CRAIG VARNEN, SBN 172603
cvarnen@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

JASON J. MENDRO, SBN 220842
jmendro@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

COLIN B. DAVIS, SBN 273942
cdavis@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
3161 Michelson Drive
Irvine, CA 92612-4412
Telephone: 949.451.3800
Facsimile: 949.451.4220

Attorneys for Defendants First American Financial Corp., Dennis J. Gilmore, Mark E. Seaton, and Shabnam Jalakian

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

IN RE FIRST AMERICAN FINANCIAL CORP. SECURITIES LITIGATION

CASE NO. 2:20-cv-09781-DSF-E

NOTICE OF MOTION AND MOTION OF DEFENDANTS TO DISMISS PLAINTIFF'S AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

Hearing:
Date: August 30, 2021
Time: 1:30 p.m.
Place: Courtroom 7D
First Street Courthouse
350 West 1st Street
Los Angeles, California

Hon. Dale S. Fischer

NOTICE OF MOTION AND MOTION

NOTICE IS HEREBY GIVEN that on August 30, 2021 at 1:30 p.m., or as soon thereafter as the matter may be heard in the courtroom of the Honorable Dale S. Fischer of the above-entitled Court, Courtroom 7D, 350 West 1st Street, Los Angeles, California 90012, Defendants First American Financial Corp., Dennis J. Gilmore, Mark E. Seaton, and Shabnam Jalakian shall and hereby do move the Court for an order dismissing Plaintiff's Amended Class Action Complaint for Violations of the Federal Securities Laws.

This Motion is made under Federal Rules of Civil Procedure 12(b)(6) and 9(b) on the ground that Plaintiff has failed adequately to plead claims consistent with the requirements of the Private Securities Litigation Reform Act of 1995. As explained further below, the Complaint should be dismissed on multiple grounds: (i) Plaintiff has not alleged any material misrepresentation or omission in violation of Section 10(b) of the Securities Exchange Act; (ii) there are no allegations supporting an inference of scienter, much less the required strong inference; (iii) Plaintiff has not adequately alleged loss causation because there has been no disclosure "revealing" that any of Defendants' statements were fraudulent; (iv) Defendant Jalakian cannot be liable for statements she did not make; and (v) because Plaintiff has failed to plead a primary violation of Section 10(b), Defendants Gilmore and Seaton cannot be held liable as control persons under Section 20(a).

This Motion is made following the conference of counsel pursuant to L.R. 7-3 on May 13, 2021.

Dated: May 21, 2021

GIBSON, DUNN & CRUTCHER LLP
CRAIG VARNEN
JASON J. MENDRO
COLIN B. DAVIS

By: */s/ Jason J. Mendro*
Jason J. Mendro

Attorneys for *Defendants First American Financial Corp., Dennis J. Gilmore, Mark E. Seaton, and Shabnam Jalakian*

TABLE OF CONTENTS

TABLE OF CONTENTS
(Cont.)

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(Cont.)

Page(s)

TABLE OF AUTHORITIES
(Cont.)

Page(s)

TABLE OF AUTHORITIES
(Cont.)

Page(s)

TABLE OF AUTHORITIES
(Cont.)

I. INTRODUCTION

This case is the latest in a recent series of meritless lawsuits that accuse public companies of securities fraud after they disclose an unforeseen data security incident and suffer a stock price decline. This well-worn path is paved with dismissals. And for good reason: Data security incidents are an unfortunate reality of modern business, and it would be virtually unheard of for a corporation to represent that these incidents could not occur or to try to deceive their investors into believing that. Defendants made no such representations in this case, and the Complaint fails to plead otherwise.

On May 24, 2019, a blogger reported that documents containing information belonging to customers of the title and escrow operations of First American Financial Corp. ("First American" or the "Company") allegedly were accessible through links received by parties to real estate transactions. Upon being informed, First American promptly shut down access to the information and conducted an investigation. The investigation revealed that, out of 850 million images the blogger alleged were exposed, 32 customers' non-public information may have been accessed without authorization. First American notified those customers and offered them complimentary credit monitoring services. More than a year later, First American disclosed that it had received a Wells notice from the U.S. Securities and Exchange Commission ("SEC") notifying the Company that the enforcement staff was questioning the disclosures made at the time of the security incident and had preliminarily decided to recommend filing an enforcement action. Private plaintiffs then rushed to court and filed this lawsuit, claiming that the ensuing temporary dip in First American's stock price revealed that the Company had defrauded investors.

Plaintiff's theory is that Defendants committed securities fraud because they experienced an unexpected information security incident after describing First American's commitment to protecting customer data and related risks. On Plaintiff's view of the law, any public company that acknowledges the importance of data security but does not disclose unforeseen data security incidents is guilty of fraud.

Plaintiff's view is wrong. In 1995, Congress enacted the Private Securities Litigation Reform Act ("PSLRA") to curb abusive securities suits filed reflexively, and without credible evidence of fraud, when companies' stock prices declined. The PSLRA requires plaintiffs to allege with factual particularity which statements they claim are misleading and why. 15 U.S.C. § 78u-4(b)(1). It also requires them to plead a "strong inference" that the defendants perpetrated "each act or omission alleged" with scienter, i.e., a culpable state of mind embracing intentional or reckless deceit on investors. *Id.* § 78u-4(b)(2)(A). This unique pleading standard does not draw all inferences in favor of plaintiffs, but rather requires courts to balance the competing inferences of scienter and innocence. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 323–24 (2007). Securities fraud claims can survive dismissal "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference." *Id.* at 324. The Complaint does not satisfy these burdens.

First, the Complaint fails to plead any misstatement. What investors learned on May 24, 2019, is that First American—like every other company in the world—is susceptible to information security vulnerabilities. Defendants never said otherwise. And it would be absurd to assume otherwise, especially given that First American repeatedly cautioned investors that information security incidents, "regardless of their underlying causes, could … result in the loss or unauthorized release, gathering, monitoring or destruction" of confidential customer information. ¶¶ 59, 76, 81.[1]

Plaintiff strains to portray the occurrence of the incident as inconsistent with the Company's statements about the risks it faces, its information security program, and its commitment to safeguarding customer information. But First American never told investors that its systems were immune from vulnerabilities. And there is nothing

[1] Citations in the form of "¶ __" or "¶¶ __" refer to the paragraphs of Plaintiff's Amended Class Action Complaint ("Complaint") (ECF No. 46). Citations to "Mendro Ex." refer to the exhibits to the Declaration of Jason Mendro, filed concurrently. Unless otherwise noted, all emphasis is added, and all internal quotations and citations are omitted.

inconsistent between being committed to protecting customer data and later discovering that information inadvertently had been exposed. Plaintiff's attacks on the Company's disclosures about the information security incident fare no better. Plaintiff distorts what Defendants actually said and fails to plead any facts demonstrating that Defendants lied to investors about the cause of the security incident or the results of the Company's investigation and remediation efforts.

Second, Plaintiff fails to allege scienter. There is not a single allegation that supports an inference that Defendants tried to trick investors into believing that First American was immune from information security vulnerabilities or spoke with reckless disregard for whether investors would draw that conclusion. To the contrary, the Complaint is replete with allegations that support compelling inferences of innocence. Plaintiff admits the Company spent significant capital on information security, including "millions of dollars a year on technical security." ¶ 72; *see also* ¶ 67. It admits that First American conducted regular information security audits and reported their results to the Company's Audit Committee and Board of Directors. *See* ¶¶ 37–38. And it fails to plead that Defendants had anything to gain by misleading investors. Viewed holistically, the inferences that Defendants acted innocently eclipse any inference of scienter.

At the end of the day, Plaintiff's attempt to concoct a securities fraud claim from an unfortunate, but inadvertent, information security incident that affected less than a few dozen customers falls flat. Defendants never said that the Company's information security systems were invincible; indeed, they repeatedly warned otherwise. The Court should dismiss Plaintiff's Complaint.

II. SUMMARY OF THE ALLEGATIONS

A. The Parties

First American is the second-largest provider of title insurance in the United States. ¶ 24. First American performs title searches, facilitates closings for homebuyers, and insures owners and lenders against defects to their title to real property, such as liens, encumbrances, and adverse ownership claims. ¶¶ 24, 26.

The three "Individual Defendants" are First American officers. Mr. Gilmore is the Company's Chief Executive Officer and Director. ¶ 18. Mr. Seaton is the Company's Executive Vice President, Chief Financial Officer. ¶ 19. And Ms. Jalakian is First American's Senior Vice President, Chief Information Security Officer. ¶ 20.

St. Lucie County Fire District Firefighters Pension Trust Fund ("Plaintiff") is the Court-appointed Lead Plaintiff for this lawsuit. ECF No. 34. Plaintiff is a pension plan that allegedly acquired First American stock during the class period. ¶ 16.

B. First American's Image Repository, EaglePro, and the Company's Information Security Practices

To facilitate closings for homebuyers and provide title insurance services, First American routinely collects voluminous publicly available records and data. ¶¶ 26, 72. First American also collects some non-public information ("NPI") necessary to the services it offers. ¶ 26. First American stores digital copies of these documents in an image repository. ¶¶ 30–31. First American's employees tag documents containing NPI when uploading them to the repository. ¶¶ 31, 37(d), 49.

To share documents stored in the image repository with parties to real estate transactions, First American employed a web-based document-delivery application called EaglePro. ¶ 39. EaglePro allowed transaction participants to share images of documents stored in the repository by emailing a link to the document images. ¶ 40. The link contained an ImageDocumentID number that enabled the recipient to render an image of the document in the repository. ¶ 40.

First American disclosed the importance of securing customer data (including its image repository) and the potential for malicious actors or others to access customer information without authorization. As the Company explained in its public filings, information security is "critically important to its successful operation." ¶ 57; *see also* ¶¶ 63, 69, 74, 78–79, 85. First American warned investors that information security incidents, "regardless of their underlying causes," could "result in the loss or unauthorized release, gathering, monitoring or destruction" of confidential customer

information. ¶ 59; *see also* ¶¶ 63, 69, 76, 78, 81, 85.[2] As the Company's disclosures made clear, an information security incident could expose it to "lawsuits," "adverse publicity," and "governmental proceedings." ¶ 83; *see also* ¶ 85.

To safeguard data, First American established a "formal information security program" (¶ 64) that regularly reviewed the Company's information security system for potential vulnerabilities. ¶ 34. First American invested significant capital in securing data, including "millions of dollars a year on technical security." ¶ 72; *see also* ¶ 67.

Although Plaintiff alleges that First American failed to respond adequately to potential vulnerabilities it identified, it does not allege that First American had previously identified the vulnerability that caused the information security incident underlying Plaintiff's Complaint. *See, e.g.*, ¶ 37. Additionally, although Plaintiff alleges that First American conducted a penetration test of EaglePro in December 2018, the results of which were reflected in a January 2019 report (¶¶ 47–48), Plaintiff does not allege that the test or the report identified that vulnerability or found that NPI had been disclosed, or that the report ever was communicated to any of the Individual Defendants. *See* ¶ 48.

C. First American's Investigation and Resolution of the Information Security Incident

In May 2019, blogger Brian Krebs informed the Company that First American documents containing NPI were accessible through links received by parties to real estate transactions. ¶¶ 56, 86, 92. The Company investigated Mr. Krebs's claims and determined that the vulnerability related to the ImageDocumentID in the link generated by EaglePro. ¶ 41. Documents in the Company's image repository were numbered sequentially, so an individual who received an EaglePro link for one document could

---

[2] *See also* Mendro Ex. 2 at 15–16 ("[U]nauthorized data disclosures may disrupt the Company's business, harm the Company's reputation, result in material claims for damages or otherwise adversely affect the Company."); *accord* Mendro Ex. 3 at 15–16, Ex. 4 at 15. The Court can take judicial notice of SEC filings and consider documents incorporated by reference in the complaint without converting a motion to dismiss into a motion for summary judgment. *See In re Am. Apparel, Inc. S'holder Litig.*, 855 F. Supp. 2d 1043, 1060–62 & n.141 (C.D. Cal. 2012).

render other documents by changing the ImageDocumentID in the URL they entered into their internet browser. ¶¶ 40–41. Mr. Krebs published an article describing the vulnerability on May 24, 2019. ¶¶ 56, 86.

Upon receiving notice of the vulnerability—and before Mr. Krebs published his article—First American immediately "shut down external access" to the image repository and remediated the vulnerability. ¶ 89; *see* ¶ 92. The Company also engaged an outside forensic firm to "asses[s] the extent to which any customer information may have been compromised." ¶ 89. The investigation concluded that 32 customers of First American's title and escrow operations had documents containing NPI that "likely were accessed without authorization." ¶ 95; *see also* ¶ 97. First American notified those 32 customers and "offered complimentary credit monitoring services." ¶ 95. Although Plaintiff claims that more than 350,000 documents were accessed without authorization, it does not allege that any of those documents contained NPI beyond those related to the 32 customers First American identified. *See* ¶¶ 44, 96, 98, 103.

More than a year after First American disclosed and remediated the information security incident, the Company received a Wells notice from the SEC, notifying the Company that the enforcement staff had "made a preliminary determination to recommend a filing of an enforcement action" against First American in relation to "the disclosures the Company made at the time of the [information security] incident and the adequacy of its disclosure controls."[3] ¶ 104. First American promptly disclosed the Wells notice in its quarterly report on Form 10-Q for the third quarter of 2020. ¶ 104.

---

[3] First American's receipt of a Wells notice is unremarkable in itself and "does not necessarily indicate that charges will be filed" by the SEC; rather, it indicates only "that the staff of a government agency is considering making a recommendation." *Richman v. Goldman Sachs Grp., Inc.*, 868 F. Supp. 2d 261, 272 (S.D.N.Y. 2012). Moreover, the SEC has broad discretion to pursue non-fraudulent violations of the securities laws that are not actionable in a private securities class action, like this one, under Section 10(b). *See, e.g.*, *Aaron v. SEC*, 446 U.S. 680, 695–97 (1980) (explaining that Section 10(b) and Rule 10b-5 claims require proof of scienter, whereas Section 17(a)(2) requires only negligence); *In re Wash. Public Power Supply Sys. Sec. Litig.*, 823 F.2d 1349, 1358 (9th Cir. 1987) (no private right of action under Section 17(a)).

First American's stock price temporarily declined (¶ 105) but fully recovered by December 14, 2020 (*see* Mendro Ex. 1).

D. Plaintiff's Claims

On October 25, 2020, three days after First American announced that it had received a Wells notice, a purported First American stockholder filed this putative securities class action. ECF No. 1. Plaintiff filed the operative Amended Class Action Complaint on March 29, 2021. ECF No. 46.

Seeking to sue on behalf of a class of investors, ¶ 106, Plaintiff claims that Defendants made misleading statements or omissions between February 17, 2017, and October 22, 2020 (the "Class Period"), regarding the Company's commitment to protecting customer's NPI, its efforts to identify and resolve potential information security vulnerabilities, and the adequacy of its response to the information security incident discovered in May 2019. The Complaint borrows heavily from unproven allegations made in a separate proceeding instituted by the New York State Department of Financial Services (the "NYDFS") (*see* ¶¶ 8, 36–37, 49), and recites the cursory opinions of two unidentified former employees regarding First American's response to information security vulnerabilities (¶¶ 53–56). The Complaint, however, pleads no specific allegations controverting the truth of Defendants' statements at the time they were made, or addressing Defendants' beliefs or intentions regarding their communications with investors.

III. ARGUMENT

A. The PSLRA Imposes Strict Pleading Standards.

To state a Section 10(b) claim, a complaint must allege facts sufficient to establish (1) a material misrepresentation or omission; (2) made with scienter; (3) in connection with the purchase or sale of a security; (4) on which Plaintiff relied; (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). A securities fraud complaint also must meet the stringent pleading standards of Federal Rule of Civil Procedure 9(b) and the PSLRA, which

require a plaintiff to plead falsity and scienter with particularity. 15 U.S.C. § 78u-4(b)(1)–(2); *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 990–91 (9th Cir. 2009). Like virtually every similar complaint that has tried to transform a data security event into a claim for securities fraud, Plaintiff's Complaint fails to meet these standards.[4]

B. Plaintiff Fails to Plead an Actionable Misstatement or Omission.

To survive a motion to dismiss, a complaint must "specify each statement alleged to have been misleading [and] the reason or reasons why the statement is misleading." *Metzler Inv. GMBH v. Corinthian Colls., Inc.*, 540 F.3d 1049, 1061 (9th Cir. 2008); *accord* 15 U.S.C. § 78u-4(b)(1). "To be misleading, a statement must be capable of objective verification." *Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1275 (9th Cir. 2017). Vague, optimistic statements (i.e., "puffery") are not actionable because they do not induce reliance by reasonable investors and thus are immaterial as a matter of law. *See Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 606 (9th Cir. 2014).

1. Defendants' Affirmative Statements Are True and Inactionable.

a. Risk Factor Disclosures

Plaintiff's attempt to cast First American's "risk factor" disclosures regarding data security as misstatements fails. *See* ¶¶ 57, 59, 63, 69, 74, 76, 78–79, 81, 83, 85. Risk-

[4] With only a few easily distinguishable exceptions, the other cases that have attempted to premise securities fraud claims on a data security incident have been dismissed. *See Reidinger v. Zendesk, Inc.*, 2021 WL 796261 (N.D. Cal. Mar. 2, 2021) (dismissing Section 10(b) claim); *In re Fed Ex Corp. Sec. Litig.*, 2021 WL 396423 (S.D.N.Y. Feb. 4, 2021) (same); *In re Alphabet, Inc. Sec. Litig.*, 2020 WL 2564635 (N.D. Cal. Feb. 5, 2020) (same); *In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980 (N.D. Cal. 2020) (same); *Sgarlata v. PayPal Holdings, Inc.*, 409 F. Supp. 3d 846 (N.D. Cal. 2019), *aff'd sub nom. Eckert v. PayPal Holdings, Inc.*, 831 F. App'x 366, 367 (9th Cir. 2020) (same); *In re Intel Corp. Sec. Litig.*, 2019 WL 1427660 (N.D. Cal. Mar. 29, 2019) (same); *In re Qudian Inc. Sec. Litig.*, 2019 WL 4735376 (S.D.N.Y. Sept. 27, 2019) (dismissing Section 11, 12, 15 claims). The most notable exception is *In re Equifax Inc. Securities Litigation*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019), which permitted limited claims to proceed only because the defendant expressly touted "advanced security protections" it knew it did not have. *Id.* at 1219–20. The absence of any similar misrepresentation requires dismissal of this case.

factor disclosures, which the SEC instructs companies to include in their public filings, are prospective "discussion[s] of the material factors that make an investment in the [specific company] risky." 17 C.F.R. § 229.105(a) (Reg. S-K, Item 105). In compliance with this instruction, First American consistently disclosed, among other things, that "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," and that cyber attacks and other external events, like natural disasters, "could 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." ¶¶ 57, 59.

Risk-factor disclosures are "inactionable to the extent plaintiffs contend defendants should have disclosed risk factors 'are' affecting financial results rather than 'may' affect financial results" because they are "not meant to educate investors on what harms are currently affecting the company." *In re ChannelAdvisor Corp. Sec. Litig.*, 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). Because "[a] reasonable investor would be unlikely to infer anything regarding the ***current*** state" of First American's cybersecurity "from a statement intended to educate the investor on ***future*** harms," Plaintiff's challenges to risk-factor disclosures fail. *Bondali*, 620 F. App'x at 491 (first emphasis added); *see also In re Violin Memory Sec. Litig.*, 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 … 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))).

Plaintiff claims that the Company's risk-factor disclosures 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." ¶¶ 58, 75, 80; *see also* ¶¶ 60, 77, 82. But Plaintiff 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, that the Company made any public assurances about compliance with its policies, or that those policies were even publicly disclosed.[5] *See infra* pp. 15–23. Plaintiff's contention that Defendants had to disclose that an information security incident "had … already occurred" before they even learned that it occurred is nonsensical. *See, e.g.*, ¶ 47 (alleging that "the data exposure was ***unquestionably unknown*** to Defendants prior to December 2018"); ¶ 86 (May 24, 2019 Krebs report "reveal[ed]" the information security incident); *see also In re Twitter, Inc. Sec. Litig.*, 2020 WL 7260479, at *8 (N.D. Cal. Dec. 10, 2020) (risk disclosures not misleading because "plaintiffs do not allege how [the company] could have failed to disclose in July that which had not happened until August at the earliest").

It surely was not misleading for First American to warn investors, in its 2018 annual report on Form 10-K, that "[i]f the Company fails to comply with applicable regulations and contractual requirements, it could be exposed to lawsuits, governmental proceedings or the imposition of fines, among other consequences." ¶ 83. This statement was inarguably true. Plaintiff does not allege that any undisclosed lawsuit or government proceeding had been commenced against First American when this statement was made; to the contrary, Plaintiff admits that government proceedings commenced *after* the information security incident was revealed in May 2019.[6] *See*

---

[5] Although Plaintiff claims that the Company did not timely remediate information security vulnerabilities (*see* ¶ 37), it does not allege that the Company made any contradictory public statements about its remediation policy (*see* ¶ 34) or disclosed the policy to investors.

[6] When litigation and regulatory proceedings commenced following disclosure of the information security incident, the Company promptly disclosed them in accordance with its obligations under SEC regulations, *see* 17 C.F.R. § 229.103 (Reg. S-K, Item 103). *See, e.g.*, Mendro Ex. 5 at 96–97.

¶¶ 8–9, 104. Thus, First American did not omit to disclose exposure to any "lawsuits, government proceedings or the imposition of fines" that were "'already affecting'" it and required to be disclosed in 2018. *Facebook*, 477 F. Supp. 3d at 1017–18.

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

Plaintiff also challenges various statements describing First American's information security program and its commitment to safeguarding customer data. Again, Plaintiff fails to plead anything more than conclusory assertions of falsity.

First American's general commitments to safeguarding customer data are not actionable because they are immaterial as a matter of law. *See, e.g.*, ¶¶ 61 ("We believe we should behave responsibly when we use information …. We endeavor to educate the users of our products and services … about the importance of consumer privacy."); 65 (Company is "serious" about the protection of consumer data); *see also* ¶¶ 64 ("The objective of information security is to support the business and maximize stakeholder benefit while protecting the information assets of both the Company and its customers from all relevant threats."); 99 ("[W]e already felt like we had strong information security …."). Numerous courts have recognized that "'commitment' statements are inactionable puffery." *In re Extreme Networks, Inc. Sec. Litig.*, 2018 WL 1411129, at *23 (N.D. Cal. Mar. 21, 2018) (collecting cases); *Alphabet*, 2020 WL 2564635, at *4 (finding "generalized statements" about "Alphabet's general commitment to … protection of [user] data … inactionable puffery"); *Intel*, 2019 WL 1427660, at *9 (finding "vague positive statements" about security "immaterial as a matter of law").

Plaintiff also alleges no facts refuting the truth of Defendants' statements that First American is "Committed to Safeguarding Customer Information" (¶ 61) or that it is "serious" about "the protection of information [consumers] entrust in [the Company's] care" (¶ 65 (first alteration in original)). There is nothing inconsistent between data being important and also subject to an undiscovered vulnerability. As in *In re Heartland Payment Systems, Inc. Securities Litigation*, 2009 WL 4798148, at *6 (D.N.J. Dec. 7,

2009), First American "did not make any statements to the effect that the company's network was immune from security breaches or that no security breach had ever occurred." *See also Irving Firemen's Relief & Ret. Fund v. Uber Techs.*, 2018 WL 4181954, at *7–8 (N.D. Cal. Aug. 31, 2018) (statements about commitment to data security not actionable because "Defendants never claimed that [the company] would never again suffer a data breach, nor does Plaintiff suggest as much").

Nor does Plaintiff allege any facts demonstrating that Defendants' general statements about First American's information security program and products were false. *See* ¶¶ 64 ("First American has established a formal information security program … to continuously oversee and strengthen our security and privacy practices," including "by implementing fundamentally sound security policies …."); 67 ("We spend capital on building our databases, to make our business more efficient."); 70 ("We offer secure, reliable, and affordable records storage solutions …."); 72 ("[T]he security we apply to [publicly available data] is clearly different than the layer of security we apply to information that belongs to our customers."). To the contrary, Plaintiff admits that "protecting consumer data was crucial to First American's business operations," and that the Company invested in technology to "strengthen [its] control over the key data assets that underlie [its] products and services." ¶¶ 27–29. Plaintiff also admits that First American conducted regular information security audits and reported their results to the Company's Audit Committee and Board of Directors. *See* ¶¶ 37–38. These allegations "do not support an inference that [First American] did not make serious efforts to protect its computer network from security breaches." *Heartland*, 2009 WL 4798148, at *6.

c. Statements About the Information Security Incident

Plaintiff fails to plead facts alleging that First American's statements following discovery of the information security incident were false. Plaintiff's critiques of the Company's disclosure of the information security incident (*see* ¶¶ 89–91) amount to quibbles with First American's chosen words. Plaintiff alleges no facts demonstrating that the security vulnerability stemmed from anything other than a "design defect," and

the Company had no obligation to engage in self-flagellation by accusing itself (inaccurately) of "fail[ing] to implement basic security standards." ¶ 91; *see also In re Facebook, Inc. Sec. Litig.*, 405 F. Supp. 3d 809, 836 (N.D. Cal. 2019) ("[C]ompanies are not required to engage in 'self-flagellation' by disclosing unproven allegations."). Nor does Plaintiff plead factual allegations that it was inaccurate to say the design defect created the "potential" for unauthorized access (it did), or that First American was not "working diligently" to remediate the issue when it said it was. ¶ 91.

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" (¶ 95; *see also* ¶ 97), and Plaintiff's allegation that 350,000 documents were accessed by automated "bots" or "scraper" programs (¶ 44). *See* ¶¶ 96, 98. As Plaintiff admits, not all documents in the EaglePro application contained NPI (*see* ¶ 49), and Plaintiff pleads no facts demonstrating that this information was present in ***any*** of the documents allegedly accessed by non-human bots or scraper programs. *See In re Stratosphere Corp. Sec. Litig.*, 1997 WL 581032, at *13 (D. Nev. May 20, 1997) (to plead falsity, plaintiff must provide "evidentiary facts contemporary to the alleged false or misleading statements from which this court can make inferences permissible under Rule 9(b)").

Plaintiff's remaining claims are unfounded. Plaintiff pleads no factual allegations refuting Defendants' statement that the issues underlying the information security incident "ha[d] … been fixed" by May 28, 2019. ¶¶ 92–93. Even crediting Plaintiff's allegation that First American's senior management "vetoed internal recommendations to improve security of EaglePro" in the wake of the incident (¶ 50), that does not mean that customer information "remained exposed" (¶ 93), and Plaintiff does not allege a continued potential for unauthorized access after the Company shut down external access to EaglePro (*see* ¶ 89). Although Plaintiff takes issue with Defendant Seaton's characterization of the information security incident as "fairly immaterial" (¶¶ 99–100), the Complaint pleads no facts contradicting First American's conclusion that only 32

customers' NPI was accessed without authorization. Nor does Plaintiff plead any facts demonstrating that Defendant Seaton's statement on a July 23, 2020 earnings call, which summarized a report by the Company's primary regulator (the Nebraska Department of Insurance), mischaracterized the results of that report, 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." ¶¶ 102–03.

2. Plaintiff Fails to Plead an Actionable Omission.

Plaintiff also fails to meet the "high bar for [pleading] a materially misleading omission[.]" *Lake v. Zogenix, Inc.*, 2020 WL 3820424, at *9–10 (N.D. Cal. Jan. 27, 2020). "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). "To be actionable under the securities laws, an omission must be misleading; in other words it 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). Thus, the PSLRA expressly requires plaintiffs to "specify each statement alleged to have been misleading" as result of an omission. 15 U.S.C. § 78u-4(b)(1). "[A]s long as [any] omissions do not make the actual statements misleading, a company is not required to disclose" other facts "even if investors would consider the omitted information significant." *In re Rigel Pharm., Inc. Sec. Litig.*, 697 F.3d 869, 880 n.8 (9th Cir. 2012).

Here, for the same reasons discussed above, nothing in the Complaint renders First American's affirmative statements misleading. Plaintiff complains that Defendants omitted to disclose that First American "failed to implement basic security standards," that the Company "disregarded its own information security policies," and that the Company "lacked controls to properly classify or protect non-public information." *E.g.*, ¶¶ 58, 60, 62, 66, 68, 71, 73, 75, 77, 80, 82. But Defendants had no duty to disparage

the Company's data security measures publicly, potentially inviting attacks, because they made no affirmative representations about those measures that were deceptively incomplete. *See, e.g.*, *Intel*, 2019 WL 1427660, at *13 n.17 (finding no "duty to disclose" security vulnerabilities because "none of defendants' statements were materially misleading"); *Uber Techs.*, 2018 WL 4181954, at *5 (holding there was no "duty to disclose [Plaintiff's] 'laundry list' of allegedly fraudulent activities that are unconnected to the actual challenged statements"). Plaintiff complains that First American omitted to announce "actual" unauthorized access when it disclosed that such access was possible (¶ 91), but Plaintiff fails to plead that Defendants knew of any actual access at that time and cannot plausibly plead a duty to disclose that which is unknown.

C. Plaintiff Fails to Plead a Strong and Compelling Inference of Scienter.

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*, 552 F.3d at 991. "[R]ecklessness only satisfies scienter under § 10(b) to the extent that it reflects some degree of intentional or conscious misconduct." *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1053 (9th Cir. 2014). A strong inference of scienter exists "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs*, 551 U.S. at 324. "In reviewing a complaint under this standard, the court must consider *all* reasonable inferences to be drawn from the allegations, including inferences unfavorable to the plaintiffs." *Metzler*, 540 F.3d at 1061.[7]

[7] The U.S. Supreme Court has not ruled on whether reckless deceit constitutes scienter. Although the Ninth Circuit has, Defendants maintain that only intentional fraud is actionable and reserve the right to advance that argument in the appropriate forum.

Plaintiff's allegations come nowhere close to pleading scienter with particularity. The Complaint rests almost entirely on bare assertions of Plaintiff's conclusion that certain facts were "known" internally at the Company and must have been known by Defendants. *See, e.g.*, ¶¶ 4–5, 23. Plaintiff does not attempt to plead scienter as to each alleged misstatement or to each Individual Defendant, as the PSLRA requires. *See May v. KushCo Holdings, Inc.*, 2020 WL 6587533, at *7 (C.D. Cal. Sept. 25, 2020) (allegations that "impermissibly group[] all of the Individual Defendants together … are insufficient to satisfy the particularized pleading required of the PSLRA"); *see also In re VeriSign, Inc., Deriv. Litig.*, 531 F. Supp. 2d 1173, 1207 (N.D. Cal. 2007) ("It is not sufficient under the PSLRA to allege scienter against defendants as a group.").

In any event, Plaintiff's generalized scienter allegations are irrelevant. They center on whether Defendants knew about "vulnerabilities" in the Company's data security and the Company's supposed failure to "remediate" them. ¶¶ 4, 34–38. Because the statements Plaintiff challenges do not disclaim such vulnerabilities or assure investors they had been "remediated," what Defendants knew about these data security topics is beside the point. The relevant inquiry is whether Defendants knew their public statements would mislead investors. *See, e.g.*, *Reidinger*, 2021 WL 796261, at *9–10.

A sister court recently rejected similarly flawed claims in *Reidinger*. There, the plaintiff challenged a company's "nondisclosure of its [supposed] failure to implement certain security best practices" before a data security incident occurred. *Id.* at *9. The court explained that the plaintiff's theory of scienter "[wa]s, at best, convoluted: [the] officers did not know about a data breach, but chose to mislead investors … by refusing to disclose past security mistakes, while nonetheless disclosing that [the company] might have suffered an undetected breach." *Id.* at *10. So, too, here: The Complaint admits that the data security incident "was unquestionably unknown to Defendants" before December 2018. ¶ 47. And there are no factual allegations that Defendants knew about purported security vulnerabilities and "also consciously disregarded a risk that these

[vulnerabilities] made [the Company's] general statements about data security … misleading." *Reidinger*, 2021 WL 796261, at *9.

As in *Reidinger*, there are no allegations supporting the inference that Defendants subjectively believed any disputed statement would lead investors to conclude that First American—unlike every other company in the world—had no security vulnerabilities or somehow was immune to data security incidents. Nor does the Complaint even try to identify a motive for Defendants to mislead investors. Thus, the Complaint must be dismissed. *See May*, 2020 WL 6587533, at *8–10.

1. Plaintiff's Second-Hand Accounts of Contemporaneous Documents Do Not Support an Inference of Scienter.

The Complaint rests largely on documents Plaintiff never saw but presumably read about in the NYDFS Amended Statement of Charges. None of Plaintiff's second-hand accounts of these contemporaneous "internal records" (*see* ¶¶ 35–37) supports an inference of scienter. Plaintiff fails to "link[]" those records "and their contents to the [defendant] executives," *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d 1051, 1063 (9th Cir. 2014), or plead how they bear on Defendants' state of mind regarding the specific statements challenged in the Complaint.

For example, Plaintiff cites a December 2016 report to the Audit Committee but does not allege that any Individual Defendant prepared or presented that report or served on the Audit Committee during the relevant period. *See* ¶¶ 18–20, 37(a); *see In re Herbalife, Ltd.*, 2015 WL 7566616, at *3 (C.D. Cal. Nov. 23, 2015) (Fischer, J.) (allegation that results of a study were "known to Defendants" was insufficient where plaintiff provided "no detailed or specific allegations about [their] exposure to the results of the study"). Plaintiff also cites a 2017 information security audit and a 2018 audit report "prepared for First American's management and Board" (¶ 37(b), (e)–(f)), but fails to allege these reports had anything to do with First American's public disclosures or the information security incident at issue here, or that the Company did not address the issues described in the reports. In short, these allegations merely plead that First

American generated routine reports that might or might not bear on any relevant issue, that might or might not have been reviewed by any relevant person, and that ultimately reflect that First American was in fact focused on securing its data.

Plaintiff also claims "Defendants were fully aware" after April 2018 that the Company's method of classifying documents "failed to identify and protect documents containing [personal data]" (¶ 49), but the Complaint contains no allegations specific to any Individual Defendant. Plaintiff does not allege, for example, that the single "June 1, 2019 email from First American's Vice President of Information Security" was even sent to—let alone received, read, and agreed with by—any Defendant. ¶ 49(ii).

Importantly, Plaintiff does not plead that *any* of these records cast doubt on the truth of Defendants' statements. Defendants never stated that First American had no data security vulnerabilities or was immune to security incidents—in fact, the Company disclosed the opposite. Even assuming Defendants "had actual knowledge" of such a vulnerability (¶ 37(d)), therefore, that knowledge would not contradict any of Defendants' public statements. The Complaint also asserts that First American "repeatedly identified vulnerabilities and vulnerability management as among its own top risks" (¶ 33), but that conclusion only underscores management's attention to this issue and is consistent with the Company's public disclosures, which cautioned that data security was a risk (*see, e.g.*, ¶¶ 59, 76).

Plaintiff's reliance on a conclusory assertion of knowledge made in the NYDFS Statement of Amended Charges is misplaced for similar reasons. *See* ¶ 36 (quoting allegation that "First American's CISO and senior personnel were fully aware" of weaknesses in vulnerability management). This allegation says nothing about Messrs. Seaton and Gilmore, and Plaintiff all but concedes that Ms. Jalakian did not play a role in preparing First American's SEC filings. *See* ¶ 23; *see also infra* p. 25. Moreover, untested allegations in other lawsuits or enforcement actions "do not significantly add to an inference of scienter." *NVIDIA Corp.*, 768 F.3d at 1062; *see also In re Intel Corp. Derivative Litig.*, 621 F. Supp. 2d 165, 175 (D. Del. 2009) (declining

to "place great weight on a 'preliminary' finding" that a company had infringed the European Commission Treaty). In any event, alleged knowledge of weaknesses in vulnerability management is not the same as knowledge of errors in the Company's public disclosures.

Plaintiff's conclusory assertion that First American violated a NYDFS regulation by "fail[ing] to timely encrypt documents" (¶ 52), likewise does not salvage its deficient scienter allegations. The Complaint does not allege Defendants made any representations about the Company's compliance with this regulation or knew of any violation. The data security incident does not show that the regulation was violated, and conclusory allegations, in hindsight, of a violation do not satisfy Plaintiff's burden to plead what each Defendant knew at the time of any challenged statement.

2. Plaintiff's Confidential Witness Allegations Fail to Plead Scienter.

Plaintiff tries to plead scienter by summarizing the opinions of two confidential witnesses, to whom it refers to as "Former Employees" or "FEs." ¶¶ 53–56. "The Ninth Circuit has articulated a two-prong test for a plaintiff relying on confidential-witness statements to prove scienter: (1) statements must be described with sufficient particularity to establish their reliability and personal knowledge; and (2) the statements must themselves be indicative of scienter." *Sgarlata*, 409 F. Supp. 3d at 856. Plaintiff's sparse allegations fail to meet either prong.

First, the Complaint pleads no facts suggesting that either FE could have personal knowledge of Defendants' state of mind. It does not allege that FE1 ever interacted with any Individual Defendant (¶¶ 53–55), and it alleges that FE2 became director of information security in July 2018—well after the start of the Class Period (*see* ¶ 56). Although FE2 allegedly reported to Ms. Jalakian "at the time of the Breach" (¶ 56), FE2 is not alleged to have communicated with her on any relevant topic. Because Plaintiff does not "allege facts demonstrating that the [FEs] consulted were in a position to know what management knew," its confidential witness allegations do not support an inference of scienter. *Knollenberg v. Harmonic, Inc.*, 152 F. App'x 674, 681 (9th Cir. 2005).

Second, neither FE statement has anything to do with Defendants' knowledge or the truth of the First American's public disclosures. FE1 merely second-guesses the Company's business decisions by stating that the EaglePro vulnerability "should have taken priority for remediation." ¶ 55. And FE2 only "confirm[ed]" that the Company began to address the data security incident in May 2019. ¶ 56. Neither statement is "indicative of scienter" or suggests that Defendants knew any challenged statement was false when made. *Sgarlata*, 409 F. Supp. 3d at 858–59; *see also Prodanova v. H.C. Wainwright & Co., LLC*, 993 F.3d 1097, 1110 (9th Cir. 2021) (to "support an inference of scienter," witness statements "must provide specific facts showing a connection between the false statement and the mindset of the person who made it").

3. The Individual Defendants' Positions Do Not Support an Inference of Scienter.

Plaintiff formulaically recites that the Individual Defendants must have had culpable knowledge because of their "positions" at the Company and resulting access to information. *See, e.g.*, ¶¶ 23, 119. But courts have repeatedly held that "[t]he mere fact of a particular defendant's position within [the Company] is insufficient … to impose liability." *VeriSign*, 531 F. Supp. 2d at 1207. Because the Complaint pleads no more detailed allegations "showing what each defendant knew, when he/she knew it, or how he/she acquired that knowledge," it falls far short of the PSLRA's particularity requirements. *Id.*

Ms. Jalakian's statement at a 2018 panel discussion that she "personally meet[s] with the Board" and "with our CEO" on a regular basis (¶ 38), adds nothing. Plaintiff claims this statement leaves "no question" that the unspecified "deficiencies" purportedly known to Ms. Jalakian "were also known to Defendant Gilmore and the rest of First American's Board and senior management." *Id.* But this "extended chain of inferences" does not satisfy the PSLRA, which "clearly establishes a preference for facts over such inferential leaps." *In re Northpoint Commc'ns Grp., Inc. Sec. Litig.*, 184 F. Supp. 2d 991, 1005 (N.D. Cal. 2001); *see Herbalife*, 2015 WL 7566616, at *3

(allegations of "interaction with other officers and employees" and "receipt of weekly or monthly reports" are "insufficient to create a strong inference of scienter").

4. The Core Operations Doctrine Does Not Apply.

The Complaint also invokes the core operations doctrine by repeating that the data security incident affected "[a] core operation" of the Company, namely, its "core Title Insurance and Services segment." ¶¶ 25, 27. But Plaintiff cannot plead scienter "by simply incanting this theory." *Plumley v. Sempra Energy*, 2021 WL 754841, at *3 (9th Cir. Feb. 26, 2021); *Police Ret. Sys. of St. Louis*, 759 F.3d at 1062 ("Proof under this theory is not easy."). Absent particularized allegations about "defendants' actual exposure to information," the core operations doctrine "permits an inference of scienter" only "in exceedingly rare cases where an event is so prominent that it would be *absurd* to suggest that key officers lacked knowledge of it." *Swartzendruber v. Colony Capital, Inc.*, 2020 WL 7754008, at *6 (C.D. Cal. Dec. 10, 2020).

The Complaint does not come close to pleading the facts necessary for the core operations doctrine to apply. Plaintiff alleges no "specific admissions by [Defendants] of detailed involvement in the minutia of [the Company's] operations" or any "witness accounts demonstrating that they had actual involvement in creating false reports" to investors. *Police Ret. Sys. of St. Louis*, 759 F.3d at 1062; *see Webb v. Solarcity Corp.*, 884 F.3d 844, 857 (9th Cir. 2018) (rejecting invocation of core operations doctrine where plaintiff failed to allege defendants "were involved in accounting decisions as minute" as those relevant to challenged statements). Nor has Plaintiff alleged facts supporting the inference that the data security incident "was so dramatic that it would be *absurd* to think that Defendants[] did not know" about it. *Webb*, 884 F.3d at 857. "Thus, the core operations doctrine does not apply." *Swartzendruber*, 2020 WL 7754008, at *6; *see Pittleman v. Impac Mortg. Holdings, Inc.*, 2009 WL 648983, at *3 (C.D. Cal. Mar. 9, 2009) ("vague allegations of [company guideline] violations are not one of th[o]se 'exceedingly rare' cases" that trigger application of the core operations doctrine), *aff'd sub nom. Sharenow v. Impac Mortg. Holdings, Inc.*, 385 F. App'x 714 (9th Cir. 2010).

5. The Timing of Announcement of the Information Security Incident Does Not Support an Inference of Scienter.

Plaintiff suggests that the five-month "delay" between the EaglePro penetration test in December 2018 and the disclosure of the information security incident in May 2019 was motivated by an intent to mislead investors. *See* ¶¶ 4, 91. Plaintiff's description of the timeline is misleading. The Complaint admits Defendants "unquestionably" lacked knowledge of the data security incident before December 2018—nearly two years after the start of the Class Period and after most statements challenged in the Complaint. ¶ 47. Although the Complaint implies that the Individual Defendants learned about the exposure of personal data in December 2018 (*see* ¶¶ 4, 91), it alleges only that a "test team" conducted a penetration test of the EaglePro application to identify the existence of security vulnerabilities (¶ 47). And it does not allege that any Individual Defendant received or reviewed the resulting report in January 2019, which would not have revealed the exposure of NPI in any event. *Id.* ¶ 48 (report "acknowledged that further investigation was … required to determine whether sensitive documents were exposed"). "[E]ven if there were a handful of lower-level employees" who were concerned in December 2018 about the possibility that documents containing personal data had been exposed or accessed, "[t]here is nothing in the Complaint that supports an inference that these concerns were … relayed to any of the Defendants." *Heartland Payment Sys.,* 2009 WL 4798148, at *8.

Plaintiff's claim that Defendants acted with culpable intent by "conceal[ing]" the data security incident (¶ 87; *see* ¶ 50), also is misleading. The Complaint pleads that First American publicly announced the incident just days after Mr. Krebs alerted it to the alleged exposure of NPI. ¶¶ 86–89; *see NVIDIA Corp.*, 768 F.3d at 1056–57, 1065 (holding that plaintiff did not plausibly allege that defendants "intentionally mislead investors, or acted with deliberate recklessness, by not disclosing [a] problem sooner").

6. The Countervailing Inferences of Innocence Are Overwhelming.

After considering the negative inferences that can be drawn from Plaintiff's largely irrelevant allegations, this Court must "comparatively weigh" them against the

"opposing inferences" of innocence. *See Metzler*, 540 F.3d at 1061, 1068. Here, the innocent inferences are not only compelling, but overwhelming.

First, Plaintiff's failure to plead any fraudulent motive or insider stock sales "detract[s] from a scienter finding." *Webb*, 884 F.3d at 856; *see Eckert*, 831 F. App'x at 367 (lack of scienter "underscored by the absence of any allegation … that any defendant sold stock during the relevant time period or otherwise had a motive to mislead investors"). Plaintiff offers no "explanation of what benefit Defendants hoped to gain by delay[ing] disclosure of … the [data] breach," an occurrence that "could not be undone, mooted, or masked by waiting." *Sgarlata*, 409 F. Supp. 3d at 859.

Second, the Complaint admits that First American filed with the SEC a current report on Form 8-K on the first business and trading day after publication of the Krebs report. *See* ¶¶ 86–89. And it admits that the Company launched an immediate investigation when it was alerted to the potential unauthorized access of personal data. ¶¶ 89, 95, 97. These allegations "demonstrat[e] a pursuit of truth rather than reckless indifference to the truth." *Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 758 (7th Cir. 2007).

Third, Defendants never suggested that First American was impervious to data security incidents and could not have expected their statements to lead investors to believe otherwise. To the contrary, First American disclosed that such incidents could occur and adversely impact its business. *See, e.g.*, ¶¶ 59, 76; *see also Reidinger*, 2021 WL 796261, at *10 (fact that defendants "warned investors about this exact possibility" strongly supported inference that defendants "did not intend" statements "to be misleading or deliberately disregard the risk that they would be misleading").

7. Plaintiff Fails to Plead Corporate Scienter.

"[A] corporation can only act through its employees and agents and can likewise only have scienter through them." *In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d 471, 475 (9th Cir. 2015). Because Plaintiff fails to plead scienter as to any Individual Defendant, it fails to plead scienter as to First American.

D. Plaintiff Fails to Plead Loss Causation.

The Complaint must be dismissed on the independent ground that Plaintiff fails to plead loss causation. To plead loss causation with the particularity required by Rule 9(b), a plaintiff "must demonstrate that an economic loss was caused by the defendant's misrepresentations, rather than some other intervening event" or "other fact." *Lloyd v. CVB Fin. Corp.*, 811 F.3d 1200, 1209–10 (9th Cir. 2016). When a securities fraud plaintiff relies on a "revelation of the fraud" theory of loss causation, the plaintiff must plead that (1) she purchased a security at a price that was artificially inflated by a specific alleged misstatement; (2) a "corrective disclosure" subsequently revealed the "truth" about that specific misstatement; and (3) the disclosure of the truth caused the company's stock price to decline. *Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 342–43, 346–47 (2005); *In re BofI Holding, Inc. Sec. Litig.*, 977 F.3d 781, 790 (9th Cir. 2020).

A corrective disclosure "must by definition reveal new information to the market." *In re BofI*, 977 F.3d at 794; *accord Rok v. Identiv, Inc.*, 2017 WL 35496, at *18 (N.D. Cal. Jan. 4, 2017). "[T]he announcement of an investigation, without more, is insufficient to establish loss causation." *Loos*, 762 F.3d at 890. This is because, "at the moment an investigation is announced, the market cannot possibly know what the investigation will ultimately reveal." *Id.* Announcing an investigation "simply puts investors on notice of a *potential* future disclosure of fraudulent conduct." *Id.*

Here, Plaintiff's loss causation allegations are premised on the October 22, 2020 disclosure that the Company had received a Wells notice regarding its disclosures and disclosure controls. ¶¶ 104–05. But the Wells notice did not reveal that Defendants committed securities fraud, *see supra* note 3, and Plaintiff does not allege any further disclosure that would suggest the ensuing stock-price drop reflected anything other than "market speculation about whether fraud has occurred." *Loos*, 762 F.3d at 890. Although Plaintiff also alleges that First American's stock price briefly declined after it disclosed the information security incident on May 28, 2019 (¶ 88), its stock price fully recovered by June 18 and continued climbing thereafter, foreclosing any damages and

thus preventing reflexive lawsuits at that time. *See* Mendro Ex. 1; 15 U.S.C. § 78u-4(e)(1) (limiting damages to the difference between plaintiff's purchase or sale price and the mean trading price of the stock in the 90-day period after the alleged corrective disclosure). Accordingly, Plaintiff fails to plead loss causation.

E. Ms. Jalakian Cannot Be Liable for Statements She Did Not Make.

Ms. Jalakian cannot be liable for the vast majority of statements Plaintiff disputes. Only "the person or entity with ultimate authority over [a] statement, including its content and whether and how to communicate it" can be liable under Rule 10b-5. *Janus Capital Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 142 (2011). The Complaint alleges that only Messrs. Gilmore and Seaton signed First American's public reports (¶¶ 18–20), and it admits that Ms. Jalakian "had the power and authority to control [only] the contents of the information and statements *attributed to her*" (¶ 23). Plaintiff's claim against Ms. Jalakian must, at minimum, be dismissed to the extent it is based on any statement other than the two attributed to her.[8] *See* ¶¶ 64–65, 72.

F. The Complaint Fails to State a Claim Under Section 20(a).

Count II of the Complaint asserts a claim against Messrs. Gilmore and Seaton for "control person" liability under Section 20(a) of the Exchange Act. ¶¶ 124–30; *see* 15 U.S.C. § 78t(a). To plead a Section 20(a) claim, a plaintiff "must show that a primary violation was committed and that the defendant directly or indirectly controlled the violator." *Paracor Fin., Inc. v. Gen. Elec. Capital Corp.*, 96 F.3d 1151, 1161 (9th Cir. 1996). Because Plaintiff has failed to allege a primary violation of Section 10(b), its Section 20(a) claims also fail. *NVIDIA Corp.*, 768 F.3d at 1052.

IV. CONCLUSION

For the foregoing reasons, the Complaint should be dismissed.

[8] Ms. Jalakian also cannot be liable for these two statements because neither is false or misleading. *See supra* pp. 8-15.

Dated: May 21, 2021

GIBSON, DUNN & CRUTCHER LLP
CRAIG VARNEN
JASON J. MENDRO
COLIN B. DAVIS

By: */s/ Jason J. Mendro*
Jason J. Mendro

Attorneys for Defendants First American Financial Corp., Dennis J. Gilmore, Mark E. Seaton, and Shabnam Jalakian