

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

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

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

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

15 UNITED STATES DISTRICT COURT
16 CENTRAL DISTRICT OF CALIFORNIA
17 WESTERN DIVISION

18 IN RE FIRST AMERICAN
19 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

1
2 NOTICE IS HEREBY GIVEN that on August 30, 2021 at 1:30 p.m., or as soon
3 thereafter as the matter may be heard in the courtroom of the Honorable Dale S. Fischer
4 of the above-entitled Court, Courtroom 7D, 350 West 1st Street, Los Angeles, California
5 90012, Defendants First American Financial Corp., Dennis J. Gilmore, Mark E. Seaton,
6 and Shabnam Jalakian shall and hereby do move the Court for an order dismissing
7 Plaintiff’s Amended Class Action Complaint for Violations of the Federal Securities
8 Laws.

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

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

23 Dated: May 21, 2021

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

24
25
26 By: /s/ Jason J. Mendro
Jason J. Mendro

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

TABLE OF CONTENTS

1		
2		<u>Page</u>
3	I. INTRODUCTION.....	1
4	II. SUMMARY OF THE ALLEGATIONS	3
5	A. The Parties.....	3
6	B. First American’s Image Repository, EaglePro, and the Company’s Information Security Practices.....	4
7		
8	C. First American’s Investigation and Resolution of the Information Security Incident	5
9	D. Plaintiff’s Claims.....	7
10	III. ARGUMENT	7
11	A. The PSLRA Imposes Strict Pleading Standards.	7
12	B. Plaintiff Fails to Plead an Actionable Misstatement or Omission.	8
13	1. Defendants’ Affirmative Statements Are True and Inactionable.....	8
14		
15	2. Plaintiff Fails to Plead an Actionable Omission.....	14
16	C. Plaintiff Fails to Plead a Strong and Compelling Inference of Scienter.....	15
17	1. Plaintiff’s Second-Hand Accounts of Contemporaneous Documents Do Not Support an Inference of Scienter.	17
18		
19	2. Plaintiff’s Confidential Witness Allegations Fail to Plead Scienter.	19
20	3. The Individual Defendants’ Positions Do Not Support an Inference of Scienter.....	20
21		
22	4. The Core Operations Doctrine Does Not Apply.	21
23	5. The Timing of Announcement of the Information Security Incident Does Not Support an Inference of Scienter.....	22
24	6. The Countervailing Inferences of Innocence Are Overwhelming.....	22
25		
26	7. Plaintiff Fails to Plead Corporate Scienter.	23
27	D. Plaintiff Fails to Plead Loss Causation.	24
28	E. Ms. Jalakian Cannot Be Liable for Statements She Did Not Make.....	25
	F. The Complaint Fails to State a Claim Under Section 20(a).	25

**TABLE OF CONTENTS
(Cont.)**

Page

IV. CONCLUSION.....25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

Page(s)

CASES

Aaron v. SEC,
446 U.S. 680 (1980)..... 6

In re Alphabet, Inc. Sec. Litig.,
2020 WL 2564635 (N.D. Cal. Feb. 5, 2020)..... 8, 11

In re Am. Apparel, Inc. S’holder Litig.,
855 F. Supp. 2d 1043 (C.D. Cal. 2012)..... 5

Basic Inc. v. Levinson,
485 U.S. 224 (1988)..... 14

In re BofI Holding, Inc. Sec. Litig.,
977 F.3d 781 (9th Cir. 2020)..... 24

Bondali v. Yum! Brands, Inc.,
620 F. App’x 483 (6th Cir. 2015)..... 9

Brody v. Transitional Hosps. Corp.,
280 F.3d 997 (9th Cir. 2002)..... 14

In re ChannelAdvisor Corp. Sec. Litig.,
2016 WL 1381772 (E.D.N.C. Apr. 6, 2016)..... 9

In re ChinaCast Educ. Corp. Sec. Litig.,
809 F.3d 471 (9th Cir. 2015)..... 23

Dice v. ChannelAdvisor Corp.,
671 F. App’x 111 (4th Cir. 2016)..... 9

Dura Pharms., Inc. v. Broudo,
544 U.S. 336 (2005)..... 24

Eckert v. PayPal Holdings, Inc.,
831 F. App’x 366 (9th Cir. 2020)..... 8, 23

In re Equifax Inc. Sec. Litig.,
357 F. Supp. 3d 1189 (N.D. Ga. 2019)..... 8

TABLE OF AUTHORITIES
(Cont.)

Page(s)

1

2

3

4 *In re Extreme Networks, Inc. Sec. Litig.*,

5 2018 WL 1411129 (N.D. Cal. Mar. 21, 2018) 11

6 *In re Facebook, Inc. Sec. Litig.*,

7 405 F. Supp. 3d 809 (N.D. Cal. 2019)..... 13

8 *In re Facebook, Inc. Sec. Litig.*,

9 477 F. Supp. 3d 980 (N.D. Cal. 2020)..... 8, 11

10 *In re Fed Ex Corp. Sec. Litig.*,

11 2021 WL 396423 (S.D.N.Y. Feb. 4, 2021) 8

12 *In re Heartland Payment Sys., Inc. Sec. Litig.*,

13 2009 WL 4798148 (D.N.J. Dec. 7, 2009) 11, 12, 22

14 *In re Herbalife, Ltd.*,

15 2015 WL 7566616 (C.D. Cal. Nov. 23, 2015) 17, 20

16 *Higginbotham v. Baxter Int’l, Inc.*,

17 495 F.3d 753 (7th Cir. 2007) 23

18 *In re Intel Corp. Derivative Litig.*,

19 621 F. Supp. 2d 165 (D. Del. 2009) 18

20 *In re Intel Corp. Sec. Litig.*,

21 2019 WL 1427660 (N.D. Cal. Mar. 29, 2019) 8, 11, 15

22 *Irving Firemen’s Relief & Ret. Fund v. Uber Techs.*,

23 2018 WL 4181954 (N.D. Cal. Aug. 31, 2018) 12, 15

24 *Janus Capital Grp., Inc. v. First Derivative Traders*,

25 564 U.S. 135 (2011)..... 25

26 *Knollenberg v. Harmonic, Inc.*,

27 152 F. App’x 674 (9th Cir. 2005)..... 19

28 *Lake v. Zogenix, Inc.*,

 2020 WL 3820424 (N.D. Cal. Jan. 27, 2020)..... 14

Lloyd v. CVB Fin. Corp.,

 811 F.3d 1200 (9th Cir. 2016) 24

TABLE OF AUTHORITIES
(Cont.)

Page(s)

1

2

3

4 *Loos v. Immersion Corp.*,

5 762 F.3d 880 (9th Cir. 2014) 7, 24

6 *May v. KushCo Holdings, Inc.*,

7 2020 WL 6587533 (C.D. Cal. Sept. 25, 2020) 16, 17

8 *Metzler Inv. GMBH v. Corinthian Colls., Inc.*,

9 540 F.3d 1049 (9th Cir. 2008) 8, 15, 23

10 *In re Northpoint Commc’ns Grp., Inc. Sec. Litig.*,

11 184 F. Supp. 2d 991 (N.D. Cal. 2001) 20

12 *In re NVIDIA Corp. Sec. Litig.*,

13 768 F.3d 1046 (9th Cir. 2014) 15, 18, 22, 25

14 *Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*,

15 774 F.3d 598 (9th Cir. 2014) 8

16 *Paracor Fin., Inc. v. Gen. Elec. Capital Corp.*,

17 96 F.3d 1151 (9th Cir. 1996) 25

18 *Pittleman v. Impac Mortg. Holdings, Inc.*,

19 2009 WL 648983 (C.D. Cal. Mar. 9, 2009) 21

20 *Plevy v. Haggerty*,

21 38 F. Supp. 2d 816 (C.D. Cal. 1998) 9

22 *Plumley v. Sempra Energy*,

23 2021 WL 754841 (9th Cir. Feb. 26, 2021) 21

24 *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*,

25 759 F.3d 1051 (9th Cir. 2014) 17, 21

26 *Prodanova v. H.C. Wainwright & Co., LLC*,

27 993 F.3d 1097 (9th Cir. 2021) 20

28 *In re Qudian Inc. Sec. Litig.*,

 2019 WL 4735376 (S.D.N.Y. Sept. 27, 2019) 8

Reidinger v. Zendesk, Inc.,

 2021 WL 796261 (N.D. Cal. Mar. 2, 2021) 8, 16, 17, 23

TABLE OF AUTHORITIES
(Cont.)

Page(s)

1

2

3

4 *Retail Wholesale & Dep’t Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.,*

5 845 F.3d 1268 (9th Cir. 2017) 8

6 *Richman v. Goldman Sachs Grp., Inc.,*

7 868 F. Supp. 2d 261 (S.D.N.Y. 2012) 6

8 *In re Rigel Pharm., Inc. Sec. Litig.,*

9 697 F.3d 869 (9th Cir. 2012) 14

10 *Rok v. Identiv, Inc.,*

11 2017 WL 35496 (N.D. Cal. Jan. 4, 2017)..... 24

12 *Sgarlata v. PayPal Holdings, Inc.,*

13 409 F. Supp. 3d 846 (N.D. Cal. 2019)..... 8, 19, 20, 23

14 *In re Stratosphere Corp. Sec. Litig.,*

15 1997 WL 581032 (D. Nev. May 20, 1997) 13

16 *Swartzendruber v. Colony Capital, Inc.,*

17 2020 WL 7754008 (C.D. Cal. Dec. 10, 2020)..... 21

18 *Tellabs, Inc. v. Makor Issues & Rights, Ltd.,*

19 551 U.S. 308 (2007)..... 2, 15

20 *In re Twitter, Inc. Sec. Litig.,*

21 2020 WL 7260479 (N.D. Cal. Dec. 10, 2020) 10

22 *In re VeriSign, Inc., Deriv. Litig.,*

23 531 F. Supp. 2d 1173 (N.D. Cal. 2007)..... 16, 20

24 *In re Violin Memory Sec. Litig.,*

25 2014 WL 5525946 (N.D. Cal. Oct. 31, 2014) 9

26 *In re Wash. Public Power Supply Sys. Sec. Litig.,*

27 823 F.2d 1349 (9th Cir. 1987) 6

28 *Webb v. Solarcity Corp.,*

884 F.3d 844 (9th Cir. 2018) 21, 23

TABLE OF AUTHORITIES
(Cont.)

Page(s)

Zucco Partners, LLC v. Digimarc Corp.,
552 F.3d 981 (9th Cir. 2009) 8, 15

STATUTES

15 U.S.C. § 78t..... 25

15 U.S.C. § 78u-4 2, 7, 8, 14, 15, 16, 20, 25

RULES

Fed. R. Civ. P. 9..... 7, 13, 24

REGULATIONS

17 C.F.R. § 229.103..... 10

17 C.F.R. § 229.105..... 9

17 C.F.R. § 240.10b-5..... 6, 14, 25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I. INTRODUCTION

1
2 This case is the latest in a recent series of meritless lawsuits that accuse public
3 companies of securities fraud after they disclose an unforeseen data security incident
4 and suffer a stock price decline. This well-worn path is paved with dismissals. And for
5 good reason: Data security incidents are an unfortunate reality of modern business, and
6 it would be virtually unheard of for a corporation to represent that these incidents could
7 not occur or to try to deceive their investors into believing that. Defendants made no
8 such representations in this case, and the Complaint fails to plead otherwise.

9 On May 24, 2019, a blogger reported that documents containing information
10 belonging to customers of the title and escrow operations of First American Financial
11 Corp. (“First American” or the “Company”) allegedly were accessible through links
12 received by parties to real estate transactions. Upon being informed, First American
13 promptly shut down access to the information and conducted an investigation. The
14 investigation revealed that, out of 850 million images the blogger alleged were exposed,
15 32 customers’ non-public information may have been accessed without authorization.
16 First American notified those customers and offered them complimentary credit
17 monitoring services. More than a year later, First American disclosed that it had
18 received a Wells notice from the U.S. Securities and Exchange Commission (“SEC”)
19 notifying the Company that the enforcement staff was questioning the disclosures made
20 at the time of the security incident and had preliminarily decided to recommend filing
21 an enforcement action. Private plaintiffs then rushed to court and filed this lawsuit,
22 claiming that the ensuing temporary dip in First American’s stock price revealed that the
23 Company had defrauded investors.

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

1 Plaintiff's view is wrong. In 1995, Congress enacted the Private Securities
 2 Litigation Reform Act ("PSLRA") to curb abusive securities suits filed reflexively, and
 3 without credible evidence of fraud, when companies' stock prices declined. The PSLRA
 4 requires plaintiffs to allege with factual particularity which statements they claim are
 5 misleading and why. 15 U.S.C. § 78u-4(b)(1). It also requires them to plead a "strong
 6 inference" that the defendants perpetrated "each act or omission alleged" with scienter,
 7 i.e., a culpable state of mind embracing intentional or reckless deceit on investors. *Id.*
 8 § 78u-4(b)(2)(A). This unique pleading standard does not draw all inferences in favor
 9 of plaintiffs, but rather requires courts to balance the competing inferences of scienter
 10 and innocence. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 323–24
 11 (2007). Securities fraud claims can survive dismissal "only if a reasonable person would
 12 deem the inference of scienter cogent and at least as compelling as any opposing
 13 inference." *Id.* at 324. The Complaint does not satisfy these burdens.

14 **First**, the Complaint fails to plead any misstatement. What investors learned on
 15 May 24, 2019, is that First American—like every other company in the world—is
 16 susceptible to information security vulnerabilities. Defendants never said otherwise.
 17 And it would be absurd to assume otherwise, especially given that First American
 18 repeatedly cautioned investors that information security incidents, "regardless of their
 19 underlying causes, could ... result in the loss or unauthorized release, gathering,
 20 monitoring or destruction" of confidential customer information. ¶¶ 59, 76, 81.¹

21 Plaintiff strains to portray the occurrence of the incident as inconsistent with the
 22 Company's statements about the risks it faces, its information security program, and its
 23 commitment to safeguarding customer information. But First American never told
 24 investors that its systems were immune from vulnerabilities. And there is nothing
 25

26
 27 ¹ Citations in the form of "¶ __" or "¶¶ __" refer to the paragraphs of Plaintiff's
 28 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.

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

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

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

23 II. SUMMARY OF THE ALLEGATIONS

24 A. The Parties

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

1 The three “Individual Defendants” are First American officers. Mr. Gilmore is
2 the Company’s Chief Executive Officer and Director. ¶ 18. Mr. Seaton is the
3 Company’s Executive Vice President, Chief Financial Officer. ¶ 19. And Ms. Jalakian
4 is First American’s Senior Vice President, Chief Information Security Officer. ¶ 20.

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

8 **B. First American’s Image Repository, EaglePro, and the Company’s**
9 **Information Security Practices**

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

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

22 First American disclosed the importance of securing customer data (including its
23 image repository) and the potential for malicious actors or others to access customer
24 information without authorization. As the Company explained in its public filings,
25 information security is “critically important to its successful operation.” ¶ 57; *see also*
26 ¶¶ 63, 69, 74, 78–79, 85. First American warned investors that information security
27 incidents, “regardless of their underlying causes,” could “result in the loss or
28 unauthorized release, gathering, monitoring or destruction” of confidential customer

1 information. ¶ 59; *see also* ¶¶ 63, 69, 76, 78, 81, 85.² As the Company’s disclosures
 2 made clear, an information security incident could expose it to “lawsuits,” “adverse
 3 publicity,” and “governmental proceedings.” ¶ 83; *see also* ¶ 85.

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

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

17 **C. First American’s Investigation and Resolution of the Information Security**
 18 **Incident**

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

25
 26 ² *See also* Mendro Ex. 2 at 15–16 (“[U]nauthorized data disclosures may disrupt the
 27 Company’s business, harm the Company’s reputation, result in material claims for
 28 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).

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

4 Upon receiving notice of the vulnerability—and before Mr. Krebs published his
 5 article—First American immediately “shut down external access” to the image
 6 repository and remediated the vulnerability. ¶ 89; *see* ¶ 92. The Company also engaged
 7 an outside forensic firm to “asses[s] the extent to which any customer information may
 8 have been compromised.” ¶ 89. The investigation concluded that 32 customers of First
 9 American’s title and escrow operations had documents containing NPI that “likely were
 10 accessed without authorization.” ¶ 95; *see also* ¶ 97. First American notified those 32
 11 customers and “offered complimentary credit monitoring services.” ¶ 95. Although
 12 Plaintiff claims that more than 350,000 documents were accessed without authorization,
 13 it does not allege that any of those documents contained NPI beyond those related to the
 14 32 customers First American identified. *See* ¶¶ 44, 96, 98, 103.

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

22
 23
 24 ³ First American’s receipt of a Wells notice is unremarkable in itself and “does not
 25 necessarily indicate that charges will be filed” by the SEC; rather, it indicates only
 26 “that the staff of a government agency is considering making a recommendation.”
 27 *Richman v. Goldman Sachs Grp., Inc.*, 868 F. Supp. 2d 261, 272 (S.D.N.Y. 2012).
 28 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)).

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

3 **D. Plaintiff's Claims**

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

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

21 **III. ARGUMENT**

22 **A. The PSLRA Imposes Strict Pleading Standards.**

23 To state a Section 10(b) claim, a complaint must allege facts sufficient to establish
24 (1) a material misrepresentation or omission; (2) made with scienter; (3) in connection
25 with the purchase or sale of a security; (4) on which Plaintiff relied; (5) economic loss;
26 and (6) loss causation. *Loos v. Immersion Corp.*, 762 F.3d 880, 886–87 (9th Cir. 2014),
27 *as amended* (Sept. 11, 2014). A securities fraud complaint also must meet the stringent
28 pleading standards of Federal Rule of Civil Procedure 9(b) and the PSLRA, which

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

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

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

16 **1. Defendants’ Affirmative Statements Are True and Inactionable.**

17 **a. Risk Factor Disclosures**

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

21
 22 ⁴ With only a few easily distinguishable exceptions, the other cases that have attempted
 23 to premise securities fraud claims on a data security incident have been dismissed.
 24 *See Reidinger v. Zendesk, Inc.*, 2021 WL 796261 (N.D. Cal. Mar. 2, 2021)
 25 (dismissing Section 10(b) claim); *In re Fed Ex Corp. Sec. Litig.*, 2021 WL 396423
 26 (S.D.N.Y. Feb. 4, 2021) (same); *In re Alphabet, Inc. Sec. Litig.*, 2020 WL 2564635
 27 (N.D. Cal. Feb. 5, 2020) (same); *In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980
 28 (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.

1 factor disclosures, which the SEC instructs companies to include in their public filings,
2 are prospective “discussion[s] of the material factors that make an investment in the
3 [specific company] risky.” 17 C.F.R. § 229.105(a) (Reg. S-K, Item 105). In compliance
4 with this instruction, First American consistently disclosed, among other things, that
5 “the integrity of the Company’s computer systems and the protection of the information
6 that resides on those systems are critically important to its successful operation,” and
7 that cyber attacks and other external events, like natural disasters, “could disrupt the
8 Company’s business and could also result in the loss or unauthorized release, gathering,
9 monitoring or destruction of confidential, proprietary and other information pertaining
10 to the Company, its customers, employees, agents or suppliers.” ¶¶ 57, 59.

11 Risk-factor disclosures are “inactionable to the extent plaintiffs contend
12 defendants should have disclosed risk factors ‘are’ affecting financial results rather than
13 ‘may’ affect financial results” because they are “not meant to educate investors on what
14 harms are currently affecting the company.” *In re ChannelAdvisor Corp. Sec. Litig.*,
15 2016 WL 1381772, at *5 (E.D.N.C. Apr. 6, 2016) (quoting *Bondali v. Yum! Brands,*
16 *Inc.*, 620 F. App’x 483, 491 (6th Cir. 2015)), *aff’d sub nom. Dice v. ChannelAdvisor*
17 *Corp.*, 671 F. App’x 111 (4th Cir. 2016). Because “[a] reasonable investor would be
18 unlikely to infer anything regarding the *current* state” of First American’s cybersecurity
19 “from a statement intended to educate the investor on *future* harms,” Plaintiff’s
20 challenges to risk-factor disclosures fail. *Bondali*, 620 F. App’x at 491 (first emphasis
21 added); *see also In re Violin Memory Sec. Litig.*, 2014 WL 5525946, at *12 (N.D. Cal.
22 Oct. 31, 2014) (“[W]here a company’s filings contain abundant and specific disclosures
23 regarding the risks facing the company ... the investing public is on notice of these risks
24 and cannot be heard to complain that the risks were masked as mere contingencies.”
25 (quoting *Plevy v. Haggerty*, 38 F. Supp. 2d 816, 832 (C.D. Cal. 1998))).

26 Plaintiff claims that the Company’s risk-factor disclosures were “false and
27 misleading” because they did not disclose that “the Company failed to implement basic
28 security standards” and “disregarded its own information security policies,” and as a

1 result, “the Company did not protect but instead exposed tens of millions of documents
 2 containing sensitive customer NPI.” ¶¶ 58, 75, 80; *see also* ¶¶ 60, 77, 82. But Plaintiff
 3 does not allege that, at the time any of the challenged statements were made, First
 4 American was not in fact implementing basic security standards, that Defendants
 5 believed the Company was “disregard[ing]” its security policies, that the Company made
 6 any public assurances about compliance with its policies, or that those policies were
 7 even publicly disclosed.⁵ *See infra* pp. 15–23. Plaintiff’s contention that Defendants
 8 had to disclose that an information security incident “had ... already occurred” before
 9 they even learned that it occurred is nonsensical. *See, e.g.*, ¶ 47 (alleging that “the data
 10 exposure was **unquestionably unknown** to Defendants prior to December 2018”); ¶ 86
 11 (May 24, 2019 Krebs report “reveal[ed]” the information security incident); *see also In*
 12 *re Twitter, Inc. Sec. Litig.*, 2020 WL 7260479, at *8 (N.D. Cal. Dec. 10, 2020) (risk
 13 disclosures not misleading because “plaintiffs do not allege how [the company] could
 14 have failed to disclose in July that which had not happened until August at the earliest”).

15 It surely was not misleading for First American to warn investors, in its 2018
 16 annual report on Form 10-K, that “[i]f the Company fails to comply with applicable
 17 regulations and contractual requirements, it could be exposed to lawsuits, governmental
 18 proceedings or the imposition of fines, among other consequences.” ¶ 83. This
 19 statement was inarguably true. Plaintiff does not allege that any undisclosed lawsuit or
 20 government proceeding had been commenced against First American when this
 21 statement was made; to the contrary, Plaintiff admits that government proceedings
 22 commenced *after* the information security incident was revealed in May 2019.⁶ *See*
 23

24
 25 ⁵ Although Plaintiff claims that the Company did not timely remediate information
 26 security vulnerabilities (*see* ¶ 37), it does not allege that the Company made any
 27 contradictory public statements about its remediation policy (*see* ¶ 34) or disclosed
 28 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.

1 ¶¶ 8–9, 104. Thus, First American did not omit to disclose exposure to any “lawsuits,
2 government proceedings or the imposition of fines” that were ““already affecting”” it
3 and required to be disclosed in 2018. *Facebook*, 477 F. Supp. 3d at 1017–18.

4 **b. General Statements About First American’s Information
5 Security Program and Commitment to Protecting Data**

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

9 First American’s general commitments to safeguarding customer data are not
10 actionable because they are immaterial as a matter of law. *See, e.g.*, ¶¶ 61 (“We believe
11 we should behave responsibly when we use information We endeavor to educate the
12 users of our products and services ... about the importance of consumer privacy.”); 65
13 (Company is “serious” about the protection of consumer data); *see also* ¶¶ 64 (“The
14 objective of information security is to support the business and maximize stakeholder
15 benefit while protecting the information assets of both the Company and its customers
16 from all relevant threats.”); 99 (“[W]e already felt like we had strong information
17 security”). Numerous courts have recognized that “‘commitment’ statements are
18 inactionable puffery.” *In re Extreme Networks, Inc. Sec. Litig.*, 2018 WL 1411129, at
19 *23 (N.D. Cal. Mar. 21, 2018) (collecting cases); *Alphabet*, 2020 WL 2564635, at *4
20 (finding “generalized statements” about “Alphabet’s general commitment to ...
21 protection of [user] data ... inactionable puffery”); *Intel*, 2019 WL 1427660, at *9
22 (finding “vague positive statements” about security “immaterial as a matter of law”).

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

1 2009), First American “did not make any statements to the effect that the company’s
2 network was immune from security breaches or that no security breach had ever
3 occurred.” *See also Irving Firemen’s Relief & Ret. Fund v. Uber Techs.*, 2018 WL
4 4181954, at *7–8 (N.D. Cal. Aug. 31, 2018) (statements about commitment to data
5 security not actionable because “Defendants never claimed that [the company] would
6 never again suffer a data breach, nor does Plaintiff suggest as much”).

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

23 c. Statements About the Information Security Incident

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

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

8 Nor is there any inconsistency between Defendants’ statements that First
9 American’s investigation “identified imaged documents containing non-public personal
10 information pertaining to 32 consumers that likely were accessed without authorization”
11 (¶ 95; *see also* ¶ 97), and Plaintiff’s allegation that 350,000 documents were accessed
12 by automated “bots” or “scraper” programs (¶ 44). *See* ¶¶ 96, 98. As Plaintiff admits,
13 not all documents in the EaglePro application contained NPI (*see* ¶ 49), and Plaintiff
14 pleads no facts demonstrating that this information was present in *any* of the documents
15 allegedly accessed by non-human bots or scraper programs. *See In re Stratosphere*
16 *Corp. Sec. Litig.*, 1997 WL 581032, at *13 (D. Nev. May 20, 1997) (to plead falsity,
17 plaintiff must provide “evidentiary facts contemporary to the alleged false or misleading
18 statements from which this court can make inferences permissible under Rule 9(b)”).

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

1 customers' NPI was accessed without authorization. Nor does Plaintiff plead any facts
2 demonstrating that Defendant Seaton's statement on a July 23, 2020 earnings call, which
3 summarized a report by the Company's primary regulator (the Nebraska Department of
4 Insurance), mischaracterized the results of that report, or that the report did not conclude
5 that First American's "IT general controls environment is suitably designed and is
6 operating effectively," that the Company "adequately and appropriately detected,
7 analyzed, contained, eradicated and recovered from a security incident," and that it was
8 "in compliance with New York's cyber security requirements for financial services
9 companies." ¶¶ 102–03.

10 **2. Plaintiff Fails to Plead an Actionable Omission.**

11 Plaintiff also fails to meet the "high bar for [pleading] a materially misleading
12 omission[.]" *Lake v. Zogenix, Inc.*, 2020 WL 3820424, at *9–10 (N.D. Cal. Jan. 27,
13 2020). "Silence, absent a duty to disclose, is not misleading under Rule 10b–5." *Basic*
14 *Inc. v. Levinson*, 485 U.S. 224, 239 n.17 (1988). "To be actionable under the securities
15 laws, an omission must be misleading; in other words it must affirmatively create an
16 impression of a state of affairs that differs in a material way from the one that actually
17 exists." *Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002). Thus,
18 the PSLRA expressly requires plaintiffs to "specify each statement alleged to have been
19 misleading" as result of an omission. 15 U.S.C. § 78u-4(b)(1). "[A]s long as [any]
20 omissions do not make the actual statements misleading, a company is not required to
21 disclose" other facts "even if investors would consider the omitted information
22 significant." *In re Rigel Pharm., Inc. Sec. Litig.*, 697 F.3d 869, 880 n.8 (9th Cir. 2012).

23 Here, for the same reasons discussed above, nothing in the Complaint renders
24 First American's affirmative statements misleading. Plaintiff complains that Defendants
25 omitted to disclose that First American "failed to implement basic security standards,"
26 that the Company "disregarded its own information security policies," and that the
27 Company "lacked controls to properly classify or protect non-public information." *E.g.*,
28 ¶¶ 58, 60, 62, 66, 68, 71, 73, 75, 77, 80, 82. But Defendants had no duty to disparage

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

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

12 The PSLRA requires that a securities complaint “shall, with respect to each act or
 13 omission alleged to violate this chapter, state with particularity facts giving rise to a
 14 strong inference that the defendant acted with the required state of mind.” 15 U.S.C.
 15 § 78u-4(b)(2)(A). Pleading the “required state of mind” means alleging that “the
 16 defendants made false or misleading statements either intentionally or with deliberate
 17 recklessness.” *Zucco Partners*, 552 F.3d at 991. “[R]ecklessness only satisfies scienter
 18 under § 10(b) to the extent that it reflects some degree of intentional or conscious
 19 misconduct.” *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1053 (9th Cir. 2014). A
 20 strong inference of scienter exists “only if a reasonable person would deem the inference
 21 of scienter cogent and at least as compelling as any opposing inference one could draw
 22 from the facts alleged.” *Tellabs*, 551 U.S. at 324. “In reviewing a complaint under this
 23 standard, the court must consider *all* reasonable inferences to be drawn from the
 24 allegations, including inferences unfavorable to the plaintiffs.” *Metzler*, 540 F.3d at
 25 1061.⁷

26
 27
 28 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.

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

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

18 A sister court recently rejected similarly flawed claims in *Reidinger*. There, the
19 plaintiff challenged a company's "nondisclosure of its [supposed] failure to implement
20 certain security best practices" before a data security incident occurred. *Id.* at *9. The
21 court explained that the plaintiff's theory of scienter "[wa]s, at best, convoluted: [the]
22 officers did not know about a data breach, but chose to mislead investors ... by refusing
23 to disclose past security mistakes, while nonetheless disclosing that [the company] might
24 have suffered an undetected breach." *Id.* at *10. So, too, here: The Complaint admits
25 that the data security incident "was unquestionably unknown to Defendants" before
26 December 2018. ¶ 47. And there are no factual allegations that Defendants knew about
27 purported security vulnerabilities and "also consciously disregarded a risk that these
28

1 [vulnerabilities] made [the Company’s] general statements about data security ...
2 misleading.” *Reidinger*, 2021 WL 796261, at *9.

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

9 **1. Plaintiff’s Second-Hand Accounts of Contemporaneous Documents Do**
10 **Not Support an Inference of Scienter.**

11 The Complaint rests largely on documents Plaintiff never saw but presumably
12 read about in the NYDFS Amended Statement of Charges. None of Plaintiff’s second-
13 hand accounts of these contemporaneous “internal records” (*see* ¶¶ 35–37) supports an
14 inference of scienter. Plaintiff fails to “link[]” those records “and their contents to the
15 [defendant] executives,” *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d
16 1051, 1063 (9th Cir. 2014), or plead how they bear on Defendants’ state of mind
17 regarding the specific statements challenged in the Complaint.

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

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

4 Plaintiff also claims “Defendants were fully aware” after April 2018 that the
5 Company’s method of classifying documents “failed to identify and protect documents
6 containing [personal data]” (¶ 49), but the Complaint contains no allegations specific to
7 any Individual Defendant. Plaintiff does not allege, for example, that the single “June 1,
8 2019 email from First American’s Vice President of Information Security” was even
9 sent to—let alone received, read, and agreed with by—any Defendant. ¶ 49(ii).

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

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

1 to “place great weight on a ‘preliminary’ finding” that a company had infringed the
2 European Commission Treaty). In any event, alleged knowledge of weaknesses in
3 vulnerability management is not the same as knowledge of errors in the Company’s
4 public disclosures.

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

12 **2. Plaintiff’s Confidential Witness Allegations Fail to Plead Scienter.**

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

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

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

11 **3. The Individual Defendants’ Positions Do Not Support an Inference of** 12 **Scienter.**

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

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

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

3 **4. The Core Operations Doctrine Does Not Apply.**

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

14 The Complaint does not come close to pleading the facts necessary for the core
15 operations doctrine to apply. Plaintiff alleges no “specific admissions by [Defendants]
16 of detailed involvement in the minutia of [the Company’s] operations” or any “witness
17 accounts demonstrating that they had actual involvement in creating false reports” to
18 investors. *Police Ret. Sys. of St. Louis*, 759 F.3d at 1062; *see Webb v. Solarcity Corp.*,
19 884 F.3d 844, 857 (9th Cir. 2018) (rejecting invocation of core operations doctrine where
20 plaintiff failed to allege defendants “were involved in accounting decisions as minute”
21 as those relevant to challenged statements). Nor has Plaintiff alleged facts supporting
22 the inference that the data security incident “was so dramatic that it would be *absurd* to
23 think that Defendants[] did not know” about it. *Webb*, 884 F.3d at 857. “Thus, the core
24 operations doctrine does not apply.” *Swartzendruber*, 2020 WL 7754008, at *6; *see*
25 *Pittleman v. Impac Mortg. Holdings, Inc.*, 2009 WL 648983, at *3 (C.D. Cal. Mar. 9,
26 2009) (“vague allegations of [company guideline] violations are not one of th[o]se
27 ‘exceedingly rare’ cases” that trigger application of the core operations doctrine), *aff’d*
28 *sub nom. Sharenow v. Impac Mortg. Holdings, Inc.*, 385 F. App’x 714 (9th Cir. 2010).

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

3 Plaintiff suggests that the five-month “delay” between the EaglePro penetration
 4 test in December 2018 and the disclosure of the information security incident in May
 5 2019 was motivated by an intent to mislead investors. *See* ¶¶ 4, 91. Plaintiff’s
 6 description of the timeline is misleading. The Complaint admits Defendants
 7 “unquestionably” lacked knowledge of the data security incident before December
 8 2018—nearly two years after the start of the Class Period and after most statements
 9 challenged in the Complaint. ¶ 47. Although the Complaint implies that the Individual
 10 Defendants learned about the exposure of personal data in December 2018 (*see* ¶¶ 4,
 11 91), it alleges only that a “test team” conducted a penetration test of the EaglePro
 12 application to identify the existence of security vulnerabilities (¶ 47). And it does not
 13 allege that any Individual Defendant received or reviewed the resulting report in January
 14 2019, which would not have revealed the exposure of NPI in any event. *Id.* ¶ 48 (report
 15 “acknowledged that further investigation was ... required to determine whether sensitive
 16 documents were exposed”). “[E]ven if there were a handful of lower-level employees”
 17 who were concerned in December 2018 about the possibility that documents containing
 18 personal data had been exposed or accessed, “[t]here is nothing in the Complaint that
 19 supports an inference that these concerns were ... relayed to any of the Defendants.”
 20 *Heartland Payment Sys.*, 2009 WL 4798148, at *8.

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

27 **6. The Countervailing Inferences of Innocence Are Overwhelming.**

28 After considering the negative inferences that can be drawn from Plaintiff’s
 largely irrelevant allegations, this Court must “comparatively weigh” them against the

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

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

10 **Second**, the Complaint admits that First American filed with the SEC a current
11 report on Form 8-K on the first business and trading day after publication of the Krebs
12 report. *See* ¶¶ 86–89. And it admits that the Company launched an immediate
13 investigation when it was alerted to the potential unauthorized access of personal data.
14 ¶¶ 89, 95, 97. These allegations “demonstrat[e] a pursuit of truth rather than reckless
15 indifference to the truth.” *Higginbotham v. Baxter Int’l, Inc.*, 495 F.3d 753, 758 (7th
16 Cir. 2007).

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

24 **7. Plaintiff Fails to Plead Corporate Scienter.**

25 “[A] corporation can only act through its employees and agents and can likewise
26 only have scienter through them.” *In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d
27 471, 475 (9th Cir. 2015). Because Plaintiff fails to plead scienter as to any Individual
28 Defendant, it fails to plead scienter as to First American.

1 **D. Plaintiff Fails to Plead Loss Causation.**

2 The Complaint must be dismissed on the independent ground that Plaintiff fails
3 to plead loss causation. To plead loss causation with the particularity required by Rule
4 9(b), a plaintiff “must demonstrate that an economic loss was caused by the defendant’s
5 misrepresentations, rather than some other intervening event” or “other fact.” *Lloyd v.*
6 *CVB Fin. Corp.*, 811 F.3d 1200, 1209–10 (9th Cir. 2016). When a securities fraud
7 plaintiff relies on a “revelation of the fraud” theory of loss causation, the plaintiff must
8 plead that (1) she purchased a security at a price that was artificially inflated by a specific
9 alleged misstatement; (2) a “corrective disclosure” subsequently revealed the “truth”
10 about that specific misstatement; and (3) the disclosure of the truth caused the
11 company’s stock price to decline. *Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 342–43,
12 346–47 (2005); *In re BofI Holding, Inc. Sec. Litig.*, 977 F.3d 781, 790 (9th Cir. 2020).

13 A corrective disclosure “must by definition reveal new information to the
14 market.” *In re BofI*, 977 F.3d at 794; *accord Rok v. Identiv, Inc.*, 2017 WL 35496, at
15 *18 (N.D. Cal. Jan. 4, 2017). “[T]he announcement of an investigation, without more,
16 is insufficient to establish loss causation.” *Loos*, 762 F.3d at 890. This is because, “at
17 the moment an investigation is announced, the market cannot possibly know what the
18 investigation will ultimately reveal.” *Id.* Announcing an investigation “simply puts
19 investors on notice of a *potential* future disclosure of fraudulent conduct.” *Id.*

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

1 thus preventing reflexive lawsuits at that time. *See* Mendro Ex. 1; 15 U.S.C. § 78u-
 2 4(e)(1) (limiting damages to the difference between plaintiff’s purchase or sale price and
 3 the mean trading price of the stock in the 90-day period after the alleged corrective
 4 disclosure). Accordingly, Plaintiff fails to plead loss causation.

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

6 Ms. Jalakian cannot be liable for the vast majority of statements Plaintiff disputes.
 7 Only “the person or entity with ultimate authority over [a] statement, including its
 8 content and whether and how to communicate it” can be liable under Rule 10b-5. *Janus*
 9 *Capital Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 142 (2011). The Complaint
 10 alleges that only Messrs. Gilmore and Seaton signed First American’s public reports
 11 (¶¶ 18–20), and it admits that Ms. Jalakian “had the power and authority to control [only]
 12 the contents of the information and statements *attributed to her*” (¶ 23). Plaintiff’s claim
 13 against Ms. Jalakian must, at minimum, be dismissed to the extent it is based on any
 14 statement other than the two attributed to her.⁸ *See* ¶¶ 64–65, 72.

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

16 Count II of the Complaint asserts a claim against Messrs. Gilmore and Seaton for
 17 “control person” liability under Section 20(a) of the Exchange Act. ¶¶ 124–30; *see* 15
 18 U.S.C. § 78t(a). To plead a Section 20(a) claim, a plaintiff “must show that a primary
 19 violation was committed and that the defendant directly or indirectly controlled the
 20 violator.” *Paracor Fin., Inc. v. Gen. Elec. Capital Corp.*, 96 F.3d 1151, 1161 (9th Cir.
 21 1996). Because Plaintiff has failed to allege a primary violation of Section 10(b), its
 22 Section 20(a) claims also fail. *NVIDIA Corp.*, 768 F.3d at 1052.

23 **IV. CONCLUSION**

24 For the foregoing reasons, the Complaint should be dismissed.

25
 26
 27
 28 ⁸ Ms. Jalakian also cannot be liable for these two statements because neither is false or
 misleading. *See supra* pp. 8-15.

1 Dated: May 21, 2021

2 GIBSON, DUNN & CRUTCHER LLP
3 CRAIG VARNEN
4 JASON J. MENDRO
5 COLIN B. DAVIS

6 By: /s/ Jason J. Mendro
7 Jason J. Mendro

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

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28