NOS. 17-1506(L); 17-1508

United States Court of Appeals

for the

Fourth Circuit

17-1506

RHONDA L. HUTTON, O.D.; TAWNY P. KAOCHINDA, O.D.
on behalf of themselves and all others similarly situated,

Plaintiffs-Appellants,

– v. –

NATIONAL BOARD OF EXAMINERS IN OPTOMETRY, INC.,

Defendant-Appellee.

(For Continuation of Caption See Inside Cover)

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND AT BALTIMORE, IN CASE NOS.1:16-CV-03025-JKB AND 1:16-CV-03146-JKB, HONORABLE JAMES K. BREDAR U.S. DISTRICT COURT JUDGE

JOINT BRIEF FOR PLAINTIFFS-APPELLANTS

NORMAN E. SIEGEL
BARRETT J. VAHLE
J. AUSTIN MOORE
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100

– and –

HASSAN A. ZAVAREEI
TYCKO & ZAVEREEI LLP
1828 L Street NW, Suite 1000
Washington, DC 20036
(202) 973-0900

Attorneys for Plaintiffs-Appellants Rhonda L. Hutton, O.D. and Tawny P. Kaochinda, O.D.

MICHAEL LISKOW
WOLF HALDENSTEIN ADLER FREEMAN & HERZ, LLP
270 Madison Avenue
New York, New York 10016
(212) 545-4600

– and –

CARL MALMSTROM
WOLF HALDENSTEIN ADLER FREEMAN & HERZ, LLP
70 West Madison Street
Chicago, Illinois 60602
(312) 984-0000

Attorneys for Plaintiff-Appellant Nicole Mizrahi

(For Continuation of Appearances See Inside Cover)

17-1508

NICOLE MIZRAHI, Individually and on behalf of all others similarly situated,

Plaintiff-Appellant,

– v. –

NATIONAL BOARD OF EXAMINERS IN OPTOMETRY, INC.,

Defendant-Appellee.

DONALD J. ENRIGHT
LEVI & KORSINSKY LLP
1101 30th Street, NW, Suite 115
Washington, DC 20007
(202) 545-4290

Attorneys for Plaintiff-Appellant Nicole Mizrahi

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Cases **Page(s)**

STATUTES & RULES **Page(s)**

I. JURISDICTIONAL STATEMENT

Plaintiffs-Appellants Rhonda L. Hutton, O.D. ("Hutton"), Tawny P. Kaeochinda, O.D. ("Kaeochinda") and Nicole Mizrahi, O.D. ("Mizrahi," collectively "Plaintiffs"), appeal from the March 22, 2017 memorandum and order of the United States District Court for the District of Maryland dismissing Plaintiffs' separate actions, *Hutton v. National Board of Examiners in Optometry, Inc.*, No. 1:16-cv-3025 (D. Md.) ("*Hutton*") and *Mizrahi v. National Board of Examiners in Optometry, Inc.*, No. 1:16-cv-3146 (D. Md.) ("*Mizrahi*"). A-37-45.[1]

The District Court had subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d), because the amount in controversy exceeds $5,000,000, at least one plaintiff and defendant are citizens of different states, and there are more than 100 putative class members.

This Court has jurisdiction pursuant to 28 U.S.C. § 1291 to hear this appeal from the final memorandum and order of the District Court that disposed of all parties' claims in both cases. A-37-45. These appeals are timely because Appellants filed Notices of Appeal in both actions on April 19, 2017, within the period required by law. A-48-49, 75-77.

[1] Citations to "A" are to the Joint Appendix page number.

II. ISSUES PRESENTED FOR REVIEW

The question on this appeal is whether the District Court erred in granting Defendant-Appellee the National Board of Examiners in Optometry's ("NBEO's") motion to dismiss Plaintiffs' actions under Federal Rule of Civil Procedure 12(b)(1) for lack of standing despite Plaintiffs having alleged that they suffered identity theft and fraud as the result of NBEO's failure to secure their sensitive personal information ("SPI"), thereby requiring Plaintiffs to spend time and money addressing the fraud.

III. STATEMENT OF CASE

A. Statement of Facts

Plaintiffs are optometrists who, as part of the optometry licensing process, were required to pay thousands of dollars to NBEO to sit for examinations it administered. A-54, 57-58, 63. On or around June 23, 2016, Plaintiffs and various optometrists around the country began to discover that fraudulent Chase bank Amazon-branded credit cards had been opened in their name. A-7-8, 12, 54-56, 59-60, 62. Through a number of Facebook groups, Plaintiffs and other optometrists began discussing the fraud and realized they had all been victims of a similar scheme. A-7-8, 12, 54-56, 59-60, 62. Upon further comparison, Plaintiffs and the other optometrists realized that NBEO was the only organization to which all of the optometrists had given the same set of SPI necessary to complete the

unauthorized credit card applications made in their names. A-12, 55. In particular, one member of a key Facebook group stated that the source could only have been NBEO because the unauthorized credit card application was made in her maiden name, and the only entity she had given sufficient SPI to apply for such credit card was NBEO. A-55.

NBEO declined to comment on the breach for a number of days until August 2, 2016, when it released a public statement that "[a]fter a thorough investigation and extensive discussions with involved parties, NBEO has concluded that our information systems have NOT been compromised." A-8, 55. However, just two days later, NBEO reversed its position and posted a "revision" to the prior statement that "NBEO has decided further to investigate whether personal data was stolen from our information systems to support the perpetrators' fraud on individuals and Chase." A-12-13, 55. NBEO never individually notified Plaintiffs or members of the putative class that a breach occurred. A-13, 61-62.

All Plaintiffs directly experienced having a credit card fraudulently applied for in their name. A-8-9, 62. Each Plaintiff lost time and incurred out-of-pocket costs to place credit freezes on their accounts and send certified letters to credit agencies attempting to head off further identity theft. A-8-9, 63. Plaintiff Mizrahi also experienced an 11-point drop in her credit score as a result of the fraudulent application. A-62-63.

B. Procedural History

On August 30, 2016, Plaintiffs Hutton and Kaeochinda filed a putative class action complaint against NBEO in the United States District Court for the District of Maryland alleging common law claims for negligence, breach of contract, breach of implied contract, as well as violations of the California Customer Records Act, Cal. Civil Code §1798.80, and the California Unlawful and Unfair Business Practices Act, Cal. Bus. & Prof. Code § 17200. A-6-36.

On September 13, 2016, Plaintiff Mizrahi filed a putative class action complaint in the United States District Court for the District of Maryland against NBEO alleging common law claims for negligence, breach of contract, breach of implied contract, and unjust enrichment. A-54-74.

On October 22, 2016, NBEO filed Motions to Dismiss in both actions pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6) or, in the Alternative, to Strike Pursuant to Fed. R. Civ. P. 12(f) and 23(d)(1)(D). On November 2, 2016, NBEO filed Motions to Consolidate the *Hutton* and *Mizrahi* cases in both actions.

On March 22, 2017, the District Court entered a Memorandum and Order in both actions granting NBEO's Motions to Dismiss for lack of subject-matter jurisdiction pursuant to Fed. R. Civ. P. 12(b)(1), and denied Defendants' motions to strike and to consolidate the actions as moot. A-37-45.

On April 19, 2017, Plaintiffs filed Notices of Appeal of the District Court's Opinion in both actions. A-48-49, 75-77. On May 8, 2017, both appeals were consolidated by the Court.

IV. SUMMARY OF ARGUMENT

The District Court is the first and only court in the country to hold that plaintiffs lack Article III standing to sue even after they have already suffered identity theft and fraud in the wake of a data breach. The District Court relied heavily on the fact that NBEO denied responsibility for the breach, even though Plaintiffs alleged that NBEO was the only possible common source. In reaching this conclusion, the District Court erred by failing to accept the allegations in the Complaints as true, and by inappropriately weighing competing assertions of fact at the pleading stage. The District Court's opinion sets a dangerous precedent of permitting companies to avoid liability in the wake of a data breach by simply denying responsibility, and is directly at odds with opinions across the country holding that allegations of identity theft and fraud (or even the increased risk of such) in the aftermath of a data breach are sufficient to confer Article III standing.

V. ARGUMENT

A. Standard Of Review

The Fourth Circuit reviews a dismissal under Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction *de novo*. *See Beck v. McDonald*, 848 F.3d 262,

269 (4th Cir. 2017) (citing *24th Senatorial Dist. Republican Comm. v. Alcorn*, 820 F.3d 624, 628 (4th Cir. 2016)).

B. Plaintiffs Have Standing To Pursue Their Claims Because They Have Already Suffered Identify Theft And Fraud

The District Court erred in concluding that Plaintiffs do not have Article III standing to pursue their claims. In reaching its decision the District Court largely relied on its reading of this Court's decision in *Beck*, 848 F.3d 262, a recent case discussing Article III standing in the context of a data breach. However, the District Court incorrectly increased the standing requirements set forth in *Beck* and the cases *Beck* relies upon, and thereby erred in dismissing Plaintiffs' actions.

To bring suit in federal court a plaintiff must establish standing to sue under Article III of the U.S. Constitution. This requires that the plaintiff "(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) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-561 (1992)). In a class action, standing is reviewed based on the allegations of injury to the named plaintiffs. *See Beck*, 848 F.3d at 269 (citations omitted). In reviewing whether a plaintiff has sufficiently alleged Article III standing at the pleading stage, "'general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the

claim.'" *Id.* at 270 (quoting *Lujan*, 504 U.S. at 561). Therefore, at this stage of the litigation the Court must accept Plaintiffs' allegations as true where there is sufficient "'factual matter' to render the allegations 'plausible on their face.'" *Id.* at 270 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal brackets omitted).

A defendant may challenge subject-matter jurisdiction in one of two ways, facially or factually. *See id.* at 270. Here NBEO has made a facial challenge to Plaintiffs' complaints by "contend[ing] 'that a complaint simply fails to allege facts upon which subject matter jurisdiction can be based.'" *Id.* (quoting *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009)). Accordingly, in opposing NBEO's facial challenge to standing, Plaintiffs are "'afforded the same procedural protection as [they] would receive under a Rule 12(b)(6) consideration,' wherein 'the facts alleged in the complaint are taken as true,' and the defendant's challenge 'must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction.'" *Id.* (quoting *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)).

1. Plaintiffs have alleged an injury in fact

The Supreme Court recently reiterated that a plaintiff seeking to demonstrate an injury in fact 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.* at 271 (quoting *Spokeo*, 136 S. Ct. at 1548).

This Court recently addressed the injury in fact requirement in the context of data breach litigation in *Beck*. *Beck* involved plaintiffs in two actions who alleged that their SPI was mishandled by a Veterans Affairs medical center when a laptop and boxes of documents containing the SPI of thousands of patients, including the plaintiffs, was misplaced or stolen from the center. *Beck*, 848 F.3d at 267-68. The plaintiffs brought suit on behalf of themselves and the patients whose SPI was contained on the laptop or in the documents, alleging that they risked imminent harm from misuse of the lost or stolen SPI and were forced to spend money and time to closely monitor their financial records for any indicia of fraud. *See id*.

In light of these facts, *Beck* analyzed whether the injury in fact requirement was satisfied by either "the increased risk of future identity theft" or "the costs of protecting against the same." *Id.* at 273. As discussed further *infra*, *Beck* rejected the plaintiffs' contention that their increased risk of prospective identity theft amounted to a sufficient injury by contrasting the plaintiffs' insufficient allegations with those of other courts where, like here, "at least one named plaintiff alleged misuse or access of that personal information by the thief." *Id.* at 274 (citing *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010)). Indeed, "in the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide either (1) actual

examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud." *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 532 (D. Md. 2016).

The plaintiffs in *Beck* did not satisfy this standard because "even after extensive discovery, the *Beck* plaintiffs . . . uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information." *Id.*, 848 F.3d at 274. The Court also held that the plaintiffs had failed to demonstrate that there was a substantial risk that identity theft would occur in the future because there was no indication that the data was misappropriated for the purpose of committing identity fraud. *See id.* at 275-76. Finally, the Court held that the plaintiffs' incurring of costs for monitoring for potential future identity theft was not a sufficient independent ground for injury where the potential harm had already been deemed to be speculative. *See id.* at 276-77.

Here, Plaintiffs easily satisfy the injury in fact requirement set forth in *Beck* because they have alleged that they *already* suffered identity theft and fraud (as have hundreds of other class members). A-8-9, 12, 18, 23, 29, 62-63, 67. Plaintiffs have also sufficiently alleged they are at an imminent risk of future harm

because there are "actual examples of the use of the fruits of the data breach for identity theft" as well as "a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud." *Khan*, 188 F. Supp. 3d at 532. These are concrete and particularized injuries stemming from NBEO's failure to sufficiently secure Plaintiffs' SPI.

a) Plaintiffs have already been actually, concretely injured by the data breach

There is no need to speculate about the possibility or likelihood of future injury in this case because, while Plaintiffs certainly remain at imminent risk of *additional* future harm, they have *already* been the victims of actual identity theft and fraud linked to the NBEO data breach. Specifically, Plaintiffs' SPI has been stolen and Chase Amazon credit card accounts were opened, or attempted to be opened, using their SPI without Plaintiffs' authorization or knowledge. A-8-9, 62-63. Moreover, each of the Plaintiffs incurred out-of-pocket costs and time lost in attempting to deal with the fallout from the data breach. A-8-9, 62-63. Plaintiff Mizrahi also experienced an 11-point drop in her credit score as a result of the fraudulent application. A-62-63.

Other courts have held that these and similar injuries amount to the "actual harm" required to demonstrate an injury-in-fact. For example, in *Remijas*, the plaintiffs alleged that the credit card information they provided to the defendant had been stolen from the defendant's system, leading to fraudulent charges. *See*

794 F.3d at 692. The Seventh Circuit held that allegations of both "lost time and money resolving the fraudulent charges" and "lost time and money protecting themselves against the future identity theft" were sufficient at the pleading stage to demonstrate actual, and not just imminent, injury, where plaintiffs, like those here, have also sufficiently alleged imminent injury, discussed *infra*. *Id*. at 694. *See also Hapka v. Carecentrix, Inc*., No. 16-2372-CM, 2016 WL 7336407, at *2 (D. Kan. Dec. 19, 2016) ("plaintiff's personal information has been fraudulently used to file a false tax return. Plaintiff has therefore suffered some form of actual, concrete injury."); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc*., No. 3:16-CV-00014-GPC-BLM, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016) ("Plaintiff has alleged that his credit card information was stolen and misused and that he arranged to cancel and reissue the compromised credit card after learning that his PII was misused. He further alleges that the need to mitigate his exposure to fraudulent charges and potential identity theft resulted in a loss of productivity. These allegations present a concrete, non-speculative harm that befell Plaintiff as a result of the Starwood breach."); *In re Anthem, Inc. Data Breach Litig*., No. 15-MD-02617-LHK, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) (finding that plaintiffs' allegations of using their own time to monitor their credit in the aftermath of a data breach was injury in fact sufficient to confer standing); *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D.

Ala. Sep. 29, 2015) (allegations of "actual identity theft and an economic injury . . . together constitute an injury in fact sufficient to meet the first prong of the standing analysis"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014) ("A handful of Plaintiffs claims that they have suffered actual identity theft, and those Plaintiffs have clearly suffered an injury.").

The District Court erred in analogizing the facts of this case to *Beck*, where there was no evidence individuals' personal information was misused in the aftermath of the breach. Here, by contrast, Plaintiffs have clearly alleged actual, concrete damages based upon actual identity theft that has *already* impacted them. A-8-9, 62-63.

The District Court also attempted to downplay the effects of the fraud experienced by Plaintiffs, hypothesizing that there may have been a legitimate reason for an unauthorized person to make unauthorized applications for Chase Amazon cards in Plaintiffs' name using Plaintiffs' Social Security numbers without their permission. A-44. Specifically, the District Court held that:

> An additional puzzlement is Plaintiffs' certainty that unsolicited credit cards *sent to them* constitute evidence of fraud. An instance of such may more reasonably indicate a questionable use of legitimately accessed information for the purpose of opening new accounts *for Plaintiffs*—in that event, no data breach would be at issue—and not an attempt to defraud Plaintiffs. The Court does not suggest one's receipt of an unsolicited credit card is not a cause for concern, but, in itself, it is not indicative of fraud.

A-44 (emphasis added). The District Court's unconventional and unsupported speculation as to the ramifications of having an unauthorized credit card applied for in one's name is flawed. First, there is no support for the proposition that Plaintiffs' information was "legitimately accessed" because, among other reasons, in order to apply for a credit card one must, at a minimum, be able to provide the Social Security number of the applicant. *See, e.g., Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("It is not plausible that a person could apply for a credit card without a social security number."). A Social Security number is a highly sensitive piece of personal data that is not recommended to be shared unless absolutely necessary (and was not alleged to have been inappropriately shared here by Plaintiffs). In fact, Plaintiffs specifically alleged that: "The U.S. Social Security Administration (SSA) warns that "[i]dentity theft is one of the fastest growing crimes in America." Indeed, "[i]dentity thieves can use [the victim's] number and your good credit to apply for more credit in [the victim's] name. . . . In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems." A-14-15.

Moreover, the opening of a new credit card is a significant credit event that can affect one's credit score – even simply applying for a credit card can have a detrimental effect on one's score, as occurred to Plaintiff Mizrahi. A-62-63; *see*

also Alston v. Cent. Credit Servs., Inc., Civil Action No. DKC 12-2711, 2013 WL 4543364, at *1 n.3 (D. Md. Aug. 26, 2013) ("A 'hard pull' is a full credit inquiry conducted when someone applies for a loan or line of credit. It has been said that each hard pull can result in the reduction of a credit score by up to five points.") (citations omitted).

The District Court acknowledged these realities by stating that it "does not suggest one's receipt of an unsolicited credit card is not a cause for concern," A-44, but then reached the incorrect conclusion, without providing any examples or citations to authority, that this "in itself, it is not indicative of fraud." *Id*. But in fact, applying for a credit card in someone else's name without permission, otherwise known as "application fraud," *is* a criminal act. *See, e.g., United States v. Hamer*, 10 Fed. Appx. 205, 215 (4th Cir. 2001) (defendant charged under 18 U.S.C. § 1014 with filling out a credit card application in another person's name); 18 U.S.C. § 1014 (subjecting a violator to a fine of not more than $ 1,000,000 or imprisonment of up to 30 years, or both).[2]

[2] Even NBEO did not contest that the unauthorized application for Chase Amazon Visa cards in Plaintiffs' names was a fraudulent "scheme," albeit one that NBEO purports went "well beyond the optometry community." *Hutton*, ECF No. 11-1 at 11. *See also id.* ("The alleged injuries suffered by Plaintiffs cannot be traced to such an incident and could likely be attributed to one of a number of data breaches suffered by a large number of consumers over the past several years.").

Here Plaintiffs did not receive an offer of credit, but instead had unauthorized credit card applications made in their names and, in the case of Hutton, the application was approved and an unauthorized account was opened in her name. A-8-9, 62-63. The Plaintiffs then spent time and money addressing the fraud. A-8-9, 62-63. This alone constitutes an actual, concrete injury in fact, as recognized by this Court in *Beck*. *See id.*, 848 F.2d at 274 (contrasting insufficient allegations of injury with those of *Krottner* where the named plaintiff alleged "someone attempted to open a new account using his social security number.") (citing *Krottner*, 628 F.3d at 1141). As explained below, it is also an objective indicator that the threat of future harm is real and imminent. *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016) ("a 'primary incentive' for hackers is 'sooner or later to make fraudulent charges or assume those consumers' identities.'") (quoting *Remijas*, 794 F.3d 688 at 693).

b) Plaintiffs face further certainly impending injury due to NBEO's failure to secure their SPI and the fact that Plaintiffs' SPI has already been misused

Even if the fraud and efforts to mitigate such fraud described above are not considered "actual" harm standing alone, the District Court erred in holding that the misuse of Plaintiffs' SPI did not indicate a substantial risk of future harm.

For example, in *Hapka*, the plaintiff sued her former employer for failing to protect her SPI, which was used to file a fraudulent tax return in her name. The

defendant conceded that the fraud was evidence of misuse, but argued that the plaintiff's allegations of future injury "are too speculative to provide plaintiff with standing to pursue her claims based on those injuries." *Id.*, 2016 WL 7336407, at *2. In rejecting this argument, the court held: "The problem with defendant's approach is that defendant wants the court to look at each of plaintiff's alleged injuries in a vacuum. While standing is an individualized inquiry, . . . the allegation that plaintiff is the victim of tax fraud impacts plaintiff's other allegations of injury. The fact that her stolen information has been used once has a direct impact on the plausibility of future harm. The court therefore considers plaintiff's allegations of future harm in light of her allegations that her personal information was used for tax fraud shortly after the data breach." *Id.*

The same is true here. The fact that Plaintiffs have already alleged misuse of their SPI has a direct impact on the plausibility of future harm, a principle that has been recognized by this Court and many others.

In *Beck*, guided by the Supreme Court's decision in *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), this Court held that the injury in fact requirement may be met by either an allegation of a threatened injury that is "certainly impending," or that there is a "substantial risk" of future harm. *Beck*, 848 F.3d at 271-72, 275; *see also Clapper*, 568 U.S. at 1150 n.5 (endorsing finding standing "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to

reasonably incur costs to mitigate or avoid that harm.") (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153 (2010)).

Beck then favorably cited a number of cases with facts similar to those here in which the plaintiffs' allegations "sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274. For example, *Krottner* involved data breach claims by employees at a Starbucks from which a laptop containing their names, addresses and social security numbers was stolen. *See id.*, 628 F.3d at 1140-41. There, the Ninth Circuit held that the plaintiffs had sufficiently alleged a "credible threat of real and immediate harm" due to, *inter alia*, one plaintiff's allegations that "his bank notified him . . . that someone had attempted to open a new account using his social security number. The bank closed the account, and [the plaintiff] does not allege that he suffered any financial loss." *Id.* at 1141, 1143. The Plaintiffs here not only faced the same attempts to open a financial account in their name with their Social Security numbers, but additionally had to spend time and money attempting to address and prevent future injury.

Similarly, in *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016), the Sixth Circuit reversed the district court's dismissal of a data breach case in the context of a breach of Nationwide's computer network because the

information was stolen for the purpose of committing fraud. The Sixth Circuit held that:

> Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation. Plaintiffs allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of "possible future injury" or "objectively reasonable likelihood" of injury that the Supreme Court has explained are insufficient. 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.

Id. at 388 (quoting *Clapper*, 133 S. Ct. at 1147-48) (emphasis added). The Sixth Circuit noted that the "allegation in the proposed amended complaint that Plaintiff Galaria suffered three unauthorized attempts to open credit cards in his name further supports standing," *id.* at 389 n.1, and that the plaintiffs' costs expended in attempting to prevent further misuse of their data represented a "concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing." *Id.* at 389.

Similarly, in *Remijas*, the Seventh Circuit held that victims of a data breach at a department store had established injury-in-fact by alleging a "substantial risk of harm" from the theft of their data because [w]hy 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 a fraudulent charge or assume those consumers' identities." *Id.*, 794 F.3d at 693. Even absent existing fraud, and

where, unlike here, Social Security numbers were not exposed, the Seventh Circuit recognized that efforts taken by class members to mitigate future harm were sufficient to confer standing. *See id.* at 694 (purchasing credit monitoring costs "easily" qualified as Article III injury).

The Seventh Circuit reached the same conclusion in *Lewert*, where the defendant restaurant's customers' credit card data was alleged to have been stolen in a data breach, because a "primary incentive" for such a breach is to commit fraud. *Id.*, 819 F.3d at 965, 967. *Lewert* involved an alleged breach of data containing credit card information, but not Social Security numbers, and the plaintiffs later had unauthorized charges made to their card. Despite the fact that those charges were later reversed, the court *still* found that the plaintiffs had alleged imminent harm because "[e]ven if those fraudulent charges did not result in injury to his wallet (he stated that his bank stopped the charges before they went through), he has spent time and effort resolving them. He also took measures to mitigate his risk by purchasing credit monitoring for $106.89." *Id.* at 967.

Other courts have reached similar conclusions. In *In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014), hackers accessed the SPI of millions of customers, including names, credit and debit card numbers, expiration dates and mailing and email addresses. *See id.* at 1206. The court found that "the threatened harm alleged [was] sufficiently concrete and imminent"

because "the risk that Plaintiffs' personal data will be misused by the hackers . . . is immediate and very real." *Id*. at 1214. There, as here, speculation was not required as "stolen data had already surfaced on the internet." *Id*. at 1215. Accordingly "the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as 'certainly impending'" and "the threatened injury here could be more imminent *only* if Plaintiffs could allege that their stolen personal information had *already been misused*." *Id*. (emphasis added). *See also Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (rejecting argument that "plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing.").

Of course here Plaintiffs' claim of standing is even stronger than these cases because their stolen information has *already* been misused. Thus, there "is no need for speculation" as to whether substantial harm to Plaintiffs is likely to occur, because fraud has already manifested. *Galaria*, 663 Fed. App'x at 388; *see also Hapka*, 2016 WL 7336407, at *2 ("The fact that [plaintiff's] stolen information has been used once has a direct impact on the plausibility of future harm.").

The District Court further erred when it appeared to hold that actual fraudulent charges, a denial of credit, or an increased interest rate for credit are a prerequisite to injury. A-44. Victims of data breaches need not wait until their clearly stolen SPI is *successfully* misused in a manner that concretely affects their

finances. Instead, the fact that Plaintiffs' SPI, and in particular their Social Security numbers, have been confirmed to be in the hands of any number of malevolent actors who have already exploited such personal data, and can continue to exploit it in the future at the time of their choosing, is more than injury enough. *See, e.g.*, *Adobe*, 66 F. Supp. 3d at 1215 ("[T]o require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact.") (citing *Clapper*, 133 S. Ct. at 1150 n.5); *Lewert*, 819 F.3d at 967 (same); *Chambliss v. CareFirst, Inc.*, 189 F. Supp. 3d 564, 570-71 (D. Md. 2016) (distinguishing case where data breach plaintiff lacked standing from cases that "concerned information more easily used in fraudulent transactions" such as Social Security or credit card numbers, or "relied on factual allegations that the hackers had already misused the stolen data such that the risk of future harm was certainly impending."); *see also id*. at 571 ("where credit card and social security numbers are stolen, the future harm is not speculative as '[w]hy else would hackers break into a store's database and steal consumers' private information?'") (quoting *Remijas*, 794 F.3d at 694) (brackets in original).[3]

[3] Plaintiffs made extensive allegations of the never-ending nightmare that one faces when their Social Security number has been stolen by those with an intent to misuse it. A-14-17, 59, 63-66.

Plaintiffs' SPI *was* misused to make unauthorized applications for credit cards, requiring the unauthorized use of Plaintiffs' stolen Social Security numbers, which applications were successful in Plaintiff Hutton's case and led to a decrease in Plaintiff Mizrahi's credit score. A-8-9, 62-63. In light of these allegations, Plaintiffs have clearly met the injury in fact requirement under *Beck* and *Clapper* by plausibly alleging both actual and certainly impending injuries, as well as a substantial risk of future harm.

2. Plaintiffs' injuries are fairly traceable to NBEO's conduct

Plaintiffs have also more than plausibly alleged that their injuries are traceable to NBEO's negligent failure to secure the SPI of Plaintiffs and the class. To satisfy Article III's "traceability" requirement a plaintiff must plausibly allege "'a causal connection between the injury and the conduct complained of,' rather than [that] the injury occurr[ed] as a result of 'the independent action of some third party not before the court.'" *Daniels v. Arcade, L.P.*, 477 Fed. Appx. 125, 129 (4th Cir. 2012) (quoting *Lujan*, 504 U.S. at 560) (citation omitted). "Traceability, however, does not require the defendant to be the only party responsible for the injury, or the party that contributes most significantly to the injury." *EarthReports, Inc. v. U.S. Army Corps of Engineers*, No. 8:10-CV-01834-AW, 2011 WL 4480105, at *6 (D. Md. Sep. 26, 2011) (citations omitted). The Fourth Circuit has stated that a plaintiff does not need to prove traceability with scientific certainty;

rather, a plaintiff must merely show that a defendant takes an action "'that causes *or contributes* to the kinds of injuries alleged' in the specific geographic area of concern." *Id.* (quoting *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 161 (4th Cir. 2000)) (emphasis added). Moreover, the element of traceability is "not focused on whether the defendant caused the plaintiff's injury in the liability sense, because causation to support standing is not synonymous with causation sufficient to support a claim." *Galaria*, 663 F. App'x at 390 (internal quotations omitted). Instead, "the traceability requirement mainly serves to eliminate those cases in which a third party and not a party before the court causes the injury." *Id.* (internal quotations omitted); *see also Nat. Res. Def. Council v. Watkins*, 954 F.2d 974, 980 n.7 (4th Cir. 1992) ("'fairly traceable" requirement . . . not equivalent to a requirement of tort causation.'") (quoting *Pub. Interest Research Grp. v. Powell Duffryn Terminals*, 913 F.2d 64, 72 (3d Cir. 1990)).

Here the District Court erred in holding that Plaintiffs' allegations regarding NBEO's culpability for the data breach rested solely upon "sheer speculation," and therefore Plaintiffs "failed to allege a plausible, inferential link between the provision of [SPI] to NBEO at some point in the past and their recent receipt of unsolicited credit cards." A-8. But far from providing only "sheer speculation," Plaintiffs' allegations, when properly considered as a whole, demonstrate that it is

not only plausible, but likely that a breach of NBEO's database was the event that led to Plaintiffs' SPI falling into the hands of hackers who used the SPI to commit identity theft. *See Tobey v. Jones*, 706 F.3d 379, 387 (4th Cir. 2013) (citing *Iqbal*, 556 U.S. at 698-99). For example, Plaintiffs' complaints include extensive allegations tying the breach to NBEO, including facts establishing that NBEO is the only national optometry group that collected Social Security numbers during relevant time periods, that fraudsters used outdated personal information (such as maiden names) on credit applications that were provided only to NBEO, and that optometrists across the country formed Facebook groups to discuss the fraud and determined that NBEO was the only common source for their fraud:

1. Each of the three Plaintiffs, optometrists who had provided SPI including their Social Security numbers to NBEO, had an unauthorized individual or individuals apply for, specifically, a Chase Amazon credit cards in their names at about the same time. A-8-9, 56, 62-63.

2. On or around July 23, 2016, optometrists from around the country began to notice that fraudulent Chase accounts were being opened in their names. They started discussing it on various Facebook groups and soon realized they were all victims of the same type of fraud. In particular, many optometrists learned that a Chase Amazon Visa credit card had been applied for in their name, or some other line of credit, and all within a few days of one another. The optometrists soon realized that the only common source amongst them and to which they had all given their SPI that included Social Security numbers and dates of birth (information necessary to apply for new lines of credit, among other things), was NBEO, where every graduating optometry student has to submit their SPI to sit for board-certifying exams. This also affected optometrists who served as examiners or committee members for NBEO and optometrists who

later sat for additional NBEO competency exams well after graduating from optometry school. Individuals that submitted their SPI to NBEO even more than fifteen years ago have been affected, and the fraud has expanded from only Chase accounts to other means. A-7-8, 12, 59-60, 62.

3. The unauthorized application for a Chase Amazon card in Plaintiff Hutton's name was made in her maiden name that she had previously provided to NBEO. A-9. This was similar to another optometrist who reported that an unauthorized credit card application was made in her maiden name, which she had last (and possibly only) used when applying to NBEO. A-55.

4. NBEO collects the full Social Security numbers and dates of birth of exam takers, among other types of SPI, and maintains it, in some instances, for fifteen years or more after the exam-takers have ceased to have a relationship with NBEO. A-7-8, 12, 56, 60.

5. To apply for any credit card, including the Chase Amazon card, one must be able to provide, *inter alia*, the applicant's full Social Security number and date of birth. A-7-8, 58-60, 64; *Antman*, 2015 WL 6123054, at *11.

6. In July 2016, after multiple optometrists around the country began reporting that there had been fraudulent, unauthorized applications made in their names for, specifically, Chase credit cards, members of the optometric community analyzed which common organizations they had provided their SPI to, and concluded that the only match was NBEO because, *inter alia*, other potential common sources, including the American Optometric Association ("AOA"), the American Academy of Optometry ("AAO"), and the Association of Schools and Colleges of Optometry ("ASCO"), neither gather nor store Social Security numbers and therefore could not have been the source of the SPI hackers required to apply for the Chase Amazon cards. A-12, 59-60, 62.

7. NBEO failed to implement basic data security measures as demonstrated by its retention of some exam-takers' SPI for fifteen years or more, and its inadvisable practice of allowing exam-takers to access their account by entering the last six digits of their Social Security number. A-12-14, 23, 26, 28, 31-32, 59-60, 69-71.

Pre-discovery, it is difficult to imagine what more Plaintiffs could allege to establish that the breach was fairly traceable to NBEO. Accordingly, Plaintiffs easily meet *Iqbal* and *Twombly*'s requirement that their traceability allegations be "'plausible on [their] face.'" *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

The District Court reached its erroneous conclusion by improperly focusing on a handful of these allegations in isolation to the exclusion of others, and in some instances misapprehends Plaintiffs' allegations. First, the District Court decided that "Plaintiffs do not explain why NBEO's denial of a data breach is less credible than those of the other optometry-related organizations." A-43-44. But Plaintiffs *did just this* in the very allegation that the District Court cites to, where Plaintiffs stated that "[t]he other potential common links, the [AOA, AAO, and the ASCO], *neither gather nor store Social Security numbers*." A-12 (emphasis added). In other words, as Plaintiffs alleged elsewhere in their complaints, the other organizations *could not* have been the source of the data breach which led to unauthorized attempts to apply for credit cards in Plaintiffs' names because these organizations did not solicit or maintain the Social Security numbers required to commit the fraud. *See* A-7-8, 12, 58-60, 64; *Antman*, 2015 WL 6123054, at *11.

The District Court similarly held that Plaintiffs' "speculation is mistakenly fueled by NBEO's announcements that it is looking into whether an intrusion

occurred and that it denies such in fact happened." A-43. The District Court then concluded that such "neutral announcement does not imply culpability, despite Plaintiffs' preferred interpretation otherwise." A-43. But the District Court is making factual determinations rather than accepting the allegations in the Complaints as true. If NBEO is not the source of the breach, it can certainly produce evidence to that effect on a summary judgment motion. *See Lewert*, 819 F.3d at 968-69. But the facts as *alleged* – including that hundreds of optometrists have conferred and confirmed online that NBEO is the only common source for their fraud – are sufficient, at the pleading stage, to plausibly trace the breach to NBEO. A-12, 18, 23, 29, 67.

The District Court also observed that "the complaints do not allege that only optometrists registered with NBEO received unsolicited Chase Amazon Visa cards." A-44. This argument is a red herring. The fact that individuals *other than optometrists* may have experienced a similar *type* of fraud has no bearing on whether the harm at issue is traceable to the NBEO breach. Indeed, in a world where a seemingly endless parade of data breach incidents have occurred involving almost every type of credit card and payment instrument, it is no surprise that fraudsters use stolen information to perpetrate similar types of fraud.

For example, millions of individuals last year had fraudulent tax returns filed in their name. Some victims may have had their information compromised through

their employer, while others may have had their information comprised through a retail store breach. The fact the victims suffered the same *type* of fraud has no bearing on what entity suffered a breach. Indeed, the fact that other individuals may have unauthorized Chase Amazon credit cards opened in their name establishes only that this was a quick and easy fraud to perpetrate.[4] It does not diminish Plaintiffs' allegations that each of the three Plaintiff *optometrists*, as well as other *optometrists* who provided their data to NBEO, *specifically* had an Amazon Chase credit card fraudulently applied for in their name around the same period of time.[5] *See* A-7, 9, 56, 62-63. This fact more than plausibly suggests that a single common criminal or group used the same identity theft scheme to steal and misuse the same set of stolen data, here the SPI of NBEO's test-takers.

Moreover, Plaintiffs are not required to rule out all other potential hackers or data breaches as the cause of their injury. *See Remijas*, 794 F.3d at 696 (where

[4] Fraudsters engaged in this scheme because it was a simple way to take advantage of a promotion offered by Amazon whereby Amazon users received a free $50 in their Amazon account upon applying for a Chase Amazon credit card. Therefore, the fraudsters would use victims' real information to apply for a Chase Amazon credit card, and then link the card to a dummy Amazon account where the fraudster would receive a free $50. The victims would then receive a copy of the unauthorized credit card at their home address.

[5] NBEO's citation to the Shelbyville news report, which warned that the scam "affected dozens of residents in the central Illinois area," actually aligns with Plaintiffs' argument, as it is apparently another example of a localized fraud that stemmed from a breach of SPI of individuals in the central Illinois region. Similarly here Plaintiffs have alleged that their SPI, and the SPI of the similarly-situated class, was stolen from a single data source, NBEO.

data breach allegations against a defendant are plausible the fact that another party "might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue."); *Lewert*, 819 F.3d at 969 ("Merely identifying potential alternative causes does not defeat standing."). Instead, NBEO's contention that Plaintiffs' injury may stem from a different data breach is merely "a legal theory that [NBEO] might later raise as a defense." *Id.*

The District Court further erred by grounding its decision on the incorrect finding that "in all of the cases discussed by the *Beck* Court, and in all of the cases that have been cited by the parties in the instant cases, an actual data breach had occurred and had been acknowledged or announced by the entity whose data files had been breached." A-43. As an initial matter, whether NBEO had acknowledged or announced that the breach occurred is not a prerequisite of standing, and the creation of such a requirement would provide a simple roadmap for defendants who believe or know that a data breach may have occurred – simply deny the breach. Moreover, Plaintiffs *did* cite cases where the defendant denied the alleged breach, *Lewert*, 819 F.3d 963, and *Khan*, 188 F. Supp. 3d 524, and which support Plaintiffs' position. *See Hutton* ECF No. 15 at 3-6, 7, 11; *Mizrahi* ECF No. 13 at 4, 7.

In *Lewert*, the plaintiffs alleged that credit card information they had provided one of the defendant's restaurants in Northbrook, Illinois was stolen from

the restaurant and later used to make unauthorized purchases. *See id.*, 819 F.3d at 965. The defendant performed an investigation into the alleged breach and determined that while data had been stolen from some of its restaurants, none had been stolen from the specific Northbrook location that the plaintiffs had allegedly patronized. *See id.* Accordingly, the defendant argued that the plaintiffs lacked standing because, unlike in other similar cases, the defendant contested that the plaintiff's alleged breach had occurred. *See id.* at 967-68.

The Seventh Circuit rejected this challenge to standing, noting that as the plaintiffs' allegations were plausible they must be accepted as true at the motion to dismiss stage, and the defendant's argument that the alleged breach did not occur merely "creates a factual dispute about the scope of the breach, but it does not destroy standing. [The defendant] will have the opportunity to present evidence to explain how the breach occurred and which stores it affected." *Id.* at 968.[6]

Similarly, in *Khan*, 188 F. Supp. 3d 524, the plaintiff alleged that the SPI it had provided to the defendant children's hospital was stolen from the hospital's emails in a data breach. *See id.* at 527. In response the defendant contended, after

[6] *See also id.* at 969 ("[the defendant] argues that the plaintiffs cannot show causation because . . . any fraudulent charges cannot be attributed to its data breach. The former argument assumes the answer to a disputed fact - whether the Northbrook restaurant was among those hit by the hackers. Plaintiffs have alleged that it was, and they have included enough facts to push that allegation to the point of plausibility. The latter argument is a theory of defense that [the defendant] will be entitled to pursue at the merits phase.").

having conducted an investigation by an outside forensics firm, that there was "no evidence that the information in the emails has been misused or even accessed." *Id.* (citations omitted); *see also Khan*, Civil Action No. TDC-15-2125, ECF No. 22-2 (letter from defendant to plaintiff describing results of data breach investigation). Despite this, neither the defendant nor the court took issue with the plaintiff's allegations that the data breach was traceable to the defendant. *See id.* at 528 (defendant "limits its attack on Khan's standing to . . . injury in fact.").

At bottom, the District Court improperly made factual determinations at the motion to dismiss stage and, in so doing, ignored this Court's holding in *Beck* where the Court noted that as the plaintiffs had alleged that their SPI had been stolen, "[w]e of course accept this allegation as true." *Id.* at 275; *see also Galaria*, 663 F. 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 criminal."); *Id.* at 390 n.3 ("We must accept as true Plaintiffs' allegations about the nature of the breach and the data stolen, and construe the complaints in Plaintiffs' favor. These allegations might not be borne out by discovery, but are plausible, based on rational inferences from known facts, and are sufficient to survive a motion to dismiss.") (citations omitted). Plaintiffs have sufficiently alleged traceability here.

3. Plaintiffs' injuries can be redressed by an award of damages

Plaintiffs must also plausibly allege that it is "'likely and not merely speculative that the plaintiff's injury will be remedied by the relief plaintiff seeks in bringing suit.'" *Beck*, 848 F.3d at 269 (quoting *David v. Alphin*, 704 F.3d 327, 333 (4th Cir. 2013)).[7] "[N]o explicit guarantee of redress to a plaintiff is required to demonstrate a plaintiff's standing." *Equity in Ath., Inc. v. Dep't of Educ.*, 639 F.3d 91, 100 (4th Cir. 2011). Here Plaintiffs have clearly alleged that they are the victims of identity theft and fraud, and have and will continue to expend time and money in mitigation of that harm. *See* A-8-9, 16-18, 56, 62-66. Plaintiffs maintain, and NBEO does not contest, that an award of monetary damages may redress their injuries. A-35, 73. *See also, e.g., Beck*, 848 F.3d at 274 n.5 ("in data-breach cases, there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely.") (internal citations omitted); *Galaria*, 663 F. App'x at 391 ("Plaintiffs seek compensatory damages for their injuries, and a favorable verdict would provide redress."); *Lewert*, 819 F.3d at 969 (finding redressability where plaintiffs can show that they "spent time and resources tracking down the possible fraud."). Based on the foregoing, Plaintiffs

[7] Neither NBEO nor the District Court disputed that Plaintiffs' claims satisfy the redressability requirement.

have satisfied each element of Article III standing, and the District Court erred in holding to the contrary.

VI. CONCLUSION

For the reasons stated herein, Plaintiffs respectfully request that the Court reverse the District Court's grant of NBEO's Motion and remand the cases for further proceedings.

Respectfully submitted this 19th day of June, 2017.

/s/ Michael Liskow
Michael Liskow
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
270 Madison Avenue
New York, New York 10016
liskow@whafh.com
Telephone: 212/545-4600
Facsimile: 212/545-4653

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl Malmstrom
One South Dearborn St., Suite 2122
Chicago, IL 60603
malmstrom@whafh.com
Telephone: 312/984-0000
Facsimile: 312/212-4401

Attorneys for Plaintiff-Appellant Nicole Mizrahi

/s/ Norman E. Siegel
Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City MO 64112
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
Telephone: (816) 714-7100
Facsimile: (816) 714-7101

Attorneys for Plaintiffs-Appellants Rhonda L. Hutton, O.D. and Tawny P. Kaeochinda, O.D.

STATEMENT REGARDING ORAL ARGUMENT

If this Circuit has any inclination to affirm the District Court's decision, Plaintiffs respectfully request a hearing for oral argument on this Appeal.

Dated: June 19th, 2017

Respectfully submitted,

/s/ Michael Liskow
Michael Liskow
Counsel for Appellant Nicole Mizrahi

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(b) because this brief contains 8,231 words, excluding the parts of the brief exempted by Fed. R. App. P. 32 (a)(7)(B)(iii).

This brief complies with the typeface requirement of Fed. R. App. P. 32 (a)(5) and the type style requirements of Fed. R. App. P. 32 (a)(6), because this brief has been prepared in a proportionally spaced typeface Microsoft Word, in fourteen-point font size using Times New Roman type style.

/s/ Michael Liskow
Michael Liskow
Counsel for Appellant Nicole Mizrahi

CERTIFICATE OF SERVICE

I hereby certify that on this 19th day of June, 2017, I caused this Joint Brief of Appellants and Joint Appendix to be filed electronically with the Clerk of the Court using the CM/ECF System, which will send notice of such filing to the following registered CM/ECF users:

Claudia Drennen McCarron, Esq.
MULLEN COUGHLIN LLC
1275 Drummers Lane, Suite 302
Wayne, PA 19087

Norman E. Siegel
Barrett Jay Vahle
STUEVE SIEGEL HANSON, LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112

Hassan A. Zavareei
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, DC 20036

I further certify that on this 19th day of June, 2017, I caused the required copies of the Joint Brief of Appellants and Joint Appendix via express mail to the Clerk of the Court.

/s/ Michael Liskow
Michael Liskow
Counsel for Appellant Nicole Mizrahi

793502