/PHI exposed.

(Dkt. 194 at ¶ 214)

Plaintiffs propose a putative nationwide class action on behalf of themselves and all persons whose PII and PHI have been compromised or made publicly accessible as a result of the Data Breach. (Dkt. 194 at ¶ 3) The fourteen named Plaintiffs are citizens of the following six states: California, Florida, Arizona, Kentucky, Rhode Island, New Jersey. (Dkt. 194 at ¶¶ 19–107) The Complaint details the alleged impact that the Data Breach has had on each named Plaintiff. (Id.) Some Plaintiffs have experienced misuse of their private information, such as, for example, fraudulent attempts to open credit card and/or bank accounts in their name. (See, e.g., Allegations by Plaintiff Timothy Meulenberg at Dkt. 194 at ¶ 71 (alleging that "on March 10, 2016, an attempt was made by unauthorized parties to open a . . . credit card account," and that "on or about November 2016, Plaintiff Meulenberg discovered unauthorized charges totaling $173 on his . . . credit card account")) Other Plaintiffs, however, do not allege that their information has been misused subsequent to the Data Breach. (See, e.g., Allegations by Plaintiff Robert Russell at Dkt. 194 at ¶¶ 19–23) Nevertheless, all Plaintiffs have alleged that they (1) have endured past and will endure future costs for credit monitoring, (2) have spent hours checking their accounts and monitoring their credit, and researching the Data Breach, and (3) have suffered emotional distress as a result of the Data Breach. (Dkt. 194 at ¶¶ 19–107)

II. LEGAL STANDARD

a. Standing

"The Constitution of the United States limits the subject matter jurisdiction of federal courts to 'Cases' and 'Controversies.'" CAMP Legal Defense Fund, Inc. v. City of Atlanta, 451 F.3d 1257, 1269 (11th Cir. 2006) (quoting U.S. Const. Art. III, § 2). "[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III." Id. (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)). "In the absence of standing, a court is not free to opine in an advisory capacity about the merits of a plaintiff's claims, and the court is powerless to continue." Id. (quotation marks omitted). Accordingly, "[i]t is by now axiomatic that a plaintiff must have standing to invoke the jurisdiction of the federal courts." KH Outdoor, LLC v. City of Trussville, 458 F.3d 1261, 1266 (11th Cir. 2006).

The U.S. Supreme Court has "established that the 'irreducible constitutional minimum' of standing consists of three elements." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016), as revised (May 24, 2016) (quoting Lujan, 504 U.S. at 560). "The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016). "The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." Id.

To establish the injury in fact element, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Id. (quoting Lujan, 504 U.S. at 560). An injury is particularized if it "affect[s] the plaintiff in a personal and individual way." Id. at

1548 (citations omitted). An injury is concrete when it is "real," not "abstract." Id. Moreover, intangible injuries may be concrete. Id. at 1549. In determining whether an intangible injury is concrete, "'[w]hether [the] alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts' is instructive because the case-or-controversy requirement is 'grounded in historical practice.'" Nicklaw v. Citimortgage, Inc., 839 F.3d 998, 1002 (11th Cir. 2016) (citing Spokeo, 136 S. Ct. at 1549). "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a "'substantial risk" that the harm will occur.'" Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)).[2] Moreover, a plaintiff may not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Clapper, 568 U.S. at 416.

b. Failure to State a Claim

The threshold for surviving a motion to dismiss for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6) is a low one. Quality Foods de Centro Am., S.A. v. Latin Am. Agribusiness Dev. Corp., S.A., et al., 711 F.2d 989, 995 (11th Cir. 1983). A plaintiff must plead only enough facts to state a claim to relief that is plausible on its face. Bell Atlantic Corp. v. Twombly, 127 S. Ct. 1955, 1968–69 (2007) (abrogating the

2 The Court notes that the circuit court decisions addressed in the Court's injury-in-fact analysis infra do not consistently use one standard or the other in data breach cases. Some circuits have used the "substantial risk" standard, others have used the "certainly impending" standard, and at least one court, the Fourth Circuit, has used both. See Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017). Due to this lack of uniformity, the Court refers to the decisions generally as either finding an injury in fact or not. As to the facts of this case, the Court finds that it is unnecessary to distinguish between the two standards as Plaintiffs have sufficiently demonstrated an injury in fact that satisfies both of the standards.

"no set of facts" standard for evaluating a motion to dismiss established in Conley v. Gibson, 355 U.S. 41, 45–46 (1957)). Although a complaint challenged by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff is still obligated to provide the "grounds" for his entitlement to relief, and "a formulaic recitation of the elements of a cause of action will not do." Berry v. Budget Rent A Car Sys., Inc., 497 F. Supp. 2d 1361, 1364 (S.D. Fla. 2007) (quoting Twombly, 127 S.Ct. at 1964–65). In evaluating the sufficiency of a complaint in light of a motion to dismiss, the well pleaded facts must be accepted as true and construed in the light most favorable to the plaintiff. Quality Foods, 711 F.2d at 994–95. However, the court should not assume that the plaintiff can prove facts that were not alleged. Id. Thus, dismissal is warranted if, assuming the truth of the factual allegations of the plaintiff's complaint, there is a dispositive legal issue which precludes relief. Neitzke v. Williams, 490 U.S. 319, 326 (1989).

III. DISCUSSION

a. Standing

Defendants argue that Plaintiffs' Amended Complaint should be dismissed as to seven of the named plaintiffs ("Non-Misuse Plaintiffs")[3] for lack of subject matter jurisdiction under Rule 12(b)(1). Specifically, Defendants contend that seven plaintiffs have not alleged that their PII/PHI has actually been misused and therefore, have failed to allege an injury in fact sufficient to confer standing.[4]

3 According to Defendants, the seven plaintiffs are Robert Russell, Roxanne Haatvedt, Veneta Delucchi, Matthew Benzion, Kathleen LaBarge, Sharon McDermid, and James Corbel. (Dkt. 116 at 13 n.2)

4 Defendants do not assert a standing challenge against any Plaintiffs on the basis of causation or redressability.

Defendants insist that the Court reject the following theories of injury asserted by the Non-Misuse Plaintiffs: (1) an increased risk of future identity theft, (2) time and expenses related to mitigating future harms, (3) overpayment for Defendants' services due to inadequate protection of PII/PHI, and (4) loss in value of PII/PHI. Moreover, at the Motion to Dismiss hearing, the Court questioned the Plaintiffs' ability to allege an injury-in-fact based on an increased risk of bodily injury or death. (Dkt. 167 at 71) The Court addresses each of these theories in turn.

i. Increased Risk of Future Identity Theft

Defendants argue that Non-Misuse Plaintiffs' alleged increased risk of future identity theft does not constitute an injury in fact under Clapper because they only assert a "mere possibility" that identity theft or misuse of their PII/PHI will occur in the future. (Dkt. 116 at 13–14) Plaintiffs respond that all Plaintiffs in this action face a substantial risk of identity theft, fraud, or other harm in light of the fact that PHI/PII from Defendant's database has already been offered for sale on the Internet and that several Plaintiffs have already experienced identity theft and other harm. (Dkt. 146 at 17–20)

The Eleventh Circuit has not yet addressed whether an increased risk of identity theft subsequent to a data breach is a cognizable injury in fact. See Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012) ("As Plaintiffs have alleged only actual—not speculative—identity theft, we need not address the issue of whether speculative identity theft would be sufficient to confer standing.") Other circuits, however, have addressed the question and have come to differing conclusions.[5] Beck v. McDonald, 848 F.3d 262,

5 There is a comparable disarray among district courts. Compare Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 316CV00014GPCBLM, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3,

273 (4th Cir. 2017) ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury in fact based on an increased risk of future identity theft."). The Ninth, Seventh, Sixth (in an unpublished decision), and D.C. Circuits have each found that an increased risk of identity theft subsequent to a data breach can be a sufficient injury in fact. In re Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (relying in part on Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010)); Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (relying in part on Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)). On the other hand, the First, Eighth, and Second (in an unpublished decision) Circuits have found no injury in fact in such circumstances. In re SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012). The Third and Fourth Circuit have straddled the circuit split with decisions finding no injury in fact based on an increased risk of identity theft based on one set of facts and a cognizable injury in fact on another set of facts. Hutton v. Nat'l Bd. of Examiners in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) (finding injury in fact); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (finding no injury in fact); In re Horizon Healthcare Services Inc. Data Breach Litigation,

---

2016) (finding injury in fact); Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *2 (C.D. Cal. June 15, 2015) (same); In re Adobe Systems, Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014) (same), with Provost v. Aptos, Inc., No. 1:17-CV-02120-ELR, 2018 WL 1465766, at *5 (N.D. Ga. Mar. 12, 2018) (finding no injury in fact); In re Cmty. Health Sys., Inc., Master File No. 15-CV-222-KOB, 2016 WL 4732630, at *8 (N.D. Ala. Sept. 12, 2016) (same); Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016) (same); Green v. eBay, Inc., No. 14–1688, 2015 WL 2066531, at *6 (E.D. La. May 4, 2015) (same); Storm v. Paytime, Inc., 90 F.Supp.3d 359, 364 (M.D. Pa. 2015) (same). For purposes of this Order, however, the Court will focus on the circuit court decisions that have addressed the issue.

846 F.3d 625 (2017) (in dicta, finding injury in fact); Reilly v. Ceridian Corp., 664 F.3d 38 (2011) (finding no injury in fact).

Notably, however, although the circuits have diverged in result, the bases behind the differing decisions have several commonalities. That is to say, the differing sets of facts involved in each circuit's decision are what appear to have driven the ultimate decision on standing, not necessarily a fundamental disagreement on the law. See In re SuperValu, Inc., 870 F.3d at 769 (noting that the differing results from the circuits on this issue "ultimately turned on the substance of the allegations before each court"). In this way, the Court can reconcile the decisions by extracting common guiding principles from the circuit decisions on the question of whether a plaintiff has adequately alleged an injury in fact based on an increased risk of identity theft.[6]

First, several of the circuits base their decisions, in part, on the alleged motive of the unauthorized third-party who received access to the plaintiffs' sensitive information. Among the circuits that consider the third-party's motive as a factor in the analysis, the rule is the same: a plaintiff is more likely to establish an injury in fact based on the increased risk of identity theft where the plaintiff has alleged that the third party behind the data breach targeted the plaintiff's personal information with an intent to use the information fraudulently. See e.g., In re Zappos.com, 888 F.3d at 1029 n.9 (finding that its decision that plaintiff adequately asserted an injury in fact is "consistent" with Fourth Circuit's finding in Beck that the plaintiffs did not sufficiently assert an injury in fact, based on the plaintiffs' differing allegations regarding the unauthorized third-party's intent).

6 The Court notes that each of the following guiding principles appears in some, but not all, of the circuits' decisions. Thus, in the explanations for each factor, the Court addresses only those circuit decisions that substantively addressed the subject factor in making its determination.

Applying this analysis, the Ninth, Seventh, and Sixth Circuits found an injury in fact in their respective cases because the plaintiffs alleged that the third-party *targeted* their personal information. The courts reasoned that a cognizable future injury existed because the ill-intentioned hackers' purpose was ultimately to use the plaintiffs' private information fraudulently. In re Zappos.com, 888 F.3d at 1029 n.9 (finding that plaintiffs' sufficiently alleged an injury where they "allege[d] that hackers specifically targeted their PII on Zappos's servers"); In re Horizon Healthcare Services Inc. Data Breach Litigation, 846 F.3d at 639 n. 19 (noting, in dicta, that a data breach created a material risk of harm where "[t]he theft appear[ed] to have been directed towards the acquisition of such personal information"); Galaria, 663 Fed. App'x. at 388 ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . 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."); Lewert, 819 F.3d at 967 (quoting Remijas, 794 F.3d at 693); ("It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is 'sooner or later to make fraudulent charges or assume those consumers' identities.'"); Remijas, 794 F.3d at 693 ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identities.").

Likewise, in Reilly, the Third Circuit, applying the same analytical framework, found the plaintiff's alleged heightened risk of identity theft was too speculative and insufficient to establish an injury in fact where there was "no evidence that the intrusion was

intentional or malicious." 664 F.3d at 44 (distinguishing the case from Ninth and Seventh Circuit cases where malicious intent and attempted use were alleged). In Beck, the Fourth Circuit found no injury in fact where the plaintiffs submitted no evidence that the thief of a laptop computer connected to a medical device at a medical facility "stole the laptop with the intent to steal [the plaintiffs'] private information." Beck, 848 F.3d at 274. On this basis, the Fourth Circuit distinguished the facts of its case from that of the cases decided by the Sixth and Seventh Circuits, in which the plaintiffs alleged that "the data thief intentionally targeted the personal information compromised in the data breaches." Id.

Thus, the Court finds that one factor considered by the diverging circuits in determining whether Plaintiffs have alleged an injury based on an increased risk of identity theft is the alleged motive of the unauthorized third-party that obtained access to Plaintiffs' personal information.

Second, several circuit courts on opposing sides of the "split" have considered the type of information compromised in the analysis of whether an increased risk of identity theft is an injury in fact. The courts addressing this factor have made a distinction between easily changeable or replaceable information, such as credit and debit card information, and personally identifiable information, such as social security numbers, birth dates, or driver's license numbers, which is more static.

Where credit card and debit card information is stolen, the circuits are divided on whether such information may enable a thief to assume the identity of the victim. The Second and Eighth Circuits have declined to find an injury in fact based on an increased risk of identity theft in such circumstances because card information generally cannot be

used alone to commit identity theft. In re SuperValu, Inc., 870 F.3d at 770 (citations omitted) (finding no injury in fact where the allegedly stolen information "does not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers" and "compromised credit or debit card information, like the Card Information here, generally cannot be used alone to open unauthorized new accounts"); Whalen, 689 F. App'x at 91–92 (finding no injury in fact where plaintiff could not "plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen" and distinguishing case from the Sixth Circuit's decision in Galaria, where breach involved personal information). Still, the Seventh and Ninth Circuit have held that such information can give rise to a threat of identity theft. In re Zappos, 888 F.3d at 1027 (finding that where plaintiffs' "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information" were stolen, but there was "no allegation … that the stolen information included social security numbers, as there was in *Krottner*, the information taken in the data breach still gave hackers the means to commit fraud or identity theft"); Lewert, 819 F.3d 963 (finding the threat of identity theft existed where plaintiffs alleged that their "debit-and credit- card data had been stolen," because "the information stolen from payment cards can be used to open new cards in the consumer's name").

Where personally identifying information, such as social security numbers and birth dates, is compromised the circuits that consider the type of information compromised as a factor have found an injury in fact because such information can be used for identity

theft. See Attias, 865 F.3d at 628 (quoting Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009)) (stating that the defendant "does not seriously dispute that plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were accessed by a network intruder, and drawing on 'experience and common sense,' we agree"); In re Horizon Healthcare Services, 846 F.3d at 639 n.19 (noting, in dicta, that a data breach compromising individuals' names, addresses, member identification numbers, dates of birth, social security numbers, and limited clinical information created a material risk of harm because "the information that was stolen was highly personal and could be used to steal one's identity"). What can be can be gleaned from the circuits' decisions in this respect is that the type of information compromised can play a role in the Court's injury in fact analysis, and, where that information includes personally identifiable information, this factor will weigh in favor of a finding of injury in fact.

Third, the circuits have found that 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. Attias, 865 F.3d at 628 ("Here . . . an unauthorized party has already accessed personally identifying data on [the defendant's] servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill."); In re Horizon Healthcare Services, 846 F.3d at 639 n. 19 (explaining, in dicta, that in accordance with the Seventh Circuit's decision in Remijas, a material risk of harm to plaintiffs existed because one plaintiff "alleged that he had already been a victim of identity theft as a result of the breach").

Accordingly, where there is no allegation that "the data has been—or will ever be—misused," an increased risk of identity theft has been found to be too speculative to constitute an injury. Reilly, 664 F.3d at 40 (finding plaintiff's alleged injury too speculative where it was not known "whether the hacker read, copied, or understood the data"); see also Beck, 848 F.3d at 274 (differentiating its case from the Seventh and Ninth Circuits' decisions where "at least one named plaintiff alleged misuse or access of [ ] personal information by the thief," since "even after extensive discovery, [the plaintiffs] uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft"); Katz, 672 F.3d at 80 (emphasis added) (recognizing as a "common denominator" among the circuit split that an increased risk of identity theft results where "the plaintiffs' data actually had been accessed by one or more unauthorized parties" and holding that plaintiffs alleged injury failed because she only alleges that "someone *might* access her data"). Indeed, based on this factor and the motive factor described above, the Fourth Circuit distinguished its holding in Beck that plaintiffs failed to establish an injury in fact based on an increased risk of identity theft from its later holding in Hutton v. National Board of Examiners in Optometry, Inc., where it found that plaintiffs did establish an injury in fact. 892 F.3d 613 (4th Cir. 2018). The Fourth Circuit explained:

> At a minimum, Plaintiffs have sufficiently alleged an imminent threat of injury to satisfy Article III standing. On that score, these cases stand in stark contrast to *Beck*, where we concluded that the threat was speculative because "even after extensive discovery" there was "no evidence that the information contained on [a] stolen laptop [had] been accessed or misused or that [the plaintiffs had] suffered identity theft." *See Beck*, 848 F.3d at 274. In fact, there was no evidence that the thief even stole the laptop with the intent to steal private information. *Id.* Here, the Plaintiffs allege that their data has been stolen, accessed, and used in a fraudulent manner.

Id. at 622.

In sum, in an attempt to harmonize the principles relied on by the circuits in the circuit split, the Court has distilled three non-exhaustive guiding factors for determining whether a plaintiff has sufficiently alleged that an injury in fact based on an increased risk of identity theft subsequent to a data breach: (1) the motive of the unauthorized third-party who accessed or may access the plaintiff's sensitive information, (2) the type of sensitive information seized, and (3) whether the information was actually accessed and whether there have been prior instances of misuse stemming from the same intrusion. In this case, Plaintiffs have sufficiently pleaded facts that satisfy each of these factors.

As to the intent of the unauthorized third-party, Plaintiffs have alleged that the third-party who accessed the Plaintiffs' personal information advertised the information for sale on the internet. (Dkt. 194 at ¶114 (citations and quotation marks omitted) ("[T]he FBI learned that an unauthorized party was attempting to sell compromised 21st Century Oncology data, which was advertised, in Russian, as approximately 10 million patient records from 21st Century Oncology available to purchase for $10,000.")) This allegation demonstrates that the interception of the Plaintiffs' data was not merely incidental or accidental, but rather driven by an intent to sell such data. Because Plaintiffs' sensitive information was targeted in the Data Breach, this factor weighs in favor of an injury in fact.

Regarding the type of information seized, Plaintiffs allege that "[t]he Data Breach resulted in the release, disclosure, and publication of private and highly sensitive PII/PHI including: names, Social Security numbers, physicians' names, medical diagnoses, treatment information, and insurance information." (Dkt. 194 at ¶ 6) Plaintiffs explain,

"PII/PHI such as Social Security numbers can be used indefinitely, because unlike credit and financial accounts, these numbers are extremely difficult to change. In addition, medical identity theft can continue to harm Plaintiffs and Class members indefinitely, because this information is often shared among numerous providers," and hackers may use it to procure prescription drugs or expensive medical equipment for months or years before the fraud is detected. (Dkt. 194 at ¶¶ 14, 207) Therefore, according to the Amended Complaint, "hackers today are targeting non-financial information, so they can continue to monetize victims' identities over a longer period of time." (Dkt. 194 at ¶ 208 (citations and quotation marks omitted)) Plaintiffs claim that on the black market, an individual healthcare record is worth more than a U.S-based credit card and personal identity with social security number combined. (Dkt. 194 at ¶ 205) Because the information compromised in the Data Breach is highly sensitive, not easily replaceable, and can be used over a long period of time, the Court finds that this factor too supports a finding of injury in fact. (Dkt. 194 at ¶ 114)

Finally, Plaintiffs have adequately pleaded that their information has been accessed and/or misused. First, Plaintiffs allege that the intruder accessed the information because he/she placed an advertisement for the information on the internet for sale. Second, according to Plaintiffs, an FBI informant purchased a sample of the advertised data and informed Defendants that "the unauthorized party listed additional data beyond the sample for sale." (Dkt. 194 at ¶ 119) Thus, the intruder not only accessed the information, but has also used the information in at least one transaction. This allegation factually distinguishes this action from the circuit court cases that precede it. Plaintiffs do not merely allege that they fear that their compromised information *may*

be advertised and sold on the Dark Web, Plaintiffs allege that it has *already happened*.[7] Third, half of the named plaintiffs, against whom Defendants do not assert an injury in fact challenge, have alleged that their personal information has already been misused. Among the alleged instances of misuse subsequent to the Data Breach, these Plaintiffs allege that unauthorized individuals made fraudulent purchases on their credit cards, attempted to open credit cards in their names, and fraudulently wired funds from their bank accounts, and one Plaintiff alleges that his health insurance was cancelled because his social security number was compromised. (See Dkt. 194 at ¶¶ 45–51, 61–95,101–107) Therefore, the factor of access/misuse likewise weighs in favor of Plaintiffs on the facts alleged in this case.

As the D.C. Circuit noted in Attias, "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already simply by virtue of the hack and the nature of the data that plaintiffs allege was taken." 865 F.3d at 629. Accordingly, based on the facts alleged in the Complaint, the Court finds that Plaintiffs have demonstrated an Article III injury in fact based on an increased risk of identity theft.

7 Plaintiffs contend that this allegation alone supports the notion that all plaintiffs have experienced actual misuse of their information, which they contend is sufficient on its own to constitute an injury in fact. (Dkt. 205 at 3–4) They likewise contend that all plaintiffs have experienced a concrete injury though emotional distress, including anxiety, concern and unease about unauthorized parties viewing and potentially using their compromised PII/PHI. (Dkt. 146 at 16) The Court need not reach whether these alleged harms satisfy the injury in fact requirement as it finds that that all plaintiffs have alleged an injury in fact due to their increased risk of identity theft and their mitigation efforts. See e.g., Attias, 865 F.3d at 626 n.2 (emphasis in original) ("Because we conclude that all plaintiffs, including the Tringlers, have standing to sue CareFirst based on their heightened risk of future identity theft, we need not address the Tringlers' separate argument as to *past* identity theft.").

ii. Mitigation Expenses

Defendants also challenge the Non-Misuse Plaintiffs' alleged injury caused by the cost of mitigating their increased risk of identity theft. Defendants assert that since Non-Misuse Plaintiffs' future risk of identity theft is not "certainly impending" as would be necessary to confer standing, any time or expense spent to mitigate such hypothetical future harm is likewise insufficient to constitute a cognizable injury. (Dkt. 116 at 15) Courts have found that the harm resulting from mitigation of a risk of future harm is largely dependent on whether the risk itself is substantial enough to be a standalone injury. See Provost, 2018 WL 1465766 at *5 (quoting Torres, 195 F. Supp. 3d at 1284) ("[T]he majority of courts in data breach cases have held that 'the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent.'"). Thus, in data breach cases, where courts have found an injury in fact based on an increased risk of identity theft, they have also found an adequate injury in fact based on the harm incurred by protecting against that risk. See e.g., Galaria, 663 F. App'x. at 388 (holding that plaintiffs' expenditure of "time and money to monitor their credit, check their bank statements, and modify their financial statements" was a concrete injury suffered to mitigate an imminent harm, and satisf[ied] the injury requirement of Article III standing"). Likewise, where the risk of identity theft is too speculative to constitute an injury in fact, the alleged injury of mitigation efforts to minimize that risk is likewise typically found to be non-cognizable. See e.g., In re SuperValu, 870 F.3d at 771 (citing Clapper, 133 S. Ct. at 1151) ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury."). Here, as described above, Plaintiffs

have sufficiently alleged an injury in fact based on an increased risk of identity theft. Thus, the Court finds that the time and money spent to protect themselves from that risk is also an injury in fact.

iii. Overpayment

Defendants move the Court to reject Plaintiffs' alleged overpayment theory because the Non-Misuse Plaintiffs never alleged that they paid anything specific for data protection, that they received a higher level of protection than those who did not pay for data protection services, that they paid a premium or otherwise bargained for data protection, or that they received any information about data protection other than a HIPAA notice. (Dkt. 116 at 16) (quoting In re Cmty. Health Sys., Inc., Master File No. 15-CV-222-KOB, 2016 WL 4732630, at *7 (N.D. Ala. Sept. 12, 2016)) Plaintiffs respond that overpayment does constitute an injury in fact because Plaintiffs would not have obtained services from Defendants had Defendants disclosed their data security problems. (Dkt. 146 at 22) As noted in In re Cmty. Health Sys., Inc., however, "a number of courts have rejected an 'overpayment' theory of damages as an injury in fact for standing purposes." 2016 WL 4732630 at *8 (collecting cases where courts rejected an "overpayment" theory of damages as injury in fact for standing purposes). Here, there are no factual allegations demonstrating that the Parties mutually agreed that any portion of the sums paid from Plaintiffs to Defendants would be allocated to data security. "Put another way, Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid." In re Sci.

Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 30 (D.D.C. 2014). Thus, the Court finds that this theory of injury in fact fails.

iv. Decreased Value of PII/PHI

Defendants further argue that Non-Misuse Plaintiffs may not base their injury-in-fact assertion on a claim of loss monetary value of their PII/PHI. (Dkt. 116 at 16) Plaintiffs claim that a growing number of federal courts have recognized the loss of value of PII/PHI as a cognizable harm. (Dkt. 146 at 22) (citing In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *43 (N.D. Cal. May 27, 2016)) The Court rejects this theory of injury in fact because Plaintiffs have not alleged that their personal information has an independent monetary value that is now less than it was before the Data Breach. See Provost v. Aptos, Inc., No. 1:17-CV-02120-ELR, 2018 WL 1465766, at *4 (N.D. Ga. Mar. 12, 2018) ("The Court is not persuaded by the hypothetical diminution of value propounded by Plaintiff. Plaintiff has failed to allege with particularity any facts explaining how her personal identity information is less valuable than it was before the Breach."); Welborn v. Internal Revenue Serv., 218 F. Supp. 3d 64, 78 (D.D.C. 2016) (collecting cases) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value.").

v. Increased Risk of Bodily Injury or Death

Plaintiffs also assert that they face an increased risk of bodily injury or death due to the Data Breach. (Dkt. 146 at 20) According to Plaintiffs, if identity thieves use Plaintiffs' PHI/PII for medical services and thereby commingle Plaintiffs' legitimate medical records with the thieves' records, the misinformation on the Plaintiffs' records

could result in misdiagnosis and erroneous medical treatment. (Dkt. 146 at 20) The Court finds that this theory of future risk of harm is too attenuated to constitute an injury in fact. Unlike the threat of identity theft described above, this theory depends on a "speculative chain of possibilities" that do not make out a "certainly impending" threat or create a "substantial risk" of harm. Clapper, 568 U.S. at 414. For Plaintiffs' potential harm to manifest: (1) Plaintiffs' medical information must be sold on the dark web, (2) the buyer/perpetrator must successfully use that information for medical services, (3) the medical services used by the perpetrator must be documented on plaintiffs' medical record; (4) the medical services used by the perpetrator must be inconsistent with Plaintiffs' own treatment plan such that it creates a risk of harm in Plaintiffs' future treatment, (5) Plaintiffs must receive medical treatment subsequent to the perpetrators' use of the medical information, (6) Plaintiffs must be harmed by such future treatment, and (7) the harm suffered by Plaintiffs' must be caused by the misinformation placed on Plaintiffs' medical record due to the perpetrators' use of Plaintiffs' medical information. The Court finds this chain of possibilities too speculative to constitute an Article III injury in fact.

In sum, although some of Plaintiffs' theories of injury fail to constitute an Article III injury in fact, Plaintiffs' Complaint survives Defendants' standing challenge because they have pleaded an injury in fact due to an increased risk of identity theft and the cost of mitigation efforts undertaken to minimize that risk.

b. Failure to State a Claim

Defendants also contend that Plaintiffs' Consolidated Complaint is due to be dismissed under Rule 12(b)(6) for failure to state a claim. Upon review of the filings, however, the Court finds that further briefing is required regarding which state's or states' law should apply to the claims as the Amended Complaint asserts only common law claims that require the application of state law.

In the ordinary case, a federal court sitting in diversity must apply the choice of law rules of the forum state. Pierce v. Prop. & Cas. Ins. Co. of Hartford, 303 F. Supp. 3d 1302, 1303 (M.D. Fla. 2017) (citing Travelers Prop. Cas. Co. of Am. v. Kan. City Landsmen, L.L.C., 592 F. App'x. 876, 881 (11th Cir. 2015)).[8] In a multidistrict litigation action, however, the transferee court is typically obliged to follow the choice of law rules attendant to the forum state of each transferor court. In re Takata Airbag Prod. Liab. Litig., No. 14-24009-CV, 2016 WL 3388713, at *2 (S.D. Fla. June 15, 2016) (quoting In re Managed Care Litig., 298 F.Supp.2d 1259, 1296 (S.D. Fla. 2003); Van Dusen v. Barrack, 376 U.S. 612, 639 (1964); In re Toyota Motor Corp. Unintended Acceleration, 785 F.Supp.2d 925, 931 (C.D. Cal. 2011)) ("In cases transferred pursuant to 28 U.S.C. § 1407, the transferee district court must apply the state law, including its choice of law rules, that would have been applied had there been no change of venue."). This is because when plaintiffs in multidistrict litigation proceedings file a consolidated pleading, it is usually a procedural device used for the purpose of convenience and not intended to disrupt the individual nature of each of the actions joined in the multidistrict litigation. In

8 The Court notes that "[a]lthough an unpublished opinion is not binding on this court, it is persuasive authority. See 11th Cir. R. 36-2." United States v. Futrell, 209 F.3d 1286, 1289 (11th Cir. 2000).

re Takata Airbag Prod. Liab. Litig., No. 14-24009-CV, 2016 WL 3388713, at *2 (S.D. Fla. June 15, 2016) ("This choice of law framework is not altered by the use of a consolidated complaint as a procedural device to streamline the litigation, unless the parties so consent").

The Supreme Court has noted in dicta that "[p]arties may elect to file a 'master complaint' and a corresponding 'consolidated answer,' which supersede prior individual pleadings. In such a case the transferee court may treat the master pleadings as merging the discrete actions for the duration of the MDL pretrial proceedings." Gelboim v. Bank of Am. Corp., 135 S. Ct. 897, 905, n.3 190 L. Ed. 2d 789 (2015) (citing In re Refrigerant Compressors Antitrust Litigation, 731 F.3d 586, 590–592 (6th Cir. 2013)); In re Conagra Peanut Butter Prod. Liab. Litig., 251 F.R.D. 689, 693 (N.D. Ga. 2008) (citations omitted) ("Using a master complaint as the operative pleading for choice of law purposes is not unprecedented in multidistrict litigation. . . . However, it is generally used as a substantive pleading only when the parties have consented to such an arrangement."). Therefore, courts have found that a consolidated complaint may be treated as a substantive complaint replacing the individual complaints only where the Parties consent to such treatment. Smokey Alley Farm P'ship v. Monsanto Co., No. 4:17 CV 2031 JMB, 2018 WL 278624, at *4 (E.D. Mo. Jan. 3, 2018) (emphasis added) ("Even if an MDL were established, a master complaint will not govern the action because master complaints cannot take the place of individual complaints *unless all the parties consent*."); In re Gen. Motors LLC Ignition Switch Litig., No. 14-MC-2543 (JMF), 2017 WL 3382071, at *8 (S.D.N.Y. Aug. 3, 2017) (The prevailing view, however, is that "a master complaint" in an MDL should not be used "as the operative pleading for choice of law purposes"

unless "the parties have consented to such an arrangement."); In re Takata Airbag Prod. Liab. Litig., 2016 WL 3388713 at *2 (emphasis added) ("This choice of law framework is not altered by the use of a consolidated complaint as a procedural device to streamline the litigation, *unless the parties so consent*"); In re Mercedes-Benz Tele Aid Contract Litig., 257 F.R.D. 46, 55–56 (D.N.J. 2009) (citations omitted) ("The use of a superseding complaint as the operative pleading for determining the proper choice of law rules in a multi-district litigation is not without precedent. Doing so is only appropriate, however, when the parties have agreed to such an arrangement."); In re Bridgestone/Firestone, Inc. Tires Prods. Liab. Litig., 155 F.Supp.2d 1069, 1078 (D.C. Ind. 2001) ("[T]he parties agree that this Court should be treated as the forum court because Plaintiffs filed their Master Complaint in this Court. Indiana's choice of law rules therefore are applicable.").

At the Motion to Dismiss hearing in this case, the Court discussed with the Parties' their intent regarding Plaintiffs' Consolidated Complaint. Plaintiffs made clear that their filing of the Amended Complaint was intended to supplant the individual complaints with a singular substantive complaint for choice of law purposes. (See Dkt. 167 at 4–5) However, Defendants were not as definitive and indicated that they may raise a choice of law issue later in the litigation. (Id. at 5–6) Nonetheless, Defendants indicate in a footnote in a subsequent filing that they agree that Florida's choice of law rules apply in this case, which suggests their agreement that the consolidated complaint should operate as a superseding pleading. (See Dkt. 157 at 1 n.1 (using Florida's choice of law rule to cursorily argue that Florida substantive law should apply to tort claims in this action))

Moreover, even if the Parties agree on which state's choice of law rules apply in this action, the Parties have not explained, except by passing reference in a footnote,

how such rules would apply to the claims asserted here. For instance, neither party has sufficiently applied the "most significant relationship test," Florida's choice of law rule regarding tort claims, to the factual allegations asserted in the Complaint to determine which state's substantive law should apply to Plaintiffs' tort claims. (See Plaintiffs' Supplemental Memorandum in Opposition to Defendants' Motion to Dismiss, Dkt. 156 at 2 (stating that "Florida applies the 'most significant relationship' test and it is unclear on this record which states' substantive law would apply to common law . . . claims asserted by citizens of different states")). Likewise, neither party has attempted to explain which state's or states' substantive law should apply to Plaintiffs' contract claims based on Florida's choice of law rule for contract claims. Instead, the Parties support their respective arguments concerning Defendants' Motion to Dismiss for failure to state a claim with law from an assortment of states. They also indicate that the substantive law of the various states on Plaintiffs' claims may differ in material ways. (See e.g., Dkt. 167 at 10 (suggesting that although Florida may require heightened pleading for a negligent misrepresentation claim sounding in fraud, "we know certain states [e.g., California and Arizona] diverge from the notice requirements under 9(b)."); Dkt. 146 at 29 n. 37 (distinguishing Florida's law on a breach of implied covenant of good faith and fair dealing, which requires that express term of a contract to be breached, from California, Arizona, and New Jersey's law on the claim, which do not)) Thus, the Court finds that briefing on the Parties' positions as to the substantive state law that is applicable to each of Plaintiffs' claims is necessary for the Court to resolve Defendants' motion to dismiss for failure to state a claim. Thus, to this point, the motion is denied without prejudice.

IV. CONCLUSION

Upon consideration of the foregoing, it is hereby **ORDERED** as follows:

1. Defendants' Motion to Dismiss Plaintiffs' Consolidated Complaint, (Dkts. 116, 195), is **DENIED** with respect to its lack of subject matter jurisdiction challenge.
2. Defendants' Motion to Dismiss Plaintiffs' Consolidated Complaint, (Dkts. 116, 195), is **DENIED WITHOUT PREJUDICE** with respect to its failure to state a claim challenge.
3. Defendants shall have up to and including **twenty-one (21) days** from the date of this Order to file an answer to Plaintiffs' Amended Consolidated Class Action Complaint.
4. The **CLERK** to is **DIRECTED** to **REOPEN** this case.

DONE and **ORDERED** in Tampa, Florida, this 11th day of March, 2019.

MARY S. SCRIVEN
UNITED STATES DISTRICT JUDGE

Copies furnished to:
Counsel of Record
Any Unrepresented Person