No. 14-3122

In the
United States Court of Appeals
for the Seventh Circuit

HILARY REMIJAS, on behalf of herself and all others
similarly situated, et al.,

Plaintiffs-Appellants,

v.

NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company,

Defendant-Appellee.

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division, No. 1:14-cv-01735.
The Honorable **James B. Zagel**, Judge Presiding.

BRIEF OF PLAINTIFFS-APPELLANTS HILARY REMIJAS, MELISSA FRANK, DEBBIE FARNOUSH and JOANNE KAO

TINA WOLFSON
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, California 90069
Tel: (310) 474-9111
Fax: (310) 474-8585

JOSEPH J. SIPRUT
SIPRUT PC
17 North State Street, Suite 1600
Chicago, Illinois 60602
Tel: (312) 236-0000
Fax: (312) 267-1906

Attorneys for Plaintiffs-Appellants

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 14-3122

Short Caption: Remijas v. Neiman Marcus Group, LLC

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao (Plaintiffs-Appellants)

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Siprut PC; Ahdoot & Wolfson, PC; Morgan & Morgan Complex Litigation Group; Heninger Garrison Davis, LLC; Glancy Binkow & Goldberg, LLP; Kazerouni Law Group, APC; Hyde & Swigart; Law Offices of Paul C. Whalen, PC.

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

N/A

Attorney's Signature: s/ Joseph J. Siprut Date: 10/15/14

Attorney's Printed Name: Joseph J. Siprut

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** X **No** ____

Address: 17 N. State St., Suite 1600, Chicago IL 60602

Phone Number: 312-236-0000 Fax Number: 312-267-1906

E-Mail Address: jsiprut@siprut.com

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 14-3122

Short Caption: Remijas v. Neiman Marcus Group, LLC

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao (Plaintiffs-Appellants)

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Siprut PC; Ahdoot & Wolfson, PC; Morgan & Morgan Complex Litigation Group; Heninger Garrison Davis, LLC; Glancy Binkow & Goldberg, LLP; Kazerouni Law Group, APC; Hyde & Swigart; Law Offices of Paul C. Whalen, PC; Law Office of Wendy R. Stein.

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

N/A

Attorney's Signature: s/ Tina Wolfson Date: 10/15/14

Attorney's Printed Name: Tina Wolfson

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: 1016 Palm Avenue, West Hollywood, California 90069

Phone Number: 310-474-9111 Fax Number: 310-474-8585

E-Mail Address: twolfson@ahdootwolfson.com

rev. 01/08 AK

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

I. JURISDICTIONAL STATEMENT

The district court has jurisdiction under 28 U.S.C. § 1332(d)(2) because the plaintiffs' class-action complaint alleges claims of plaintiffs and the other class members that exceeds $5,000,000, exclusive of interests and costs, and there are numerous class members who are citizens of states other than Defendant's state of citizenship. Plaintiff Hilary Remijas is an individual and a citizen of Illinois. Plaintiff Melissa Frank is an individual and a citizen of New York. Plaintiffs Debbie Farnoush and Joanne Kao are individuals and citizens of California. On information and belief, Defendant is a Delaware limited liability company with a single member, Neiman Marcus Group LTD LLC. On information and belief, Neiman Marcus Group LTD LLC is an LLC with a single member, Mariposa Intermediate Holdings LLC, which in turn is an LLC with a single member, NM Mariposa Intermediate Holding, Inc. On information and belief, NM Mariposa Intermediate Holdings, Inc., is a Delaware corporation with its principal place of business in Texas.[1] As such, Defendant is a citizen of Delaware and Texas.

On September 16, 2014, the district court issued a Memorandum Opinion and Order granting Defendant's Motion to Dismiss, itself filed April 2, 2014 (Dkt. 16), under Federal Rule of Civil

[1] Neiman Marcus Group LTD LLC's Quarterly Report indicates that NM Mariposa Intermediate Holdings, Inc., acts wholly through Neiman Marcus Group LTD LLC and its subsidiaries: "[Neiman Marcus Group LTD LLC] has elected to be treated as a corporation for U.S. federal income tax purposes and all operations of [NM Mariposa Intermediate Holdings, Inc] are conducted through [Neiman Marcus Group LTD LLC] and its subsidiaries . . . There are no differences between [Neiman Marcus Group LTD LLC's] and [NM Mariposa Intermediate Holdings, Inc's] current and deferred income taxes." Neiman Marcus Group LTD LLC, Quarterly Report (Form 10-Q) at 18 (June 6, 2014), *available at* http://phx.corporate-ir.net/phoenix.zhtml?c=118113&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk2NDk3MjAmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d. As such, the principal place of business of NM Mariposa Intermediate Holdings, Inc., is the same as the principal place of business of Neiman Marcus Group LTD LLC: Texas.

Procedure 12(b)(1). (Dkt. 49.)[2] Plaintiff's Notice of Appeal was timely filed on September 25, 2014. (Dkt. 50.)

Because the September 16, 2014 Order constitutes a final judgment, jurisdiction in the Court of Appeals for the Seventh Circuit is provided by 28 U.S.C. § 1291, which provides jurisdiction over appeals from all final decisions of district courts. *See also Kaplan v. Shure Bros.*, 153 F.3d 413, 417 (7th Cir. 1998) ("The fact that no judgment document appears in the record . . . does not deprive us of jurisdiction."); *Rothner v. City of Chicago*, 929 F.2d 297, 300 (7th Cir. 1991) (recognizing that "dismissal of the entire case" can support appellate jurisdiction). The District Court "terminated" the entire action upon entry of the order at issue. (Dkt. 48.)

II. STATEMENT OF THE ISSUES

This appeal raises the following issues:

1. Does the risk of future harm presented to consumers whose Private Information has been stolen from a retailer that employed deficient data security measures, by hackers who are misusing that Private Information, constitute a cognizable injury in fact giving such consumers Article III standing to pursue claims against the retailer under state data breach and unfair competition laws?

2. Can victims of data breaches have a cognizable injury in fact, and Article III standing, without pleading and proving that they suffered unreimbursed fraudulent charges on compromised payment cards, by virtue of other harms suffered and increased risks of such harms that result from data breaches affecting inadequate data security systems?

---

[2] Citations to "Dkt." refer to the District Court's docket entries in the case below, all of which are included in the record on appeal. Citations to "App." refer to the concurrently filed Appendix.

3. Do allegations that plaintiffs lost time and money resolving fraudulent charges and monitoring their credit as a result of Defendant's inadequate security and attendant data breach describe a cognizable injury in fact?

4. Do allegations that plaintiffs lost use of their credit or debit cards and thus access to their funds, for a period of time, as a result of Defendant's inadequate security and attendant data breach state a cognizable injury in fact?

5. Do allegations that Defendant failed to spend a portion of the money that Plaintiffs paid for defendant's goods on adequate security describe a cognizable injury in fact?

6. Does the loss of control over, and value of, consumers' Private Information in a data breach constitute a cognizable injury in fact?

7. Does violation of state laws giving affected consumers rights and claims following a data breach constitute a cognizable injury in fact?

III. STATEMENT OF THE CASE

A. Facts Relevant to Issues Raised on Appeal

Defendant is a luxury specialty department store. (Dkt. 27, First Amended Complaint ("FAC") ¶ 11.) Defendant advises its customers that it collects its customer's name, address, telephone number, mobile telephone number, driver's license number, birth date, and email address; and, if the customer uses a credit or debit card or pays by check, will also collect the customer's account number. ¶13. Defendant, thus, stores massive amounts of payment card data ("PCD") and other personally identifiable information ("PII" and, together with PCD, "Private Information") on its servers. (*Id.* ¶ 14.)

In 2013, hackers breached Defendant's servers and made off with at least 350,000 customers' unencrypted credit and debit card numbers, and other PII (the "Data Breach"). (*Id.* ¶¶ 28-40.) The hackers accomplished the Data Beach using malicious software (malware) installed on Defendant's

computer servers, which collected and then transmitted to the hackers, consumers' Private Information. Although Defendant contends that the Private Information was stolen between July 16 and October 30, 2013, Defendant concedes that the malware appeared on its Network as early as March 2013 and did not appear "contained and disabled" until January 10, 2014. (*Id.* ¶¶ 33, 40.)

During the Data Breach, the hackers' activities triggered 59,746 alerts indicating "suspicious behavior." (*Id.* ¶ 36.) However, Defendant's ability to automatically block the suspicious activity its Network flagged was inexplicably "turned off." (*Id.*) Plaintiffs also allege that Defendant negligently failed to properly segregate customers' PCD from PII, which allowed the hackers to access both. (*Id.* ¶ 39.)

Defendant claims it first learned about the Data Breach on December 13, 2013. (*Id.* ¶ 28.) And although plaintiffs dispute this fact, assuming it is true Defendant nevertheless waited until news of the Data Breach was published by a blogger on January 10, 2014, approximately 28 days later, before making any public statement regarding the Data Breach. (*Id.* ¶ 29.) Even then, Defendant delayed in formally notifying Plaintiffs and Class members of the Data Breach. (*Id.* ¶¶ 31-32.)

Plaintiffs Frank and Kao received undated notice letters from Defendant informing them that their PII was compromised in the data breach. (*Id.* ¶¶ 4, 6; Dkt. 40, Wolfson Decl. Exh. A.) Defendants failed completely to notify other Plaintiffs. (Dkt. 27, FAC ¶ 3.) Defendant stated that it "[wa]s notifying customers whose cards it ha[d] now determined were used fraudulently." (*Id.* ¶ 31.) It is therefore clear that these plaintiffs' information, at a minimum, was compromised in the data breach.

Had Defendant provided timely notice in mid-December, or earlier, Defendant would have experienced an extraordinary loss in revenue because the holiday-shopping season was well

underway in mid-December. Target provided notice of its data beach in mid-December 2013. As a result, "Target's profit was down 46 percent [in the fourth quarter] over the year before."[3] By delaying notification, Defendant, thus, avoided the drastic financial losses experienced at Target and effectively encouraged consumers like Plaintiffs and Class members to shop at Defendant's stores during the holiday season even though its security was defective.

Each Plaintiff suffered injuries. Plaintiff Remijas, an Illinois resident, used a credit card to purchase products at Defendant's stores on August 7 and December 21, 2014, but Defendant failed to provide Plaintiff Remijas with any notice of the Data Breach. (*Id.* ¶ 3.)

Plaintiff Frank, a New York resident, used her debit card to purchase products at Defendant's stores in New York in December 2013. (*Id.* ¶ 4.) Frank never suffered any type of fraud, identity theft or phishing before the Data Breach. (*Id.* ¶ 44.) On January 9, 2014, Frank was the victim of unauthorized fraudulent charges. (*Id.* ¶¶ 4, 45-46.) Frank was without the use of her card for approximately one day as a result of the fraud. (*Id.* ¶ 47.) In mid-March, Frank was the victim of a "phishing" incident. (*Id.* ¶¶ 4, 50-52.) In January, Defendant provided an undated letter purporting to notify Frank's husband, with whom Frank held a joint account, of the Data Breach. (*Id.* ¶¶ 4, 48.)

Plaintiff Farnoush, a California resident, used her credit card at Defendant's stores in California in 2013, and subsequently was the victim of unauthorized fraudulent charges. (*Id.* ¶ 5.)

Plaintiff Kao, a California resident, used her credit cards at Defendant's stores in California on numerous dates in San Francisco, California, from February through December, 2013. (*Id.* ¶ 5.) In January, Kao received an email from Chase Bank that her card had been compromised and that a new card would be issued. (*Id.* ¶ 54.) Kao was temporarily without the use of her card as a

---

[3] (Dkt. 39, Opp. to Mot. to Dismiss at n.2 (citing Elizabeth A. Harris, *Still Hurt by Data Breach and Losses in Canada, Target Lowers Forecast*, N.Y. TIMES, May 21, 2014, *available at* <http://www.nytimes.com/2014/05/22/business/after-more-weak-earnings-target-lowers-forecast.html?_r=0> (last visited Oct. 21, 2014).

consequence of the Data Breach. (*Id.* ¶ 55.) At some point in January, Defendant provided an undated letter purporting to notify Kao of the Data Breach. (*Id.* ¶¶ 6.)

B. Procedural History and Rulings Relevant to This Appeal

On March 12, 2014, Plaintiff-Appellant Hilary Remijas filed her original Complaint against The Neiman Marcus Group, LLC (Dkt. 1), containing claims for breach of implied contract and violations of the Illinois Consumer Fraud Act ("ICFA") and substantially similar laws of other consumer fraud states. Defendant-Appellee, The Neiman Marcus Group, LLC ("Defendant" or "Neiman Marcus"), filed a Motion to Dismiss Plaintiff's Complaint. (Dkt. 16.)

After that initial filing, Ms. Remijas's Counsel met and conferred with Plaintiff's counsel in other consumer class actions implicating the same data breach at Neiman Marcus in order to self-organize the cases for the sake of judicial economy and efficiency. These other matters included: *Frank v. Neiman Marcus Group* (Case No. 14-cv-00233-ADS-GRB), U.S. Dist. Court, E.D.N.Y.; *Chau v. Neiman Marcus Group, Ltd, Inc.* (Case No. 14-cv-597), U.S. Dist. Court, S.D. Cal.; and *Shields v. The Neiman Marcus Group, LLC* (Case No. 14-cv-752), U.S. Dist. Court, S.D. Cal. All Plaintiffs agreed to consolidate and proceed with their cases in the Northern District of Illinois, before the District Court below. Ms. Remijas moved for leave to amend the complaint in her action to include these additional plaintiffs and their claims (Dkt. 22), which the District Court granted on June 2, 2014 (Dkt. 26).

The named Plaintiffs then filed the FAC in this action on June 2, 2014. (Dkt. 27.) Plaintiffs are from Illinois, New York, and California, and bring claims under each state's consumer protection laws, on behalf of a putative class consisting of "[a]ll persons whose personal and/or financial information was disclosed in the data incursion affecting Neiman Marcus in 2013." (*Id.* at ¶ 70.)

Defendant filed a motion to dismiss the FAC under Rules 12(b)(1) and (b)(6) on July 2, 2014 (Dkt. 35), and Plaintiffs filed their opposition on July 30 (Dkt. 39). Without hearing oral argument,

the court granted Defendant's motion in the order appealed from on September 16, 2014 (Dkt. 49, App. 2), and the entire action was "terminated" (Dkt. 48, App. 1). In the September 16 Order at issue, the District Court held that Plaintiffs lacked Article III standing, and did not address Defendant's motion to dismiss for failure to state a claim. Plaintiffs filed their notice of appeal on September 25, 2014.

IV. SUMMARY OF ARGUMENT

In the order appealed from, the District Court wrongly dismissed the claims of *all* named Plaintiffs, including those who received notice that their Private Information was compromised in the Data Breach, those who suffered fraud and phishing incidents as a result, and those who temporarily lost access to their financial instruments as a result, because it concluded that other unidentified "customers" may not have Article III standing. (Dkt. 49, App. 2 at 6.) The court purported to follow the Article III standing requirements set out by the Supreme Court in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1146 (2013), which it appeared to construe as limiting if not overruling this Court's Article III analysis as set forth in *Pisciotta*. In reality, however, the District Court disregarded allegations by the Plaintiffs that satisfied any enunciation of Article III's injury-in-fact standing requirement, whether one adopts *Clapper*'s wording, that of the Supreme Court in the subsequent case of *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014), or that of this Court in *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007).

Under each and every one of the above case's enunciation of Article III's injury-in-fact standing requirement, which accord with one another, Plaintiff-Appellants' allegations suffice: The risk these consumers face is "clearly impending," *Clapper*, 134 S. Ct. at 1150 n.5; there is "a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," *id.* (quoted in *Susan B. Anthony List*, 134 S. Ct. at 2341); and

Defendant's alleged failure to implement proper security measures "harms the plaintiff[s] . . . by increasing the risk of future harm," *Pisciotta*, 499 F.3d at 634.

The District Court's requirement that consumers affected by a data breach show that they suffered unreimbursed charges in order to have standing lacks support in law or common sense. *See In re Adobe Sys.*, 2014 U.S. Dist. LEXIS at *28 ("[T]o require Plaintiffs to wait until they actually suffer identity theft or [unreimbursed] 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.") (quoting *Clapper*, 123 S. Ct. at 1150 n.5). The injuries at issue here are not conjectural; they are concrete, particularized, and supported by the facts. *See also In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL No. 11-md-2258, 2014 WL 223677, at *9 (S.D. Cal. Jan. 21, 2014) ("Plaintiffs have plausibly alleged a 'credible threat' of impending harm based on the disclosure of their Personal Information following the intrusion.").

The District Court misconstrued and misapplied Article III standing law so that it presents a virtual bar against claims arising out of data breaches, despite state laws specifically designed to give such plaintiffs claims — and standing to bring such claims — against businesses that mishandle consumers' Private Information and that fail to give prompt notices of data breaches to affected consumers. This Court should reverse the decision below.

V. STANDARD OF REVIEW

A motion to dismiss under Rule 12(b)(1) challenges the Court's subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). This Court "review[s] *de novo* a district court's dismissal for lack of subject matter jurisdiction." *Apex Digital, Inc. v. Sears, Roebuck & Co.*,572 F.3d 440, 443 (7th Cir. 2009).

The standard of review for a Rule 12(b)(1) motion to dismiss depends upon the purpose of the motion. *Apex Digital*, 572 F.3d at 443-44. In a facial challenge, where defendant challenges the sufficiency of the allegations regarding subject matter jurisdiction, the Court must accept all well-

pleaded factual allegations as true and draw all reasonable inferences in the plaintiff's favor. *See id*. In a factual challenge, where defendant submits competent evidence that controverts the truth of the jurisdictional allegations, the Court may look beyond the pleadings and view any competent proof submitted by the parties to determine if the plaintiff has established jurisdiction by a preponderance of the evidence. *Id.*

Defendant did not factually challenge Plaintiffs' standing. While Defendant submitted a declaration in support of its Motion (Dkt. 36-1) — which Plaintiffs challenged as inadmissible — the District Court did not refer to or rely on that Declaration in dismissing Plaintiffs' claims. Moreover, as Plaintiff-Appellants argued, Defendant never articulated what facts in the FAC it sought to controvert through that declaration. Accordingly, the Court must accept as true all of Plaintiff-Appellants well-pled allegations in the FAC.

VI. ARGUMENT

A. Article III's Injury-in-Fact Standing Requirement.

> Article III of the Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U. S. Const., Art. III, §2. The doctrine of standing gives meaning to these constitutional limits by "identify[ing] those disputes which are appropriately resolved through the judicial process." . . . To establish Article III standing, a plaintiff must show (1) an "injury in fact," (2) a sufficient "causal connection between the injury and the conduct complained of," and (3) a "likel[ihood]" that the injury "will be redressed by a favorable decision."

Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U. S. 555, 560-61 (1992).

"An injury sufficient to satisfy Article III must be concrete and particularized and actual or imminent, not conjectural or hypothetical." *Susan B. Anthony List*, 134 S. Ct. at 2341. "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.'" *Id.* (quoting *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 n.5 (2013)) (emphasis added).

This Court addressed the question of what these standards require of plaintiffs in data breach cases in *Pisciotta v. Old Nat'l Bancorp*, holding that Article III's "injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." 499 F.3d 629, 634 (7th Cir. 2007). Plaintiffs in that case sought to maintain a class action against a bank that "solicited personal information from applicants for banking services, but had failed to secure it adequately. As a result, a third-party computer 'hacker' was able to obtain access to the confidential information of tens of thousands of . . . users" of the bank's website. *Id.* at 631; *see also Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010) (following *Pisciotta* and holding that Starbucks employees whose PII was lost on a stolen computer had Article III standing to bring suit against their employer for negligence, although "they d[id] not allege that any [identity] theft ha[d] actually occurred.").

B. The Increased Risk of Future Harm Alleged in This Case Presents a Cognizable Injury in Fact

1. The District Court Misinterpreted *Clapper*

The District Court cited *Clapper* and wrongly conclude that "[a]llegations of future potential harm may suffice to establish Article III standing, but the future harm must be 'certainly impending.'" (Dkt. 49, App. 2 at 2-3 (quoting *Clapper*, 133 S.Ct. at 1147).) In so reasoning, the District Court ignored footnote 5 of the *Clapper* decision, which cannot be ignored given that the Supreme Court itself quoted and followed the language of this very footnote in *Susan B. Anthony List* to hold that petitioners in that case — advocacy organizations challenging a statute — had Article III standing, despite the fact that no complaint against either of the organizations was pending. 134 S. Ct. at 2341 (quoting *Clapper*, 133 S. Ct. at 1150 n.5); *see also In re Adobe Sys. Privacy Litig.*, No. 13-cv-05226-LHK, 2014 U.S. Dist. LEXIS 124126 at *24 (N.D. Cal. Sept. 4,

2014) (quoting and following footnote 5 of *Clapper* to hold that plaintiffs had standing in data breach case).

In footnote 5 of *Clapper*, the Supreme Court recognized that its "cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found 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." *Clapper*, 133 S. Ct. at 1150 n.5 (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, ——, 130 S. Ct. 2743, 2754-55 (2010)).

The *Clapper* Court went on to find that plaintiffs' allegations in that case fell short of the "'substantial risk' standard," to the extent that it "is distinct from the 'clearly impending' requirement." *Clapper*, 133 S. Ct. at 1150 n.5.

Clapper addressed a challenge to Section 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), by U.S.-based attorneys, human rights, labor, legal, and media organizations who alleged that their work required them to communicate with individuals outside the United States who were likely to be targets of surveillance under that Section. *Id*. at 1142, 1145. The *Clapper* Court focused on the fact that respondents in that case did not allege that any of their communications had actually been intercepted, or even that the government sought to target them directly. *Id*. at 1148. Rather, the respondents' argument rested on the "highly speculative fear" that:

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [Section 702]'s many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.

Id.

As Judge Koh recognized in *In re Adobe Sys.*:

> The [*Clapper*] Court observed that the first three steps of the chain depended on the independent choices of the Government and the Foreign Intelligence Surveillance Court, yet the respondents could only speculate as to what decision those third parties would take at each step. *Id*. at 1149-50 ("[W]e have been reluctant to endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment. . . ."). Moreover, respondents could not show with any certainty that their communications with the foreign persons allegedly under surveillance would be intercepted. *Id*. As a result, the overall chain of inferences was "too speculative" to constitute a cognizable injury. *Id*. at 1143.
>
> ***
>
> *Clapper* did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability. *Accord Sony*, 996 F. Supp. 2d 942, 2014 WL 223677, at *8-9 ("[T]he Supreme Court's decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent . . . ."). *Clapper* merely held that the Second Circuit had strayed from these well-established standing principles by accepting a too-speculative theory of future injury. *See* 133 S. Ct. at 1146 (characterizing the Second Circuit's view of standing as "novel"). In the absence of any indication in *Clapper* that the Supreme Court intended a wide reaching revision to existing standing doctrine, the Court is reluctant to conclude that *Clapper* represents the sea change that Adobe suggests. Moreover, *Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result. *Id*. at 1147.

In re Adobe Sys., 2014 U.S. Dist. LEXIS 124126 at *23-25.

The *In re Adobe Sys.* court recognized that *Clapper* does not foreclose claims by those whose PII has been lost or stolen, but who have not suffered actual monetary loss due to identity theft. Judge Koh reasoned that:

> Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," 133 S. Ct. at 1148, the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real. . . . [I]n contrast to *Clapper*, where there was no evidence that any of respondents' communications either had been or would be monitored . . . , here there is no need to speculate as to whether Plaintiffs' information has been stolen. . . .

> Neither is there any need to speculate as to whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so. . . . Some of the stolen data has already surfaced on the Internet, and other hackers have allegedly used it . . . . Given this, the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as "certainly impending." Indeed, the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused. However, to 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. *Clapper*, 133 S. Ct. at 1150 n.5.

In re Adobe Sys., 2014 U.S. Dist. LEXIS 124126 at *27; *see also Moyer v. Michaels Stores, Inc.*, No. 14-c-561, 2014 WL 3511500 at *6 (N.D. Ill. July 14, 2014) ("[T]he elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing."); *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL No. 11-md-2258, 2014 WL 223677 at *9 (S.D. Cal. Jan. 21, 2014) ("Plaintiffs have plausibly alleged a 'credible threat' of impending harm based on the disclosure of their Personal Information following the intrusion.").

2. The District Court Disregarded Allegations that Clearly Satisfy Article III's Injury-in-Fact Standing Requirement

a. All Members of the Class (at Least 350,000 By Defendant's Admission) Suffered Injury In Fact Because Their Private Information Actually Was Stolen

The putative Class on whose behalf Plaintiff-Appellants filed the FAC consists only of "persons whose personal and/or financial information was disclosed in the data incursion affecting Neiman Marcus in 2013." (Dkt. 27, FAC at ¶ 70.) Far from the "speculative" allegations of injury in *Clapper*, Plaintiff-Appellants here allege that their Private Information *already* has been stolen and, moreover, that harm *already* has occurred to affected customers as a result. As Plaintiff-Appellants allege, "[a]ccording to Defendant, 350,000 credit and debit cards swiped in 77 U.S. stores were affected by the Data Breach in 2013." (*Id.* at ¶ 41.) Plaintiff-Appellants allege at multiple points in the FAC that their information actually was stolen in the Data Breach, and several of them

actually received notices from Defendant confirming this fact. (*E.g.*, *id.* at ¶¶ 4, 6.)[4] The risk of injury to all class members, including those who have not yet suffered fraudulent charges or identity theft is even more "certainly impending" in light of the fact that at least 9,200 of the class members have already suffered fraudulent charges. (*Id.* at ¶ 42.)

Despite Plaintiff-Appellants' allegations that their Private Information and that of other Class members actually was stolen in the Data Breach, the District Court held that "the increased risk of future harm" present in this case could not satisfy Article III's requirements because: "Unlike the *Pisciotta* plaintiffs, the plaintiffs here do not allege that data belonging to all of the customers at issue were in fact stolen." (Dkt. 49, App. 2 at 2, 6.) Thus, the District Court appears to have dismissed all named Plaintiffs' claims — even claims of those Plaintiffs who have been told their information was compromised in the data breach and who have suffered fraudulent charges and/or phishing as a result — because other unidentified "customers" who are not members of the class may not have been affected by the Data Breach. (*Id.*) This is clear error.

Plaintiff-Appellants' allegations that their Private Information, and that of other Class members, actually was stolen in the Data Breach is enough, alone, to satisfy Article III's injury-in-

---

[4] Such facts not only set this case apart from *Clapper*, but distinguish district court authority that the court below followed in this case. The plaintiff in *Strautins* "failed even to plausibly allege that her PII was stolen and so she . . . failed to establish even the proposition that she [was] at an increased risk of identity theft as a result of the . . . data breach." *Strautins*, 2014 WL 960816 at *5 n.11. "Plainly, the data breach" at issue in *Strautins* "did *not* result in the compromise of data of all taxpayers filing South Carolina returns" (*id.* at *7), and the plaintiff's only allegation supporting any inference that her data was affected was that "she filed tax returns in South Carolina" (*id.* at *6).

Similarly, the plaintiffs in *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013), failed to set forth facts demonstrating with reasonable plausibility that their information had in fact been stolen. 2013 WL 4759588 at *9-10; *see also id.* at *12 ("[Plaintiffs] have not sufficiently alleged the information they are trying to protect was actually stolen. Because of this, the costs they incurred in attempting to minimize their risks due to the security breach do not qualify as actual harm and thereby do not confer standing."); *In re Adobe Sys.*, 2014 U.S. Dist. LEXIS 124126 at *31 (distinguishing *Strautins* and *Barnes & Noble* on the basis that, in those cases, "it was unclear if the plaintiffs' information had been taken at all").

fact requirement under cases such as *Susan B. Anthony List*, *Clapper*, *Pisciotta*, *Krottner*, *In re Adobe Sys.*, and *Sony*. *See Susan B. Anthony List*, 134 S. Ct. at 2341 (holding petitioners had standing to challenge statue despite the fact that no complaint against them was pending) (following *Clapper*, 133 S. Ct. at 1150 n.5); *Pisciotta*, 499 F.3d at 634 ("[T]he injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."); *Krottner*, 628 F.3d at 1142 (following *Pisciotta* to hold that Starbucks employees whose PII was lost on a stolen computer had Article III standing to bring suit against their employer for negligence, although "they d[id] not allege that any [identity] theft ha[d] actually occurred"); *In re Adobe Sys.*, 2014 U.S. Dist. LEXIS 124126 at *27 (holding plaintiffs had Article III standing where their information was stolen in data breach); *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 2014 WL 223677 at *9 (same).

b. Plaintiffs' Allegations Establish that the Theft of Their Private Information Already Has Resulted in Cognizable Injury

Not only do Plaintiff-Appellants allege that their Private Information and that of all Class members actually was stolen in the Data Breach, but their allegations go further and establish that this theft of Private Information has already resulted in real and palpable harm to members of the Class, including the unauthorized use of Plaintiffs Frank's, Farnoush's, and at least 9,200 other Class members' payment cards. (Dkt. 27, FAC ¶¶ 4-5, 42.) That some Plaintiffs and Class members already have been the victims of fraudulent charges makes future harm substantially more likely both for them and for the rest of the putative class. Defendant's admission that at least 9,200 payment cards used at its stores have suffered fraud confirms not only that the Plaintiffs' and Class members' data was, *in fact*, taken during the Data Breach, but also demonstrates that the data was *actually* misused.

Ultimately, the District Court dismissed the claims of Plaintiff-Appellants Frank, Farnoush, at least 9,200 other customers whose cards Defendant admits were used fraudulently, and the entire class consisting of customers whose Private Information was compromised in the Data Breach because, without relying on any actual allegation in the FAC, the court somehow concluded that the "majority of the plaintiffs allege only that their data *may* have been stolen." (Dkt. 49, App. 2 at 5.) The Court dismissed Plaintiff-Appellants' allegations concerning the 9,200 cards already used fraudulently, including those of Frank and Farnoush, on the basis that "Plaintiffs have not alleged that any of the fraudulent charges were unreimbursed." (Dkt. 49, App. 2 at 6.)

The District Court did not cite any authority for its requirement that plaintiffs in such cases allege unreimbursed fraudulent charges in order to have standing, and this requirement flies in the face of established precedent: "[T]o require Plaintiffs to wait until they actually suffer identity theft or [unreimbursed] credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or by 'literally certain' in order to constitute injury-in-fact." *In re Adobe Sys.*, 2014 U.S. Dist. LEXIS at *28 (quoting *Clapper*, 123 S. Ct. at 1150 n.5).

The theft of Private Information caused by the Data Breach and Defendant's inadequate security can result in myriad injuries to consumers other than unreimbursed, fraudulent charges on a payment card. In addition to the injuries Plaintiff-Appellants alleged they suffered, which included phishing incidents and time and money spent resolving fraudulent charges, waiting for replacement cards, and monitoring their credit, the FAC describes myriad additional injuries that can befall such consumers. (*E.g.*, Dkt. 27, FAC at ¶¶ 60-65.) There is no principled basis for requiring Plaintiffs to allege and prove the existence of unreimbursed fraudulent charges to their payment cards. The injuries at issue here are not conjectural; they are concrete, particularized, and supported by the facts.

See also In re: Sony Gaming Networks & Customer Data Sec. Breach Litig., 2014 WL 223677 at *9 ("Plaintiffs have plausibly alleged a 'credible threat' of impending harm based on the disclosure of their Personal Information following the intrusion.").

C. Plaintiffs Have Standing Based on the Loss of Time and Money Associated with Resolving Fraudulent Charges, Loss Of The Use Of Their Cards And Access To Funds, and Monitoring Their Credit and Finances for Additional Fraud

Plaintiff-Appellants allege that the loss of time and money spent to resolve fraudulent charges, to obtain replacement cards, and to monitor their accounts for additional fraud constitutes actual injury. (*E.g.*, Dkt. 27, FAC at ¶ 89.) Plaintiffs further allege they spent money and/or time on credit monitoring (*id.* at ¶ 104), and could not use their cards while new ones were being issued and fraudulent charges were being addressed (*id.* at ¶¶ 47, 55, 90).

The District Court relied on the same misguided reasoning by which it dismissed standing due to an increased risk of future harm (discussed above) to dismiss these allegations of actual harm as well, reasoning: "The cost of guarding against a risk is an injury sufficient to confer standing only if the underlying harm the plaintiff is seeking to avoid is itself a cognizable Article III injury." (Dkt. 49, App. 2 at 7.)

Thus, the District Court parlayed its prior reasoning that, essentially, there can be no standing based on risk of future harm in a data breach case unless plaintiffs can allege the existence of unreimbursed fraudulent charges on affected payment cards, to conclude that time and money reasonably spent by affected consumers to protect themselves against the very real threat of identity theft caused by Defendant's negligence cannot convey standing. Because, as discussed above, the District Court was wrong to conclude that the risk of future injury here, alone, is insufficient to give Plaintiff-Appellants standing, it also was wrong to rely on that same reasoning to conclude that

Plaintiff-Appellants lack standing based on the loss of time and money they reasonably spent to mitigate the risks of future identity theft and fraud.

D. The District Court Wrongly Dismissed Plaintiffs' Allegations that Defendant Failed to Spend a Portion of the Money Plaintiffs Paid for Defendant's Goods on Adequate Security

A quintessential injury-in-fact occurs where, as here, Plaintiffs spent money that, absent defendant's actions, they would not have spent. *In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) ("The plaintiffs' loss is financial: they paid more for the toys than they would have, had they known of the risks the beads posed to children. A financial injury creates standing"); *see also Maya v. Centex Corp.*, 658 F.3d 1060, 1069 (9th Cir. 2011) ("quintessential injury-in-fact" occurs when "plaintiffs spent money that, absent defendants' actions, they would not have spent"). Additionally, if plaintiffs "state that they would not have purchased [a product] had there been proper disclosure," they sufficiently plead causation. *Id.* at 1070.

Aqua Dots is dispositive here. In *Aqua Dots*, plaintiffs sued the manufacturer and distributors of a children's toy consisting of beads containing a chemical that, when swallowed, could cause severe illness and even death. 654 F.3d at 749. Plaintiffs were the parents of children who had suffered no physical injury. *Id.* at 750. The Seventh Circuit held that these plaintiffs had Article III standing, explaining: "[The fact] that members of the class did not suffer physical injury . . . does not mean that they were uninjured. The plaintiffs' loss is financial: they paid more for the toys than they would have, had they known of the risks the beads posed to children. A financial injury creates standing." *Id.* at 751.

Similarly, in *Chicago Faucet Shoppe, Inc. v. Nestle Waters N. Am. Inc.*, Judge Tharp held that "[t]he plaintiff was injured because it would not have purchased the Ice Mountain five-gallon bottled water had it known that it was municipal tap water instead of 100% natural spring water." 12

C 08119, 2014 WL 541644, *3 (N.D. Ill. Feb. 11, 2014). Judge Tharp explained that "the injury, which was financial in nature, was complete at the time of purchase, because—as a result of Nestlé Waters' deceptive conduct—Chicago Faucet allegedly paid more than it otherwise would have for the water." *Id.* And in *Muir v. Playtex Products, LLC*, Judge Feinerman held that a plaintiff had Article III standing to sue the manufacturer of a diaper disposal product for false claims on the product's packaging under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), where plaintiff alleged that if he had known that "Proven #1 in Odor Control" claim on packaging was false, he would not have purchased the product and certainly would not have paid a premium price. 983 F. Supp. 2d 980, 986-87 (N.D. Ill. 2013).

The same result obtains here. Plaintiffs allege they made purchases at Defendant with their credit and/or debit cards that they would not have made had they known that Defendant does not take all necessary precautions to secure their personal and financial data. (Dkt. 27, FAC ¶ 15-16; *see also id.* at ¶¶ 69, 89.) Plaintiffs further allege that Defendant's products are sold at a premium because a portion of the purchase price is allocable to Defendant's cost of providing security for Plaintiffs' and Class member's Private Information. (*Id.* at ¶ 16.) Taking these allegations as true and construing them in the light most favorable to Plaintiffs, Plaintiffs have adequately alleged a "financial injury that creates standing." *Aqua Dots*, 654 F.3d at 751.

Nothing about Plaintiffs' financial injury is speculative. Indeed, numerous courts in this Circuit and elsewhere conclude that the price differential between what a plaintiff paid and what the plaintiff received constitutes a concrete injury-in-fact. *Aqua Dots*, 654 F.3d at 751; *Chicago Faucet Shoppe*, 2014 WL 541644, *3; *Muir*, 983 F. Supp. 2d at 986-87; *see also Bridenbaugh v. Freeman–Wilson*, 227 F.3d 848, 849–50 (7th Cir. 2000) (holding plaintiffs seeking to invalidate a state statute had standing where they alleged that the statute resulted in their payment of a premium price for a

certain wine, and noting that "this difference in price is [a] source of injury"); *Lipton v. Chattem, Inc.*, 2012 WL 1192083, at *3–4 (N.D. Ill. Apr. 10, 2012) (same where the plaintiff alleged that the weight loss drug she bought was worth less than what she paid because it contained a dangerous ingredient and that she would not have purchased the product had she known that the drug contained that ingredient); *Askin v. Quaker Oats Co.*, 818 F. Supp. 2d 1081, 1084 (N.D. Ill. 2011) (same where the plaintiff alleged that she paid a premium price for a food product based on the defendant manufacturer's false representations that the product did not contain unhealthy trans fats, and noting that this "price differential represents a concrete injury-in-fact").

The District Court summarily dismissed Plaintiff-Appellants' argument that they have standing through the loss of money they incurred when they purchased products from Defendant, while Defendant failed to pay for adequate security, as "creative, but unpersuasive." (Dkt. 49, App. 2 at 8.) The District Court then read into Plaintiffs' cited authority, including *Aqua Dots* and *Chicago Faucet Shoppe*, its own "creative" and entirely new "vital limited principle to this theory of injury," requiring "that the value-reducing deficiency . . . alway [be] intrinsic to the product at issue." (*Id.*)[5]

[5] Like the District Court below, the *Barnes & Noble* court also refused to find standing where plaintiffs asserted they overpaid for products and services purchased from Barnes & Noble, because they were paying for the security measures Barnes & Noble was supposed to employ to protect credit and debit transactions. 2013 WL 4759588, at *5. The plaintiffs alleged that Barnes & Noble's failure to employ those security measures diminished the value of Plaintiffs' purchased products and services. *Id.* Without engaging in any meaningful analysis or any discussion of *Aqua Dots*, 654 F.3d at 751, and the other authorities cited above, the *Barnes & Noble* court concluded that plaintiffs' argument was "not persuasive, particularly as Plaintiffs have not pled that Barnes & Noble charged a higher price for goods whether a customer pays with credit, and therefore, that additional value is expected in the use of a credit card." *Id.*

The costs incurred by any retailer for implementation of security measures are passed along to *all* consumers in the form of higher prices for products.[6] That those costs may be passed along *equally* to consumers paying with a card and to consumers paying with cash does not ameliorate the card-paying consumers' right to claim that they did not receive bargained-for security measures, the cost of which is included in the price they paid for the products. Retailers also pass along the costs of providing electric lighting to consumers in the form of the price paid for products and services. That proposition is no less true because retailers do not charge a higher price to sighted people who use electric lighting than to blind people who do not require electric lighting.

Simply put, Plaintiffs adequately allege monetary harm, particularly given that questions regarding the measure of damages are fact-intensive and should not be determined on a motion to dismiss. *See, e.g.*, *Smith v. Aon Corp.*, No. 04 C 6875, 2006 WL 1006052 (N.D. Ill. Apr. 12, 2006) ("The court, however, will not engage in a fact-based analysis of the amount of damages at the motion to dismiss stage"); *Pietrangelo v. NUI Corp.*, CIV. 04-3223 (GEB), 2005 WL 1703200, 4

---

[6] As Plaintiff-Appellants argued below, That retailers pass overhead costs on to consumers in the form of higher prices is so "generally known" throughout the United States that it is subject to judicial notice. Fed. R. Evid. 201(b)(1); *see also In the Matter of Peacock Buick, Inc., et al.*, 86 F.T.C. 1532 (1975) ("components of overhead are included in the quoted price."). That is true with respect to aviation fuel costs. *Nw. Airlines, Inc. v. Cnty. of Kent, Mich.*, 510 U.S. 355, 376, 114 S. Ct. 855, 867, 127 L. Ed. 2d 183 (1994) ("Any cost an airline bears is in some sense an "indirect" charge "on persons traveling in air commerce," because the airline ultimately will pass that cost on to consumers in the form of higher ticket"). That is true with respect to postage costs. *Hotaling v. Chubb Sovereign Life Ins. Co.*, 241 F.3d 572, 581 (7th Cir. 2001) ("This would inevitably increase costs which, *as we all know*, would be passed on to the consumer in the form of higher premiums.") (emphasis added). That is true with respect to advertising costs. *Magid Mfg. Co., Inc. v. U.S.D. Corp.*, 654 F. Supp. 325, 327 (N.D. Ill. 1987) ("this extra cost is generally passed on to the consumer in the form of a higher price for that product."). That also is true with respect to security costs related to data incursions. *See* "Identity theft growing, costly to victims," http://www.usatoday.com/story/money/personalfinance /2013/04/14/identity-theft-growing/2082179 (last visited on July 31, 2014) ("The costs [incurred to respond to security breaches] are passed on to consumers in the form of higher retail prices . . . ."). Plaintiffs allege that the costs of Defendant's security is embedded in the purchase price of all products sold by Defendant. (FAC ¶¶ 15-16.) Those allegations must be accepted as true on a motion to dismiss.

(D.N.J. July 20, 2005) ("allegations that the Plan suffered damages as a result of Defendants' breaches are sufficient" at motion to dismiss stage); *Muller v. M.D. Sass Assocs., Inc.*, No. Civ.A. 91-3762, 1992 WL 80938, at *8 (D.N.J. Apr. 22, 1992) ("discussion of the measure of damages is somewhat premature when considering a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6)").[7]

E. Plaintiffs Have Standing Based on the Loss of Control Over, and Loss in Value of, Their Private Information

Plaintiffs allege that the loss of control over their Private Information constitutes actual injury. (*E.g.*, FAC ¶ 89.) In *In re Facebook Privacy Litig.*, the Ninth Circuit recently held that plaintiffs' allegations that "they were harmed both by the dissemination of their personal information and by losing the sales value of that information" are "sufficient to show the element of damages for their breach of contract and fraud claims." 12-15619, 2014 WL 1815489 (9th Cir. May 8, 2014); *see also Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011) ("the breach of his PII has caused him to lose some ascertainable but unidentified 'value' and/or property right inherent in the PII"); *accord State v. Mayze*, 622 S.E. 2d 836, 841 (Ga. 2005) ("identity fraud is an offense against the victim's possessory interest in his or her personal information," and PII is an intangible commodity). Defendant's failure to safeguard and protect Plaintiffs' Private Information, thereby allowing this right to be taken from Plaintiffs without their authorization, constitutes injury-in-fact and supports Article III standing.

---

[7] Courts have found standing where a defendant charges money for a good or service but fails to honor its own policies in connection with providing the good or service. *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011) ("[A] plaintiff who is a consumer of certain services (i.e., who 'paid fees' for those services) may state [a claim requiring monetary loss] when a company, in violation of its own policies, discloses personal information about its customers to the public."). The *Sony* court noted that economic injury can occur both when a plaintiff gives more or acquires less in a transaction than he or she otherwise would have. *Sony*, 2012 WL 4849054 at *15; *see also Resnick v. AvMed*, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012) (economic injury stemming from the failure to implement security policies, for which plaintiffs allegedly paid as a part of their monthly premiums).

The District Court did not really explain its reasoning in declining to find that Plaintiff-Appellants' loss of control over their Private Information constitutes a cognizable injury. Instead, the District Court simply stated it was "unpersuaded" by this argument, and that "[a]gain, the injury as pled is not sufficiently concrete." (Dkt. 49, App. 2 at 9.) The District Court cited *Barnes & Noble*, but failed to acknowledge that, in that case, plaintiffs failed to set forth facts demonstrating that their information had in fact been stolen. *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588 at *9-10 (N.D. Ill. Sept. 3, 2013). *Barnes & Noble* thus is not persuasive, and Plaintiff-Appellants loss of control over their Private Information should constitute a cognizable injury in fact here.

F. The District Court Failed to Recognize that Plaintiff-Appellants Suffered Injury by Virtue of Defendant's Violation of State Laws

As the Supreme Court recognized in *Warth v. Seldin*, 422 U.S. 490, 500 (1975), "the actual or threatened injury required by [Article III] may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . . ." The Supreme Court has applied this principle to hold that "a plaintiff suffers an 'injury in fact' when the plaintiff fails to obtain information which must be publicly disclosed pursuant to a statute." *Fed. Election Com'n v. Akins*, 524 U.S. 11, 21 (1998) (citing *Pub. Citizen v. Dep't of Justice*, 491 U.S. 440, 449 (1989) (failure to disclose information pursuant to Federal Advisory Committee Act "constitutes sufficiently distinct injury to provide standing to sue"); *see also Havens Realty Corp. v. Coleman*, 455 U.S. 363, 374 (1982) (injury in fact when information required under the Fair Housing Act was withheld); *Sargeant v. Dixon*, 130 F.3d 1067, 1070 (D.C. Cir. 1997) ("The receipt of information is a tangible benefit the denial of which constitutes an injury.").

1. The California Plaintiffs Have Standing to Pursue Their Claims Under, and the District Court's Reasoning Eviscerates, the California Customer Records Act (Count VI)

Along with all their other claims, the District Court dismissed Plaintiffs' sixth cause of action, brought by the California Plaintiffs for violation of the California Customer Records Act, § 1798.80, *et seq*. (the "CRA"). Section 1798.84(b) of the CRA provides that customers injured by a violation of *any* provision of the CRA may institute a civil action. *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 467 (2013). Here, Plaintiffs allege they were injured by Defendant's violations of three such provisions: § 1798.81.5(b) (failure to implement reasonable security measures); § 1798.82(a) (failure to timely notify customers of a breach), and § 1798.82(d) (failure to include all required information on notice of a breach). (Dkt. 27, FAC ¶¶ 5, 6, 138(a), 139, 142, 143.)

Plaintiffs allege a cognizable injury, and have statutory standing, because they allege they were deprived of disclosures they are statutorily entitled to receive under Section 1798.82(d)(2). *See, e.g., Akins*, 524 U.S. at 21. Defendant's Notice is also undated and, thus, the notice is defective on its face. (Dkt. 40, Wolfson Decl. Exh. A.) The District Court should have denied the Motion to Dismiss on this basis alone. *See also Sony*, 2014 WL 223677 at *53 (denying motion to dismiss, reasoning that "Plaintiffs may pursue their injunctive relief claims under § 1798.84(e), which affords relief when a 'business violates, proposes to violate, or has violated' the [CRA].'").

2. Plaintiff Remijas Has Standing to Pursue Her Claim Under the Illinois Personal Information Protection Act (Count VI)

Likewise, the District Court dismissed Plaintiff Remijas's claim for violation of the Illinois Personal Information Protection Act, 815 ICLS 530/1 *et seq.* ("PIPA"), on the same standing grounds. The PIPA requires, *inter alia*, that a "data collector that owns or licenses personal information concerning an Illinois resident *shall notify* the resident at no charge that there has been a

breach of the security of the system data following discovery or notification of the breach." 815 ICLS 530/10(a). Plaintiff Remijas alleges that she made purchases using a credit card at Defendant's stores during the period of the Data Breach, and that Defendant failed to provide her with *any* notice about the Data Breach. (Dkt. 27, FAC ¶ 3.)

Like the California Plaintiffs, Plaintiff Remijas adequately alleges injury as a result of Defendant's violation of the PIPA's mandate to provide Notice. *See, e.g., Warth*, 422 U.S. at 500; *Akins*, 524 U.S. at 21 (failure to disclose information required under statute "constitutes sufficiently distinct injury to provide standing to sue").

VII. CONCLUSION

For all the reasons set forth above, this Court should reverse the District Court's Orders dismissing this case for lack of subject matter jurisdiction (App. 1-2), and remand for further proceedings.

DATED: November 5, 2014

Respectfully submitted,

/s/ Joseph J. Siprut

Joseph J. Siprut
SIPRUT PC
17 North State Street
Suite 1600
Chicago, Illinois 60602
Tel: 312-236-0000
Fax: 312-267-1906

Tina Wolfson
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, California 90069
Tel: 310-474-9111
Fax: 310-474-8585

Attorneys for Plaintiffs-Appellants

Statement Regarding Oral Argument

In accordance with Fed. R. App. P. 34(a)(1) and Circuit Rule 34(f), Plaintiff-Appellants request that the Court hear oral argument in this case because it presents significant issues concerning the ability of consumers who are injured by data breaches to bring claims against those who allow such data breaches to occur through negligence or other illegal conduct.

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATIONS, TYPEFACE REQUIREMENTS
AND TYPE STYLE REQUIREMENTS

This brief complies with the length limitations Fed. R. App. P. 32(a)(7) because it is under 30 pages and with the type-volume limitations of Rule 32(a)(7)(B) because it contains 9,377 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Circuit Rule 32, Fed. R. App. P. 32(a)(5), and Fed. R. App. P. 32(a)(6), because its has been prepared using a proportionally spaced typeface using Microsoft Word for Mac 2011 with 12-point Times New Roman font.

DATED: November 5, 2014

s/ Joseph J. Siprut
Joseph J. Siprut
Attorney for Plaintiffs-Appellants

CERTIFICATE OF SERVICE

I hereby certify that on November 5, 2014 the Brief of Plaintiffs-Appellants Hilary Remijas, Melissa Frank, Debbie Farnoush and Joanne Kao was filed with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the appellate CM/ECF system.

The following participants in the case are registered CM/ECF users and will be served by the appellate CM/ECF system:

Daniel Craig
Tracy Fletcher Flint
David H. Hoffman
SIDLEY AUSTIN LLP
One S. Dearborn Street
Chicago, IL 60603

s/ Joseph J. Siprut
Joseph J. Siprut

APPENDIX

Statement of Compliance
With Circuit Rule 30(d)

All materials required by Cir. R. 30(a) & (b) are included in the Appendix of Plaintiffs-Appellants Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao.

/s/ Joseph J. Siprut
Joseph J. Siprut
jsiprut@siprut.com
SIPRUT PC
17 North State Street, Suite 1600
Chicago, Illinois 60602
Tel: 312-236-0000
Fax: 312-267-1906

Attorney for Plaintiffs-Appellants

APPENDIX
TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
FOR THE Northern District of Illinois − CM/ECF LIVE, Ver 6,1
Eastern Division

Hilary Remijas, et al.

Plaintiff,

v.

Case No.: 1:14−cv−01735
Honorable James B. Zagel

The Neiman Marcus Group, LLC

Defendant.

NOTIFICATION OF DOCKET ENTRY

This docket entry was made by the Clerk on Tuesday, September 16, 2014:

MINUTE entry before the Honorable James B. Zagel: In accordance with the Court's Memorandum Opinion and Order, Defendant's Motion to Dismiss is granted for lack of standing. Enter Memorandum Opinion and Order. Civil case terminated. Mailed notice(ep,)

ATTENTION: This notice is being sent pursuant to Rule 77(d) of the Federal Rules of Civil Procedure or Rule 49(c) of the Federal Rules of Criminal Procedure. It was generated by CM/ECF, the automated docketing system used to maintain the civil and criminal dockets of this District. If a minute order or other document is enclosed, please refer to it for additional information.

For scheduled events, motion practices, recent opinions and other information, visit our web site at ***www.ilnd.uscourts.gov***.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HILARY REMIJAS, MELISSA FRANK, DEBBIE FARNOUSH, and JOANNE KAO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company,

Defendant.

No. 14 C 1735
Judge James B. Zagel

MEMORANDUM OPINION AND ORDER

Plaintiffs Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao, individually and on behalf of all others similarly situated, have brought this action against Defendant Neiman Marcus for negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of several state data breach acts. Defendant now moves to dismiss pursuant to Fed.R.Civ.P. 12(b)(1) for lack of Article III standing, and pursuant to Fed.R.Civ.P. 12(b)(6) for failure to state a claim. For the following reasons, Defendant's motion to dismiss is granted for lack of standing.

BACKGROUND

Defendant is a high-end department store. In 2013, hackers breached Defendant's servers, resulting in the potential disclosure of 350,000 customers' payment card data and personally identifiable information. At some point following the breach, it became clear that, of the payment cards that may have been affected, at least 9,200 were subsequently used fraudulently elsewhere. Plaintiffs are among the 350,000 customers, and they have brought this

lawsuit against Defendant for failing to adequately protect against such a security breach, and for failing to provide timely notice of the breach once it happened.

Plaintiffs assert that they have been injured in that Defendant's alleged misconduct exposed them to an increased risk of future fraudulent credit card charges, and an increased risk of identity theft. Plaintiffs also assert present injuries, including the loss of time and money associated with resolving fraudulent charges, the loss of time and money associated with protecting against the risk of future identity theft, the financial loss they suffered from having purchased products that they wouldn't have purchased had they known of Defendant's misconduct, and the loss of control over and value of their private information. Defendant argues that none of these asserted injuries is sufficient to establish Article III standing.

DISCUSSION

It is a plaintiff's burden to establish Article III standing. *Apex Digital, Inc. v. Sears, Roebuck, & Co.*, 572 F.3d 440, 443 (7th Cir. 2009). This requires the plaintiff to demonstrate: (1) an "injury in fact" that is concrete and particularized and either actual or imminent; (2) that the injury is fairly traceable to the challenged action by the defendant; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013). Because standing is not a mere pleading requirement, but rather an indispensable part of the plaintiff's case, it must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation. *Apex Digital*, 572 F.3d at 443. Plaintiffs assert four principal categories of injury. I address each in turn.

A. The Increased Risk of Future Harm

Allegations of future potential harm may suffice to establish Article III standing, but the

future harm must be "certainly impending." *See Clapper*, 133 S.Ct. at 1147 (collecting cases). Three courts in this District have recently taken up the question of standing and the increased risk of future harm plaintiffs encounter in the context of such cyber-attacks. *See Moyer v. Michaels Stores, Inc.*, 2014 WL 3511500 (N.D.Ill. July 14, 2014); *Strautins v. Trustwave Holdings, Inc.*, 2014 WL 960816 (N.D.Ill. March 12, 2014); *In re Barnes & Noble Pin Pad Litigation*, 2013 WL 4759588 (N.D.Ill. Sept. 3, 2013).

The courts in *Strautins* and *Barnes & Noble* both held that the alleged increased risk of future harm was insufficient to establish standing. Defendant argues that this case is like *Strautins* and *Barnes & Noble*. In *Moyer*, the Court held that the alleged increased risk of future harm was sufficient to establish standing, but Defendant contends that this holding was premised on a misreading of relevant case law, and it should not be followed. The differing outcomes in *Strautins* and *Barnes & Noble* on the one hand, and *Moyer* on the other are in part attributable to conflicting readings of the Supreme Court's recent decision in *Clapper*.

The *Strautins* Court concluded that *Clapper* implicitly overruled a facially more relaxed standard for evaluating standing in this context articulated in *Pisciotta v. Old Nat. Bancorp*, 499 F.2d 629, 634 (7th Cir. 2007). In *Pisciotta*, the Court held that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Id*. The *Strautins* Court held that, by emphasizing the "certainly impending" standard, the Supreme Court "seems rather plainly to reject the premise, implicit in *Pisciotta* [ ], that any marginal increase in risk is sufficient to confer standing." *Strautins*, 2014 WL 960816, at *5. The *Barnes & Noble* Court relied on *Clapper*'s "certainly impending" analysis without reference to *Pisciotta*.

The *Moyer* Court, by contrast, understood *Clapper* to have applied a particularly rigorous standing analysis to a claim that particularly called for it – a claim that implicated the actions of the political branches of government in the fields of intelligence gathering and foreign affairs, and that argued that an action taken by one of the other two branches of the federal government was unconstitutional. *See Moyer*, 2014 WL 3511500, at *5; *see also Strautins*, 2014 WL 960816, at *5 n. 11. These cyber-attack/credit card cases implicate neither questions of national security nor the constitution. The *Moyer* Court concluded that there was room for *Clapper* and *Pisciotta* to co-exist. *See Moyer*, 2014 WL 3511500, at *6.

For my part, I note that the "certainly impending" standard pre-dates *Clapper*, *see Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979), though I also note that the *Clapper* Court itself acknowledged that the underlying facts called for an "especially rigorous" standing inquiry, *see Clapper*, 133 S.Ct. at 1147. Those facts are not present here. Read literally, *Pisciotta* could be understood to have held that *any* marginal increase in the risk of future injury is sufficient to confer Article III standing. That would be difficult to square with *Clapper*, which sets a threshold that an increase in the risk of harm must meet in order to confer standing. *Id*. But in my view, it is hard to imagine that that is what the *Pisciotta* Court intended, and such a literal reading of *Pisciotta* would not be reasonable. The *Pisciotta* Court raised the issue of standing *sua sponte*, and was not prompted to thoroughly discuss it. Though it does not expressly say so, *Pisciotta* was constrained by the "certainly impending" standard, first articulated 27 years earlier in *Babbit*, and I read that standard into the opinion.

Legal standards aside, the underlying facts in *Pisciotta*, *Strautins*, *Barnes & Noble*, and the instant case materially differ with respect to standing. First, in *Pisciotta*, it appears as though the plaintiffs' data were actually stolen (at the very least, the Court's analysis assumed as much).

See Pisciotta, 499 F.3d at 634. At issue with respect to the plaintiffs' injury, then, was whether and how likely the stolen data would actually be misused. *Id*. This is distinct from *Strautins* and *Barnes & Noble*, where the respective Courts found that the plaintiffs had alleged merely that there was a *possibility* that their data had been stolen. *See Strautins*, 2014 WL 960816, at *4, *6; *Barnes & Noble*, 2013 WL 4759588, at *4. Compared to the facts in *Pisciotta*, the fact that any given plaintiff's data may not have even been stolen yielded a much weaker inference that the data were actually at a sufficiently increased risk of being misused. In my view, this is a principled distinction that could justify holding that *Pisciotta* satisfied the "certainly impending" standard (albeit under a less rigorous application of the standard outside the national security/constitutional context) while holding that *Strautins* and *Barnes & Noble* did not.

The facts in the instant case present a third permutation. Here, the overwhelming majority of the plaintiffs allege only that their data *may* have been stolen. In this sense, the instant case is like *Strautins* and *Barnes & Noble*. Unlike *Strautins* and *Barnes & Noble*, however, Plaintiffs also allege (and Defendant acknowledges) that 9,200, or approximately 2.5% of these customers have actually had fraudulent charges appear on their credit cards. In other words, these customers' data were actually stolen and were actually misused. This allegation permits several inferences of varying strength with respect to Plaintiffs' claims to standing.

First, it certainly permits the inference that these 9,200 customers did indeed have their data stolen as a result of the cyber-attack on Defendant. That is an injury in fact, the sufficiency of which for purposes of standing will be addressed below. Second, it permits a weaker, though in my view still plausible, inference that others among the 350,000 customers are at a "certainly impending" risk of seeing similar fraudulent charges appear on their credit cards as a result of the cyber-attack on Defendant. The significance of that potential future injury for purposes of

standing will also be discussed below. I do not believe, however, that this allegation permits a plausible inference that any of the 350,000 customers are at a "certainly impending" risk of the other future injury claimed by Plaintiffs – identity theft.

It is not clear to me that the "fraudulent charge" injury alleged to have been incurred by the 9,200 customers, or, *a fortiori*, the risk that the same injury may befall others among the 350,000 customers at issue, is an injury sufficient to confer standing. To satisfy their burden to establish standing, plaintiffs must show that their injury is concrete, particularized, and, if not actual, at least imminent. *See Clapper*, 133 S.Ct. at 1147. As discussed above, I am satisfied that the potential future fraudulent charges are sufficiently "imminent" for purposes of standing. But of course, even having conceded imminence, both injuries (present and future) must still be concrete. Here, as common experience might lead one to expect, Plaintiffs have not alleged that any of the fraudulent charges were unreimbursed. On these pleadings, I am not persuaded that unauthorized credit card charges for which none of the plaintiffs are financially responsible qualify as "concrete" injuries. *See Barnes & Noble*, 2013 WL 4759588, at *6; *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, *8 (S.D.N.Y. June 25, 2010). Without a more detailed description of some fairly substantial attendant hardship, I cannot agree with Plaintiffs that such "injuries" confer Article III standing.

Next, as noted above, I am not persuaded that the 350,000 customers at issue are at a certainly impending risk of identity theft. Unlike the *Pisciotta* plaintiffs, the plaintiffs here do not allege that data belonging to all of the customers at issue were in fact stolen. They allege that approximately 2.5% of the customers at issue saw fraudulent charges on their credit cards, supporting a strong inference that *those* customers' data were stolen as a result of Defendant's data breach. And again, I accept the inference from this that additional customers are at a

"certainly impending" risk of future fraudulent charges on their credit cards. But to assert on this basis that either set of customers is also at a certainly impending risk of identity theft is, in my view, a leap too far.[1] The complaint does not adequately allege standing on the basis of increased risk of future identity theft.

B. Time and Money Spent to Mitigate the Risk of Future Fraud and Identity Theft

Plaintiffs also claim the time and money allegedly spent toward mitigating the risk of future fraudulent charges and identity theft constitutes injury sufficient to confer standing. The cost of guarding against a risk is an injury sufficient to confer standing only if the underlying harm the plaintiff is seeking to avoid is itself a cognizable Article III injury. *See Moyer*, 2014 WL 3511500, at *4 n. 1. As discussed above, however, on these pleadings I am not satisfied that either of the future injuries claimed in the complaint are themselves sufficient to confer standing.

The "fraudulent charge" injury, absent unreimbursed charges or other allegations of some substantial attendant hardship, is not in my view sufficiently concrete to establish standing. In any event, the complaint contains no meaningful allegations as to what precisely the costs incurred to mitigate the risk of future fraudulent charges were. Generally, when one sees a fraudulent charge on a credit card, one is reimbursed for the charge, and the threat of future charges is eliminated by the issuance of a new card, perhaps resulting in a brief period where one is without its use. If the complaint is to credibly claim standing on this score, it must allege something that goes beyond such *de minimis* injury.

As discussed above, the complaint does not adequately allege that the risk of identity theft is sufficiently imminent to confer standing. So long as that is the case, the "time and money

[1] I note that one plaintiff allegedly received a "phishing" phone call as a result of the cyber-attack on Defendant which, if she had disclosed private information, might have led to future identity theft. In my view, this allegation is sufficient neither to establish a "certainly impending" risk of identity theft, nor to qualify as a "concrete" injury for purposes of standing.

spent to mitigate" claim as to the risk of identity theft, which may well be more substantial than the same claim as to the risk of fraudulent credit card charges, is not a cognizable Article III injury.

C. The Financial Injury For Having Purchased Defendant's Products

Plaintiffs also assert that they paid a premium for the retail goods purchased at Defendant's stores, a portion of which Defendant was required to allocate to adequate data breach security measures. Because Defendant did not do so, Plaintiffs allege, Plaintiffs overpaid for their respective purchases and would not have otherwise made them. As Plaintiffs would have it, this financial injury establishes standing.

The argument is creative, but unpersuasive. All of the cases to which Plaintiffs cite in support of this proposition involved products which possessed some sort of deficiency. Plaintiffs purchased bottled water and it turned out to be municipal tap water. *Chicago Faucet Shoppe, Inc. v. Nestle Waters N. Am Inc.*, 2014 WL 541644, *3 (N.D.Ill. Feb. 11, 2014). Plaintiffs purchased children's toys and they turned out to be toxic. *In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011). As the Seventh Circuit noted, the fact that members of the class in such a case did not suffer physical injury did not mean that they were not injured. "The plaintiffs' loss is financial: they paid more for the toys [or water] than they would have." *Id*.

In my view, a vital limiting principle to this theory of injury is that the value-reducing deficiency is always intrinsic to the product at issue. Under Plaintiffs' theory, however, the deficiency complained of is extrinsic to the product being purchased. To illustrate the problem this creates: suppose a retail store does not allocate a sufficient portion of its revenues to providing adequate in-store security. A customer who is assaulted in the parking lot after patronizing the store may well have a negligence claim against the store owner. But could he or

she really argue that she overpaid for the products that she purchased? Or even more to the point: even if no physical injury actually befell the customer, under Plaintiffs' theory, the customer still suffered financial injury because he or she paid a premium for adequate store security, and the store security was not in fact adequate.

As set forth in *Aqua Dots*, this theory of injury is plainly sensible. In my view, however, expanding it to include deficiencies extrinsic to the purchased product would effectively render it meaningless.

D. The Loss of Control Over and Value of Plaintiffs' Private Information

Finally, I am also unpersuaded by Plaintiffs' claim to standing based on the loss of control over and value of their private information. Again, the injury as pled is not sufficiently concrete. *Cf. Barnes & Noble*, 2013 WL 4759588 (no actual injury of this sort where plaintiffs do not allege that their personal information was sold or that the plaintiffs themselves could have sold it).

CONCLUSION

For the foregoing reasons, Defendant's motion to dismiss for lack of Article III standing is granted.

ENTER:

James B. Zagel
United States District Judge

DATE: September 16, 2014