UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

In re First American Financial Corp. Securities Litigation	CV 20-9781 DSF (Ex) Order GRANTING Defendants' Motion to Dismiss (Dkt. 48)

This case arises out of alleged misrepresentations by Defendants First American Financial Corp. (First American or the Company), Dennis J. Gilmore, Mark E. Seaton, and Shabnam Jalakian concerning known deficiencies in First American's security practices.

Defendants move to dismiss the First Amended Complaint (FAC) filed by Lead Plaintiff St. Lucie County Fire District Firefighters Pension Trust Fund (the Fund). Dkt. 48 (Mot.). The Fund opposes. Dkt. 55 (Opp'n). The Court deems this matter appropriate for decision without oral argument. See Fed. R. Civ. P. 78; Local Rule 7-15. For the reasons stated below, the motion to dismiss is GRANTED.

I. BACKGROUND

A. The Parties

First American is a Fortune 500 company that provides title insurance and other financial services. Dkt. 46 (FAC) ¶¶ 17, 24. At all relevant times, Gilmore was the chief executive officer and a director of First American, id. ¶ 18; Seaton was the chief financial officer and executive vice president of First American, id. ¶ 19; and Jalakian was the chief information security officer (CISO) of First American, id. ¶ 20.

The Fund alleges it acquired First American securities "at artificially inflated prices" during the proposed class period – February

17, 2017 to October 22, 2020 (Class Period) – and "was damaged upon the corrective disclosures and/or materializations of concealed risks alleged herein." Id. ¶¶ 1, 16, 57.

B. First American's Cybersecurity Vulnerabilities

The Fund claims that from at least the start of the Class Period through May 2019, "Defendants misrepresented their security practices and controls to investors, and concealed the fact that the Company had declined to protect customer data including highly-sensitive NPI [non-public information] records, allowing them to be accessed by anyone with a web browser via First American's public-facing website (the 'Breach')." Id. ¶ 4.

"In performing title searches and facilitating closings, First American obtains from buyers, sellers, and internal and external databases documents that regularly contain highly-sensitive personal non-public information such as credit reports, escrow account balances, Social Security numbers, wire information and banking and investment account numbers." Id. ¶ 26. First American also "regularly collects records such as tax assessments and liens to include as part of a title insurance package." Id.

First American stores this information in its main document repository, the FAST image repository. Id. ¶ 30. First American created and maintains an application on its network known as EaglePro. Id. ¶ 39. EaglePro is a "web-based title document delivery system that allows title agents and other First American employees to share any document in FAST with outside parties." Id. "After a party to or a participant in a transaction selects documents from FAST to be shared with another participant of a real estate transaction, EaglePro emails the recipient a link to a website that allows him or her to access those documents." Id. ¶ 40. Anyone who had the link or the URL for the website could access the title package without login or authentication. Id.

A flaw in the EaglePro system, introduced in October 2014, gave rise to the Breach. Id. ¶ 41. The Breach involved automated "bots" or

"scraper" programs accessing more than 350,000 documents in FAST without authorization starting in June 2018 and continuing for 11 months. Id. ¶ 44.

Defendants have "readily and repeatedly acknowledged that protecting consumer data was crucial to First American's business operations, including to its core Title Insurance and Services segment." Id. ¶ 27. "Defendants conceded understanding during the Class Period that 'the protection of the information that resides on those systems are critically important to [First American's] successful operation.'" Id. ¶ 31. The Company's annual report filed with the SEC in February 2017, signed by Gilmore and Seaton, stated, "we are focused on growing our core title insurance and settlement services business, strengthening our enterprise through data and process advantages." Id. ¶ 27.

A 2017 Investor Letter published by Gilmore stated that "much of the Company's recent investments had been directed toward technology, including 'the continued enhancement of our title production platform and our customer-facing technologies and enterprise systems, all of which will improve our customers' experience and our internal process efficiency.'" Id. ¶ 28. In the same letter, Gilmore stated, "Strengthen the enterprise through data and process advantage . . . . These efforts strengthen our control over the key data assets that underlie our products and services and facilitate our efforts to manage risk and drive efficiencies throughout the title and settlement process." Id. ¶ 29.

Since at least 2017, First American repeatedly identified vulnerabilities and vulnerability management among its top risks. Id. ¶ 33. The Fund asserts First American withheld from investors that it had identified extensive vulnerabilities and declined to remediate those vulnerabilities as required by its own policies. Id. ¶ 34. According to First American's policies, it was supposed to:

- Scan all information assets for vulnerabilities, and provide a security overview report for each application and a risk assessment for data stored or transmitted by any application;

- Remediate critical or high-risk vulnerabilities within 15 days;
- Remediate medium risk vulnerabilities within 45 days; and
- Remediate low risk vulnerabilities within 90 days.

Id. First American deviated from these policies and did not perform a security overview or risk assessment for EaglePro. Id. ¶ 35. Tens of thousands of critical or high-risk vulnerabilities were permitted to persist for long periods of time without remediation. Id. On February 16, 2017, one of First American's regulators – the New York Department of Financial Services (NYDFS) – implemented comprehensive cybersecurity requirements, effective March 1, 2017. Id. ¶ 32.

C. Discovery of Vulnerabilities

An early 2018 test of NPI classification indicated that while 65 million of the 753 million documents then in FAST were tagged as containing NPI, hundreds of millions of documents not tagged were likely misclassified and did in fact contain sensitive NPI that required protection. Id. ¶ 37.d. Specifically, a random sampling of 1,000 non-tagged documents showed that 30% actually contained NPI, a finding that was discussed with the Board of Directors in April 2018. Id. Although Defendants had actual knowledge of this vulnerability, they neither remediated it at the time or enhanced their disclosures. Id.

On January 11, 2019, the final report of the EaglePro penetration test described the Breach in detail, including pages of screenshots demonstrating how the EaglePro website URL could be manipulated to display sensitive documents not intended for widespread viewing. Id. ¶ 48. The penetration test report also showed that more than 5,000 documents exposed by EaglePro had been indexed by Google, facilitating public searches whether or not the ImageDocumentID was known. Id.

On February 20, 2019, First American filed its 2018 annual report on Form 10-K, which stated cyberattacks and other incidents "could expose the Company to system-related damages, failures,

interruptions, and other negative events or could otherwise disrupt the Company's business and could also result in the loss or unauthorized release, gathering, monitoring or destruction of confidential, proprietary and other information pertaining to the Company, its customers, employees, agents or suppliers." Id. ¶¶ 79, 81. It also stated: "Certain laws and contracts the Company has entered into require it to notify various parties, including consumers or customers, in the event of certain actual or potential data breaches or systems failures." Id. ¶ 83.

On May 24, 2019, Brian Krebs, a journalist who reports on cybersecurity issues at KrebsOnSecurity.com, published an article revealing that First American had exposed approximately 850 million documents – some containing NPI – by rendering the documents openly accessible to the public. Id. ¶ 86. The data contained NPI such as social security numbers, drivers' licenses, and tax and banking information. Id. ¶ 87. Following publication of the Krebs report, shares of First American fell $3.46, or over 6%, to close at $51.80 on May 28, 2019. Id. ¶ 88.

According to charges filed on July 22, 2020 by the NYDFS, First American knew about the vulnerabilities both before and throughout the Class Period. Id. ¶ 36. Additionally, after interviewing First American's CISO, Jalakian, and its former senior director of information security as well as reviewing internal records, the NYDFS determined that "First American's CISO and senior personnel were fully aware of the disastrous state of First American's vulnerability management." Id.

The Fund asserts that a former employee (FE1), who worked as a security engineer at First American from July 2016 until November 2020, "was alerted to the EaglePro vulnerability when his colleague, Senior Information Security Engineer John Rehagen, documented that sensitive information was accessible outside of the network during a December 2018 penetration test." Id. ¶¶ 53, 54. "FE1 said that a high severity incident like the EaglePro vulnerability should have taken priority for remediation. Instead, First American hadn't started

remediating the EaglePro vulnerability when KrebsOnSecurity published its article in May 2019." Id. ¶ 55. Another former employee (FE2), "who worked as a director of information security for First American from July 2018 to September 2020 and reported directly to Defendant Jalakian at the time of the Breach, confirms that the Company did not begin to address the Breach until May 24, 2019, the same day that the Krebs article was published." Id. ¶ 56.

D. Misrepresentations

The Fund asserts that during 2017, Defendants made numerous misrepresentations in the "Privacy Information" section of First American's website, including that First American:

- Used its "best efforts to ensure that no unauthorized parties ha[d] access to any [customer] information";
- "[R]estrict[ed] access to nonpublic personal information about [customers] to those individuals and entities who need to know that information to provide products or services to [customers]";
- Would "use [its] best efforts to train and oversee [its] employees and agents to ensure that [customer's] information will be handled responsibly";
- "[M]aintain[ed] physical, electronic, and procedural safeguards that comply with federal regulations to guard [customers'] nonpublic personal information.

Id. ¶ 61.

On October 22, 2020, First American filed a quarterly report on Form 10-Q, announcing that the Company had received a Wells Notice – a letter from the SEC telling the recipient that the agency is planning to bring enforcement actions – regarding its disclosures to investors regarding its security Breach and disclosure controls. Id. ¶¶ 9, 104. On this news, the price of First American shares fell approximately $4.83 per share, or 9%, to close at $46.75 per share on October 22, 2020. Id. ¶ 105.

II. LEGAL STANDARD

A. Rule 12(b)(6)

Rule 12(b)(6) allows an attack on the pleadings for failure to state a claim on which relief can be granted. "[W]hen ruling on a defendant's motion to dismiss, a judge must accept as true all of the factual allegations contained in the complaint." Erickson v. Pardus, 551 U.S. 89, 94 (2007) (per curiam). However, a court is "not bound to accept as true a legal conclusion couched as a factual allegation." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007)). "Nor does a complaint suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" Id. (alteration in original) (quoting Twombly, 550 U.S. at 557). A complaint must "state a claim to relief that is plausible on its face." Twombly, 550 U.S. at 570. This means that the complaint must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 678. There must be "sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively . . . and factual allegations that are taken as true must plausibly suggest an entitlement to relief, such that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." Starr v. Baca, 652 F.3d 1202, 1216 (9th Cir. 2011).

Ruling on a motion to dismiss will be "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense. But where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged – but it has not 'show[n]' – 'that the pleader is entitled to relief.'" Iqbal, 556 U.S. at 679 (alteration in original) (citation omitted) (quoting Fed. R. Civ. P. 8(a)(2)).

As a general rule, leave to amend a complaint that has been dismissed should be freely granted. Fed. R. Civ. P. 15(a).

B. Rule 9(b)

Under Federal Rule of Civil Procedure 9(b), fraud claims must be pleaded with particularity. Kearns v. Ford Motor Co., 567 F.3d 1120, 1126 (9th Cir. 2009). "[A] plaintiff must set forth *more* than the neutral facts necessary to identify the transaction." In re GlenFed, Inc. Sec. Litig., 42 F.3d 1541, 1548 (9th Cir. 1994). A plaintiff must include "an account of the time, place, and specific content of the false representations" at issue. Swartz v. KPMG LLP, 476 F.3d 756, 764 (9th Cir. 2007) (quotation marks omitted). Fraud allegations must "be specific enough to give defendants notice of the particular misconduct so that they can defend against the charge and not just deny that they have done anything wrong." Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (citing Bly-Magee v. California, 236 F.3d 1014, 1019 (9th Cir. 2001) (punctuation omitted)).

Rule 9(b)'s particularity requirement "applies to all elements of a securities fraud action." Oregon Pub. Emps. Ret. Fund v. Apollo Grp. Inc., 774 F.3d 598, 605 (9th Cir. 2014). The Private Securities Litigation Reform Act of 1995 (PSLRA), 15 U.S.C. § 78u-4(b)(1), "imposes additional specific pleading requirements, including requiring plaintiffs to state with particularity both the facts constituting the alleged violation and the facts evidencing scienter." In re Rigel Pharms., Inc. Sec. Litig., 697 F.3d 869, 877 (9th Cir. 2012). In order to properly allege falsity, "a securities fraud complaint must . . . specify each statement alleged to have been misleading, [and] the reason or reasons why the statement is misleading." Id. (quotation marks and alteration omitted). In addition, in order to "adequately plead scienter under the PSLRA, the complaint must state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." Id. (quotation marks omitted).

III. DISCUSSION

A. Request for Judicial Notice

Defendants request judicial notice of 6 documents. The Fund objects only to Defendants' request for judicial notice of a table showing

the historical opening and closing trading prices of First American common stock from January 3, 2017, through December 30, 2020, obtained from Yahoo! Finance. Dkt. 56. The Court does not rely on the prices of the stock in reaching its decision. Defendants' request for judicial notice of the table is therefore DENIED as moot and the unopposed requests are GRANTED.

B. Rule 10b-5(b): Untrue Statement or Omission of Material Fact

Section 10(b) of the Exchange Act makes is "unlawful for any person, directly or indirectly . . . [t]o use or employ, in connection with the purchase or sale of any security . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe." 15 U.S.C. § 78j. Rule 10b-5, implementing Section 10(b), states:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
>
> (a) To employ any device, scheme, or artifice to defraud,
>
> (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
>
> (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b-5.

The elements of a claim under § 10(b) and Rule 10b-5 are: "(1) a material misrepresentation or omission; (2) made with scienter (i.e., a wrongful state of mind); (3) a connection between the

misrepresentation and the purchase or sale of a security; (4) reliance upon the misrepresentation . . .; (5) economic loss; and (6) loss causation." Loos v. Immersion Corp., 762 F.3d 880, 886-87 (9th Cir. 2014), as amended (Sept. 11, 2014). Under the heightened pleading standard of the PSLRA, complaints must "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed." Glazer Cap. Mgmt., LP v. Magistri, 549 F.3d 736, 741 (9th Cir. 2008). To establish falsity, a plaintiff "must demonstrate that a particular statement, when read in light of all the information then available to the market, or a failure to disclose particular information, conveyed a false or misleading impression." In re Convergent Techs. Sec. Lit., 948 F.2d 507, 512 (9th Cir. 1991).

Section 10(b) and Rule 10b-5(b) "do not create an affirmative duty to disclose any and all material information[;]" rather, "[d]isclosure is required under these provisions only when necessary 'to make . . . statements made, in light of the basic circumstances under which they were made, not misleading." Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27, 44 (2011) (citing 17 C.F.R. § 240.10b-5(b)). In order to be misleading, an incomplete statement "must affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists." Brody v. Transitional Hosps. Corp., 280 F.3d 997, 1006 (9th Cir. 2002); see also Reese v. Malone, 747 F.3d 557, 570 (9th Cir. 2014) ("By omitting information regarding BP's detection of high corrosion levels, [defendant] affirmatively created an 'impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]."), overruled on other grounds by City of Dearborn Heights Act 345 Police & Fire Ret. Sys. v. Align Tech., Inc., 856 F.3d 605, 619 (9th Cir. 2017)).

"By voluntarily revealing one fact about its operations, a duty arises for the corporation to disclose such other facts, if any, as are necessary to ensure that what was revealed is not 'so incomplete as to mislead.'" FindWhat Inv. Grp. v. FindWhat.com, 658 F.3d 1282, 1305

(11th Cir. 2011) (quoting Backman v. Polaroid Corp., 910 F.2d 10, 16 (1st Cir. 1990) (en banc)). "[E]ven absent a duty to speak, a party who discloses material facts in connection with securities transactions assumes a duty to speak fully and truthfully on those subjects." Id. (alteration in original) (quoting In re K-tel Int'l, Inc. Sec. Litig., 300 F.3d 881, 898 (8th Cir. 2002)). "[A] defendant may not deal in half-truths." Id. (quoting First Va. Bankshares v. Benson, 559 F.2d 1307, 1314 (5th Cir. 1977)).

1. Risk Factor Disclosures

The Fund alleges First American's risk factor disclosures regarding data security were false and misleading because they did not disclose that "the Company failed to implement basic security standards" and "disregarded its own information security policies," and as a result, "the Company did not protect but instead exposed tens of millions of documents containing sensitive customer NPI." FAC ¶¶ 58, 75, 80. Defendants assert this argument fails because the Fund does not allege that, "at the time any of the challenged statements were made, First American was not in fact implementing basic security standards, that Defendants believed the Company was 'disregard[ing]' its security policies, [or] that the Company made any public assurances about compliance with its policies." Mot. at 10.

The Fund first responds that Defendants' disclosures were misleading because, in discussing potential outcomes in the 2018 10-K after the Breach, First American stated, that "certain laws and contracts . . . require [the Company] to notify various parties . . . in the event of certain actual or potential data breaches or systems failures." This, the Fund asserts, casts as distant possibilities "the loss of customers, lawsuits, adverse publicity, diversion of management's time and energy, the attention of regulatory authorities, fines and disruptions in sales." Opp'n at 14 (quoting FAC ¶ 83). The Fund further asserts that "Defendants also misleadingly suggested that the Breach had been 'fixed' and otherwise minimized its impact, even though NPI was still very much at risk." Id. at 14-15 (citing FAC ¶¶ 92, 95, 97, 99, 102).

The Court agrees with Defendants that the Fund's first argument fails because it did not adequately plead that Defendants had actual knowledge of the Breach at the time of the disclosures, or that the disclosures were specific enough to misrepresent the current state of affairs.

Without the knowledge that the Breach had occurred, the disclosures here were generalized warnings about potential future risks. See Siracusano v. Matrixx Initiatives, Inc., 585 F.3d 1167, 1181 (9th Cir. 2009) ("[T]he passage in the Form 10-Q speaks about the risks of product liability claims in the abstract, with no indication that the risk 'may already have come to fruition.'"), aff'd, 563 U.S. 27 (2011); In re Alphabet, Inc. Sec. Litig., 1 F.4th 687, 704 (9th Cir. 2021) ("[T]he complaint plausibly alleges that Alphabet's warning in each Form 10-Q of risks that 'could' or 'may' occur is misleading to a reasonable investor *when Alphabet knew that those risks had materialized*." (emphasis added)).

The PSLRA requires that a securities complaint "shall, with respect to each act or omission alleged to violate this chapter, state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u-4(b)(2)(A). Pleading the "required state of mind" means alleging that "the defendants made false or misleading statements either intentionally or with deliberate recklessness." Zucco Partners, LLC v. Digimarc Corp., 552 F.3d 981, 991 (9th Cir. 2009).

The 2018 10-K was filed on February 20, 2019. Dkt. 50-4. But the FAC states First American first acknowledged the Breach in a report on Form 8-K with the SEC on May 28, 2019, after the issuance of the Krebs report, which revealed the Breach. FAC ¶¶ 86-89. The Fund does not plead any facts to support that First American knew of the Breach before May 2019 or at the time Defendants filed the 2018 10-K in February 2019.[1]

[1] The statements or alleged omissions in FAC ¶ 81 do not support the Fund's claims for the same reason. The statements warn of the potential of future

That the Board of Directors may have known of existing vulnerabilities also does not support that the disclosure statements were false or misleading. The Board discussed (1) that documents were misclassified as not containing NPI when they in fact contained NPI, and (2) that First American's Vulnerability Management Program was "unlikely to provide reasonable assurance that risks are being managed and objectives are being met." FAC ¶¶ 37 d, e. These generalized conversations about issues with data security do not establish that First American was aware of existing compromised data or support that the disclosure statements were specific enough to be contradicted by that general knowledge.[2]

Absent knowledge of an existing data security breach, the statements that the Company was obligated to inform certain parties of

---

attacks and do not make any representations about First American's existing data security before First American knew of the Breach.

[2] The Court notes that the knowledge of these vulnerabilities could support a claim that Defendants had a duty to correct a past statement, but the Fund does not identify any fact Defendants made in the past that would require disclosing this information. "Silence, absent a duty to disclose, is not misleading under Rule 10b-5." Basic Inc. v. Levinson, 485 U.S. 224, 239 n.17 (1988). "Section 10(b) of the Exchange Act and Rule 10b-5(b) do not create an affirmative duty to disclose any and all material information." In re Galectin Therapeutics, 843 F.3d at 1274. But Rule 10b-5(b) prohibits "any omissions of material fact 'necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading,'" such that "[b]y voluntarily revealing one fact about its operations, a duty arises for the corporation to disclose such other facts, if any, as are necessary to ensure that what was revealed is not 'so incomplete as to mislead.'" FindWhat, 658 F.3d at 1305. "Rather, to be actionably misleading, an omission 'must affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists.'" In re Ubiquiti Networks, 2014 WL 1254149, at * 10 (N.D. Cal. Mar. 26, 2014) (quoting Brody v. Transitional Hospitals Corp., 280 F.3d 997, 1006 (9th Cir. 2002)). The Fund does not adequately tie the knowledge of the defect to any representation that the state of affairs materially differed from the one Defendants' represented.

a breach were generalized statements about potential risks. "[A] reasonable investor would be unlikely to infer anything regarding the current state of a corporation's compliance, safety, or other operations from a statement intended to educate the investor on *future* harms." In re ChannelAdvisor Corp. Sec. Litig., No. 5:15-CV-00307-F, 2016 WL 1381772, at *5 (E.D.N.C. Apr. 6, 2016) (quoting Bondali v. Yum! Brands, Inc., 620 F. App'x. 483, 491 (6th Cir. 2015)), aff'd sub nom. Dice v. Channeladvisor Corp., 671 F. App'x 111 (4th Cir. 2016); cf. In Re Violin Memory Sec. Litig., No. 13-CV-5486 YGR, 2014 WL 5525946, at *12 (N.D. Cal. Oct. 31, 2014) ("[W]here a company's filings contain abundant and specific disclosures regarding the risks facing the company, as opposed to terse, generic statements, the investing public is on notice of these risks and cannot be heard to complain that the risks were masked as mere contingencies.") (quoting Plevy v. Haggerty, 38 F. Supp. 2d 816, 832 (C.D. Cal. 1998) (discussing cases)).

The Court also agrees that First American's comment that the issues were "fixed" was not misleading because "the Company shut down access to EaglePro promptly upon learning of the security incident." Reply at 4 n.4 (citing FAC ¶ 89). That customer data remained potentially vulnerable does not render the statement false or misleading, as it was clearly referring to a weakness in the database itself. FAC ¶ 92. Nor does the interpretation in a report disseminated several days later by analysts at Stephens that "[t]he Company has taken the necessary steps to fix the glitch" change the analysis. Again, Defendants stated they fixed the issue in the database, not that they had recovered all customer data.

The risk disclosure statements do not support the Fund's claims.

2. General Statements About First American's Information Security Program and Commitment to Protecting Data

Defendants assert their statements regarding general commitments to safeguarding customer data are not actionable because they are immaterial as a matter of law, are inactionable puffery, and are true. Mot. at 11. Defendants also claim there is "nothing

inconsistent between data being important and also subject to an undiscovered vulnerability." Id.

The Fund responds that the statements are material and not puffery because Defendants claimed to (1) have fundamentally sound practices when they "internally recognized widespread vulnerabilities and broad miscategorization of NPI," (2) restrict access to NPI when they in fact did not, and (3) prioritize the protection of information customers entrusted to their care but failed to remediate tens of thousands of known vulnerabilities as required by the Company's own internal policies. Opp'n at 17-18.

The Fund points to several statements to support its position that Defendants misrepresented that First American was securing customer NPI. Opp'n at 12-14. First, during 2017, First American's website stated, under the heading "Privacy Information," that First American was "committed to safeguarding customer information" and "agree[d] that [customers] have a right to know how [First American] will utilize the personal information [customers] provide to [First American]." FAC ¶ 61. The website stated, "we will not release your information to nonaffiliated parties except: (1) as necessary for us to provide the product or service you have requested of us; or (2) as permitted by law." Id. The website claimed, "We restrict access to nonpublic personal information about [customers] to those individuals and entities who need to know that information to provide products or services to [customers]." Id. The website also asserted: "We currently maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard [customers'] nonpublic personal information." Id.

Second, on May 3, 2017, Jalakian stated in an article:

> First American has established a formal information security program, led by the Corporate Information Security office, to continuously oversee and strengthen our security and privacy practices. This is accomplished by implementing fundamentally sound security policies as

> well as repeatable processes, best-of-breed technology solutions, and regular awareness training.

Id. ¶ 64. Jalakian also "claimed that the Company was 'serious' about 'the protection of information [consumers] entrust in our care,' and encouraged the Company's underwriters 'to be security evangelists for our customers and borrowers who may not have the same level of security protections at their disposal' as First American customers supposedly did." Id. ¶ 65 (brackets in original).

Third, Seaton stated during a 2017 conference that First American spent money "in technology, in customer-facing technology to make it easier for our customers to do business with us. We spend capital on building our databases, to make our business more efficient." Id. ¶ 67.

Fourth, during 2018, Defendants' website stated First American "offer[ed] secure, reliable, and affordable records storage solutions for [consumer] needs of any size to help [consumers] manage active mortgage collateral files." Id. ¶ 70. The website stated First American had a "Secure Facility Monitored 24-hours a day" featuring "Secure access to files which provides our clients with detailed information concerning their REO property closing status" Id.

Fifth, at a conference in 2018, Jalakian spoke publicly about a "layer of security we apply to information that belongs to our customers." Id. ¶ 72.

Sixth, in First American's annual report on Form 10-K for the fiscal year December 31, 2016, Defendants stated, "the integrity of the Company's computer systems and the protection of the information that resides on those systems are critically important to its successful operation." Id. ¶ 74.

The Court agrees with Defendants that the statements are either true or inactionable puffery. For example, stating First American was "committed to safeguarding customer information," ¶ 61, was not false because "commitment" is "not a word of certainty, even when viewed in context." In re Extreme Networks, Inc. Sec. Litig., No. 15-CV-04883-

BLF, 2018 WL 1411129, at *23 (N.D. Cal. Mar. 21, 2018) ("The surrounding factual allegations do not raise an inference that Defendants had an 'obligation' to achieve these results or assured the market that these results were 'certain.'"); see also Lasker v. New York State Elec. & Gas Corp., 85 F.3d 55, 59 (2d Cir. 1996) (finding a statement touting defendant's "commitment to create earning opportunities" was inactionable puffery); Lloyd v. CVB Fin. Corp., 811 F.3d 1200, 1207 (9th Cir. 2016) (holding a statement that "strong credit culture and underwriting integrity remain paramount" constituted vague and optimistic, inactionable puffery); Gammel v. Hewlett-Packard Co., 905 F. Supp. 2d 1052, 1071 (C.D. Cal. 2012) (finding statements that the defendant "underscores [its] strategy to provide a seamless, secure, context-aware experience across [its] product portfolio and to deliver innovation at unmatched scale" inactionable puffery); In re Alphabet, Inc. Sec. Litig., No. 18-CV-06245-JSW, 2020 WL 2564635, at *4 (N.D. Cal. Feb. 5, 2020) (finding representations "constitute generalized statements regarding the importance of privacy to users and Alphabet's general commitment to transparency and protection of their users' data" and therefore "are too vague and generalized to constitute the bases for misrepresentations; they are merely inactionable puffery.") aff'd in part, rev'd in part on other grounds and remanded, 1 F.4th 687 (9th Cir. 2021).

The same logic applies for statements that First American implemented a formal information security program, FAC ¶ 64, that First American was "'serious' about 'the protection of information [consumers] entrust in our care,'" id. ¶ 65 (brackets in original), that First American spent capital building its databases, id. ¶ 67, that First American applied a "layer of security" to customers' information, id. ¶ 72, and that protecting NPI was "critically important to [First American's] successful operation," id. ¶ 74.[3] These statements are either true, too vague to be material, or inactionable puffery.

[3] The Court also finds Seaton's comment at the 2019 conference that Defendants had "strong information security, but we're taking it to another level internally," FAC ¶ 99, to be immaterial and inactionable puffery

The statements that First American would not release information except as necessary or as permitted by law, id. ¶ 61, that First American restricts access to NPI, id., and that First American offered secure access to files, id. ¶ 70, are closer questions. These questions, unlike the statements above, may be "capable of objective verification." Oregon Pub. Emps. Ret. Fund, 774 F.3d at 606. But the Court finds these statements are "simply too vague to constitute a material statement of fact." Searls v. Glasser, 64 F.3d 1061, 1066 (7th Cir. 1995); see also In re Intel Corp. Sec. Litig., No. 18-CV-00507-YGR, 2019 WL 1427660, at *9 (N.D. Cal. Mar. 29, 2019) (finding a claim that processors were "vulnerability resistant" was not false and misleading although defendants knew of existing vulnerabilities).[4]

The general statements about First American's information security program and commitment to protecting data do not support the Fund's claims.

3. Statements About the Information Security Incident

Defendants contend the Fund does not plead facts supporting its assertion that certain claims relating to the information security incident were false. They claim the Fund alleges "no facts demonstrating that the security vulnerability stemmed from anything other than a 'design defect,' and the Company had no obligation to

---

because it was so vague no reasonable investor would rely on it. The comment that Seaton "think[s] [the Breach] will be fairly immaterial" is also a vague future prediction, not a material comment about the existing state of affairs.

[4] For the statements made before the discovery of vulnerable NPI in early 2018, FAC ¶ 37.d, the FAC also does not "contain allegations of specific 'contemporaneous statements or conditions' that demonstrate the intentional or the deliberately reckless false or misleading nature of the statements made," Ronconi v. Larkin, 253 F.3d 423, 432 (9th Cir. 2001), other than vague claims about First American having difficulties with vulnerability assessment, which are insufficient to meet this standard.

engage in self-flagellation by accusing itself (inaccurately) of 'fail[ing] to implement basic security standards.'" Mot. at 12-13 (quoting FAC ¶ 91). Defendants also assert the Fund does not plead facts to support "that First American was not 'working diligently' to remediate the issue when it said it was." Id. at 13 (quoting FAC ¶ 91).

The Court agrees the Fund has not identified any facts to support the allegation that Defendants' statements about the Breach were false or misleading. Even if Defendants had failed to implement certain security standards, the data leak still could have been a direct result of a design defect. Moreover, the Fund claims Defendants were not "working diligently" to address the Breach because they allowed NPI to be misclassified for years in the past. FAC ¶ 91. But what Defendants did in the years leading up to the Breach does not affect whether Defendants were "working diligently" *after* the Breach. The allegation that leaving customer NPI "exposed for many months even after the Breach was flagged internally," id., also does not support the contention that Defendants were not "working diligently," – just that they were not able to protect all customers' NPI immediately.

Nor is there any inconsistency between Defendants' statements that First American's investigation "identified imaged documents containing non-public personal information pertaining to 32 consumers that likely were accessed without authorization," and the Fund's allegation that 350,000 documents were accessed by automated "bots" or "scraper" programs. Mot. at 13. The Fund claims the report of the Breach in First American's February 18, 2020 Form 10-K was misleading because First American stated it "concluded an investigation regarding potential unauthorized access to non-public personal information as a result of a vulnerability in one of the Company's applications. The investigation identified imaged documents containing non-public personal information pertaining to 32 consumers that likely were accessed without authorization." FAC ¶ 95.

The Fund claims this statement was misleading because "the access to First American customers' NPI was not potential, but actual" and "First American was subject to a full-blown data breach, and not

'potential unauthorized access.'" Id. ¶ 96. But the use of the word "potential" is not misleading because the statement goes on to state that the "investigation identified imaged documents containing non-public information . . . that likely were accessed without authorization." FAC ¶ 95. The "potential" therefore clearly modifies "unauthorized" as opposed to "access."[5]

It was also not misleading to state that 32 customers were affected, when in fact 350,000 documents were accessed, because not all the documents in FAST contained NPI. See id. ¶¶ 49-50, 52. The statement clearly said: "The investigation identified imaged documents *containing non-public personal information* pertaining to 32 consumers that likely were accessed without authorization." Id. ¶ 95 (emphasis added). There is nothing inconsistent about saying 32 customers had NPI accessed and that many other documents not containing NPI were also accessed.

The Court also agrees the Fund does not plead facts sufficient to support the claim that Defendants mischaracterized a report by the Company's primary regulator, NYDFS, "or that the report did not conclude that First American's 'IT general controls environment is suitably designed and is operating effectively,' that the Company 'adequately and appropriately detected, analyzed, contained, eradicated and recovered from a security incident,' and that it was 'in compliance with New York's cyber security requirements for financial services companies.'" Mot. at 13-14 (quoting FAC ¶¶ 102-03).

The Fund does not indicate in what way First American's general IT controls were not operating effectively or how the Company failed to recover from the Breach. The Fund identifies only issues that existed in 2019, during the Breach, and immediately after the Breach.

Moreover, the Fund pleads that First American failed to timely encrypt documents containing NPI as required by the NYDFS's Cybersecurity Regulation. See FAC ¶ 52. But the Fund does not tie

[5] The same logic applies to the statements in FAC ¶ 89.

that to any statement or omission that would have been false or misleading. Seaton did not say First American's IT controls were operating effectively, he said a *report concluded* that First American's IT controls were operating effectively. Absent knowledge that the report was wrong, this cannot support that Seaton's statement was false or misleading. Although the Fund states Defendants were "well-aware" that First American was not in compliance with the NYDFS's cyber security requirements for financial services companies, id. ¶ 103, the Fund does not plead that Seaton specifically knew the report was wrong.

The statements about the information security incident do not support the Fund's claims.

Because the Fund does not identify any false or misleading statement or omission, its Section 10(b) and Section 20(a) claims fail. The Court therefore need not reach Defendants' arguments regarding scienter and loss causation. Should the Fund decide to amend, however, it should carefully consider Defendants' arguments on these issues rather than speculating that the Court will allow further amendment to address them.

IV. CONCLUSION

Defendants' motion to dismiss is GRANTED. An amended complaint must be filed no later than October 25, 2021. Failure to file by that date will waive the right to do so. The Court does not grant leave to add new defendants or new claims. Leave to add new defendants or new claims must be sought by a properly noticed motion.

IT IS SO ORDERED.

Date: September 22, 2021

Dale S. Fischer
United States District Judge