

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

RONALD SGARLATA, et al.,

Plaintiffs,

v.

PAYPAL HOLDINGS, INC., et al.,

Defendants.

Case No. [17-cv-06956-EMC](#)

**ORDER GRANTING DEFENDANTS'
MOTION TO DISMISS SECOND
AMENDED COMPLAINT**

Docket No. 79

Defendants PayPal Holdings, Inc., TIO Networks ULC, TIO Networks USA, Inc., Daniel H. Schulman, John D. Rainey, Jr., and John Kunze (collectively, “Defendants”) move to dismiss Plaintiffs Michael Eckert and Edwin Bells’ (“Plaintiffs”) second amended complaint (“SAC”). Plaintiffs bring this action individually and on behalf of all others who purchased PayPal securities between November 10, 2017 and December 1, 2017 (the “Class Period”). Plaintiffs claim that they purchased PayPal securities at allegedly inflated prices during the Class Period. The Court previously dismissed Plaintiffs’ first amended complaint (“FAC”) with leave to amend. Docket No. 78. The SAC continues to allege claims for relief against Defendants under 10(b), 10b–5, and 20(a).¹

Pending before the Court is Defendants’ Motion to Dismiss (“Mot.”) the SAC pursuant to Federal Rules of Civil Procedure Rule 12(b)(6), Rule 9(b), and the Private Securities Litigation Reform Act (“PSLRA”). Docket No. 79.

¹ In contrast with the FAC, Plaintiffs have not named Hamed Shahbazi (who served as Vice President of Bill Pay for PayPal during the Class Period) as a defendant.

I. BACKGROUND

A. Factual Background²

“On February 14, 2017, PayPal announced an agreement to purchase TIO Networks Corporation for \$233 million.” *Id.* ¶ 3. “TIO is a bill-pay management company that processed roughly \$7 billion in bill payments on behalf of fourteen (14) million customers in 2016.” *Id.*

Plaintiffs’ claims arise from press releases that they allege were materially misleading. On November 10, 2017, Defendants TIO and PayPal issued press releases (the “November Announcement”). The November Announcement read as follows:

PayPal Holdings, Inc. (Nasdaq: PYPL) announced that TIO Networks (TIO), a publicly traded company PayPal acquired in July 2017, has suspended operations to protect TIO’s customers. This suspension of services is a result of PayPal’s discovery of security vulnerabilities on the TIO platform and issues with TIO’s data security program that do not adhere to PayPal’s information security standards. TIO is not integrated into PayPal’s platform. The PayPal platform is not impacted by this situation in any way and PayPal’s customers’ data remains secure.

Upon the recent discovery of this vulnerability on the TIO platform, PayPal took action by initiating an internal investigation of TIO and bringing in additional third-party cybersecurity expertise to review TIO’s bill payment platform. A focus of the investigation will also include TIO’s practices and representations prior to the acquisition.

Concurrent with this press release in November, TIO posted the following statement on its website:

On Friday, November 10, 2017, TIO Networks suspended our operations due to the discovery of security vulnerabilities on the TIO platform and issues with TIO’s data security program. While we apologize for any inconvenience this suspension of services may cause, the security of TIO’s systems and the protection of TIO’s customers are our highest priorities. We are actively investigating this situation and working with appropriate authorities to safeguard TIO customers.

TIO also sent the following message to some of its customers:

On November 10, PayPal announced that TIO Networks, a publicly traded company that PayPal acquired in July 2017, suspended operations to protect TIO’s customers. This suspension of services is a result of PayPal’s discovery of security vulnerabilities on the

² The facts between the FAC and the SAC are largely unchanged, with minor amendments.

TIO platform and issues with TIO's data security program that do not adhere to PayPal's information security standards.

FAC ¶ 40. Then, on December 1, 2017, TIO and PayPal released a statement disclosing that, in fact, a breach had occurred and that the confidential information of 1.6 million users had been potentially compromised. *Id.* ¶ 5. The press release dated December 1, 2017 (the "December Announcement"), read as follows:

PayPal Holdings, Inc. (Nasdaq: PYPL) today announced an update on the suspension of operations of TIO Networks (TIO), a publicly traded payment processor PayPal acquired in July 2017. A review of TIO's network has identified a potential compromise of personally identifiable information for approximately 1.6 million customers. The PayPal platform is not impacted in any way, as the TIO systems are completely separate from the PayPal network, and PayPal's customers' data remains secure.

As announced on November 10, PayPal suspended the operations of TIO to protect customer data as part of an ongoing investigation of security vulnerabilities of the TIO platform. This ongoing investigation has identified evidence of unauthorized access to TIO's network, including locations that stored personal information of some of TIO's customers and customers of TIO billers. As a result, PayPal is taking steps to protect affected customers.

TIO has also begun working with the companies it services to notify potentially affected individuals, and PayPal is working with a consumer credit reporting agency to provide free credit monitoring memberships. Individuals who are affected will be contacted directly and receive instructions to sign up for monitoring.

Defendants' Request for Judicial Notice, Ex. E.³ The following trading day, December 4, 2017, PayPal's share price dropped \$4.33 (5.75%) and closed at \$70.97. SAC ¶ 40.

Plaintiffs contend the November Announcement failed to fully disclose the seriousness of the security breach. *Id.* ¶ 30. Instead, Plaintiffs assert that Defendants were aware of an alleged breach of TIO's security that exposed the personal information of TIO's customers, bill-pay clients, and employees. *Id.* Plaintiffs argue this omission was materially misleading. They assert the drop in price following the December Announcement, which disclosed the potential

³ The Court **DENIES** Defendants' RJN as to Exhibits A and B as moot because these exhibits are not relevant to resolving this motion. The Court **GRANTS** Defendants' RJN as to Exhibits C, D, and E as incorporated by reference because Plaintiffs referenced them throughout the SAC, and they form the basis for Plaintiffs' claims. Notice is taken of the fact that the announcements were released, but not for the truth of the statements therein.

compromise of 1.6 million users' data, caused the loss in stock value suffered by Plaintiffs.

In asserting their claims of securities fraud by Defendants, Plaintiffs rely primarily on three confidential former employees' ("FE") statements. Below are the statements from the three FEs, and how their statements in the SAC were amended from the FAC:

1. Former Employee 1

FE1 was a Support Operations Manager at TIO from February 2016 to March 2018, and reported to Senior Vice-President of Operations at TIO. FE1 learned of the breach on November 10, 2017 when FE1 and colleagues received an email around 3 p.m. inviting them to a special meeting. They learned that TIO would be shut down and were told that someone had access to confidential information for customers. *FE1 was informed at the special meeting that someone had accessed the names and addresses for customers as well as employees' information, including gender, social security, numbers, and dates of birth. FE1 also recalled that they were informed at that meeting that the intruder had accesses confidential customer information, and that PayPal said someone had tools and had accessed confidential information, which was sitting in the TIO Networks' servers.*

SAC ¶ 31 (emphasis added to illustrate amendment).

2. Former Employee 2

FE2 was a contract Senior Systems Administrator at TIO Networks in Vancouver from September 2017 to February 2018, reporting to TIO IT Manager Mike McKenzie. FE2 stating that in early November while waiting for an all-hands TIO meeting in their conference room FE2 was summoned back to a different office to hear an announcement from Kunze, telling that TIO had actually been breached. FE2 states that PayPal discovered the breach during a security analysis of the TIO network, and that when they were doing so, they discovered someone in the system. *Immediately after Kunze informed FE2 of the breach, the network team immediately severed the link between the corporate and production side of the network, the latter of which being where sensitive customer information was stored, in an attempt to minimize harm to customers. FE2 understood the decision to sever ties between the two halves of the network to demonstrate a serious concern that TIO's customer information was in jeopardy or already had been compromised.*

SAC ¶ 33 (emphasis added to illustrate amendment).

3. Former Employee 3

FE3 was Senior .NET Developer for TIO from January 2010 until April 1, 2018, who designed, implemented and maintained the billing and payment systems for TIO. FE3 also performed

integrations between clients' application programming interfaces and TIO's server. *FE3 stated that employees* of TIO learned of a security *breach* in early November when TIO announced it had discovered a vulnerability. It was FE3's understanding that this was also the time the breach was discovered.

SAC ¶ 34 (emphasis added to illustrate amendment). Plaintiffs assert that the FE statements, as amended, demonstrate that Defendants knew at the time of the November Announcement that it was materially misleading.

B. Procedural Background

Plaintiffs filed this action on December 6, 2017. Docket No. 1. On March 15, 2018, the Court appointed Michael Eckert and Edwin Bell as interim co-lead plaintiffs. Docket No. 31. Plaintiffs filed their FAC on June 13, 2018. Docket No. 57. Thereafter, Defendants filed motions to dismiss the FAC. Docket Nos. 59, 61. The Court dismissed the FAC with leave to amend. Docket No. 75. Plaintiffs filed their SAC on January 14, 2019. Docket No. 76.

II. LEGAL STANDARDS

A. Rule 12(b)(6)

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), a plaintiff's "factual allegations [in the complaint] 'must . . . suggest that the claim has at least a plausible chance of success.'" *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But "allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself

effectively.” *Levitt*, 765 F.3d at 1135 (internal quotation marks omitted).⁴ “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (internal quotation marks omitted).

B. Rule 9(b) and the Private Securities Litigation Reform Act (“PLSRA”)

The PSLRA imposes additional pleading requirements. *Ronconi v. Larkin*, 253 F.3d 423, 429 (9th Cir. 2001). “In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake.” Fed. R. Civ. P. 9(b). In order to “properly allege falsity, a securities fraud complaint must now ‘specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, . . . state with particularity all facts on which that belief is formed.’” *In re Rigel Pharm., Inc. Sec. Litig.*, 697 F.3d 869, 876–77 (9th Cir. 2012) (quoting 15 U.S.C. § 78u–4(b)(1)) (marks of omission in original).

Scienter must also be pled with greater particularity. For a private securities fraud complaint to survive a Rule 12(b)(6) motion to dismiss, pleadings must raise a “strong inference” that Defendants made misleading statements to investors knowingly or with deliberate recklessness. *Ronconi*, 253 F.3d at 429. In particular, a “plaintiff may recover money damages only on proof that the defendant acted with a particular state of mind, the complaint shall, with respect to each act or omission alleged to violate [section 10(b)], state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind.” 15 U.S.C.A. § 78u–4. The term scienter for the purposes of section 10(b) “refers to a mental state embracing intent to deceive, manipulate, or defraud.” *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 193 n.12 (1976). A plaintiff must show that “the defendants made false or misleading statements either intentionally or with deliberate recklessness.” *Zucco Partners, LLC v. Digimarc Corp.*, 552

⁴ A court “need not . . . accept as true allegations that contradict matters properly subject to judicial notice or by exhibit.” *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001).

F.3d 981, 991 (9th Cir. 2009), *as amended* (Feb. 10, 2009). Plaintiffs’ assertion of a strong inference of scienter “must be more than merely plausible or reasonable—it must be cogent and at least as compelling as any opposing inference of nonfraudulent intent.” *Tellabs, Inc. v. Makor Issues & Rights, Ltd.* 551 U.S. 308, 314 (2007). When evaluating scienter, a court must “engage in a comparative evaluation,” and must consider “not only inferences urged by the plaintiff,” but the court must also consider “competing inferences rationally drawn from the facts alleged.” *Id.*

“Section 10(b) of the Securities Exchange Act of 1934 makes it unlawful for ‘any person . . . [t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.’” *Zucco Partners, LLC*, 552 F.3d at 990 (quoting 15 U.S.C. § 78j(b)) (internal quotation marks omitted) (alterations in original).

Rule 10b–5 states:

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

17 C.F.R. § 240.10b–5. “The SEC promulgated Rule 10b–5 pursuant to authority granted under § 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b). Although neither Rule 10b–5 nor § 10(b) expressly creates a private right of action, [the Supreme] Court has held that ‘a private right of action is implied under § 10(b).’” *Janus Capital Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 141–42 (2011) (quoting *Superintendent of Ins. of N.Y. v. Bankers Life & Casualty Co.*, 404 U.S. 6, 13, n. 9 (1971)).

To succeed on a claim under section 10(b) and Rule 10b–5, a plaintiff must show: “(1) a material misrepresentation or omission; (2) scienter; (3) a connection between the

misrepresentation or omission and the purchase or sale of a security; (4) reliance; (5) economic loss; and (6) loss causation.” *Oregon Pub. Employees Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 603 (9th Cir. 2014) (citing *Stoneridge Inv. Partners, LLC v. Scientific–Atlanta, Inc.*, 552 U.S. 148, 157 (2008)). A complaint asserting claims under section 10(b) and Rule 10b–5 “must satisfy the dual pleading requirements of Federal Rule of Civil Procedure 9(b) and the PSLRA.” *Zucco Partners, LLC*, 552 F.3d at 990.

III. DISCUSSION

A. A Material Misrepresentation or Omission: Falsity

The Court previously found that Plaintiffs’ claims satisfied the pleading requirements for falsity. Docket No. 75 (the November Announcement “could plausibly have created an impression that only a potential vulnerability and not an actual breach had been discovered, and certainly not one which threatened the privacy of 1.6 million users.”). Defendants request the Court to reconsider its previous ruling, Mot. at 17, while claiming, alternatively, that they are not bound by the findings relating to an inoperative complaint. Reply at 3. Plaintiffs claim that the Court need not revisit the prior finding because the falsity argument remains unchanged from the FAC to the SAC. Opp. at 22. Defendants cite to *Askins v. U.S. Department of Homeland Security*, 899 F.3d 1035, 1043 (9th Cir. 2018), which holds that the “district court may decide the second motion to dismiss in the same way it decided the first, but permitting the filing of an amended complaint requires a new determination.”

As with the FAC, the alleged false, misleading statement arises from the November Announcement. SAC ¶¶ 39–41. Here, Defendants set forth the same arguments against falsity as they did in their prior motion to dismiss. *Compare* Mot. at 17–18, *with* Docket No. 61 at 7–10. Specifically, they claim that the November Announcement must be “necessarily inconsistent” with the subsequent December Announcement. Reply at 2.

To prove falsity for the purposes of Section 10(b) and Rule 10b–5, Plaintiffs must “specify each statement alleged to have been misleading, [and] the reason or reasons why the statement is misleading.” 15 U.S.C. § 78u–4(b)(1). As this Court concluded in its earlier ruling, a literally true statement “can be misleading and thus actionable under the securities laws.” *Brody v.*

1 *Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002) (citing *In re GlenFed Sec. Litig.*, 42
2 F.3d 1541, 1551 (9th Cir. 1994)). “To be actionable under the securities laws, an omission must
3 be misleading; in other words, it must affirmatively create an impression of a state of affairs that
4 differs in a material way from the one that actually exists.” *Id.* (citing *McCormick v. The Fund*
5 *American Cos.*, 26 F.3d 869, 880 (9th Cir. 1994)).

6 Plaintiffs’ contention was, and still is, that the November Announcement was false and
7 misleading “because they disclosed only a security vulnerability, rather than an actual security
8 breach *that potentially compromised all 16 million TIO customers*, which PayPal and TIO did not
9 acknowledge had been detected” SAC ¶ 42 (emphasis added). Specifically, Plaintiffs allege
10 “that an unknown but unauthorized person or entity was at that time logged in to TIO’s networks
11 and had access to the financial information of 1.6 million users.” *Id.* ¶ 4.⁵ Defendants continue to
12 argue that the November Announcement was consistent with the December Announcement—*i.e.*,
13 that the prior announcement disclosing the investigation of vulnerabilities was not inconsistent
14 with the subsequent announcement revealing an actual security breach. Mot. at 18.

15 As the Court found in its previous order, Defendants’ November Announcement purported
16 to disclose a “vulnerability” in TIO’s security, which triggered an investigation and review. This
17 disclosure could plausibly have created an impression that only a potential vulnerability and not an
18 actual breach had been discovered, and a vulnerability differs considerably from a breach that
19 actually threatens the privacy of 1.6 million users. *See Berson v. Applied Signal Tech., Inc.*, 527
20 F.3d 982, 987 (9th Cir. 2008) (finding that “[i]t goes without saying that investors would treat” a
21 risk and a certainty differently). Notwithstanding the December Announcement being
22 “corrective” and “not inconsistent,” the November Announcement could reasonably have created a
23 false impression that had the effect of misleading investors.

24 At the hearing, Defendants argued that plausibility is not sufficient for a finding of
25 falsity—*i.e.*, the heightened pleading standard applies to the false and misleading statement as well
26 as the scienter. *See Brody*, 280 F.3d 997 (“[i]n order to survive a motion to dismiss under the

27
28 ⁵ Apparently there are 16 million bill pay accounts that TIO served, but 1.6 million is the number
of customers whose accounts were compromised.

heightened pleading standards of the [PLSRA], the plaintiffs' complaint must specify the reason or reasons why the statements made by [the defendant] were misleading.”). But even so, the result is the same because Plaintiffs have specifically pled, with detail, why the November Announcement was misleading—*e.g.*, because current or potential investors understood the security vulnerability to be minor. *See* SAC ¶¶ 39–41. Accordingly, Plaintiffs have again adequately pled a misleading statement.

B. Scienter and Loss Causation

To survive a motion to dismiss, however, Plaintiffs must also demonstrate with particularity that the speaker (here, Mr. Kunze) made the misleading statement with a guilty state of mind. Here, scienter is premised on Plaintiffs’ argument that a holistic view of the SAC supports their allegation that Defendants, particularly Mr. Kunze, knew of an actual data breach and compromise of the privacy of millions of customers at the time of the November Announcement; Plaintiffs’ loss-causation theory relies on the fact that when the public learned about the actuality of the breach and its severity (affecting 1.6 million customers), the price of PayPal’s stock dropped 5.75%.

To succeed under the loss-causation theory alleged in the SAC, Plaintiffs must satisfy the heightened pleading requirements for scienter—specifically, that Defendants knew not only of a vulnerability but an actual breach which compromised the privacy of 1.6 million customers. *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quoting *In re Daou Sys., Inc.*, 411 F.3d 1006, 1014 (9th Cir.2005)) (recognizing that a plaintiff must “demonstrate a causal connection between the deceptive acts that form the basis for the claim of securities fraud and the injury suffered by the plaintiff”).

Plaintiffs continue to rely on three former employees of TIO to support a showing of scienter. SAC ¶¶ 30–35. In addition to these employees, Plaintiffs now also rely on the statements of a cybersecurity expert they engaged to “review[] PayPal’s and TIO’s public statements on November 10 and December 1, confidential witness statements set forth in [the SAC], and publicly available information concerning TIO’s breach.” SAC ¶ 36.

1. Former TIO employees

The Court previously dismissed the FAC when it found the FE statements failed to satisfy the scienter requirement because they showed “at most [] that some of the Defendants may have known that there was some breach in TIO’s platform. They do not substantiate allegations that Defendants on November 10, 2017, ‘determined that an unknown but unauthorized person or entity was at that time logged in to TIO’s networks *and had access to the personal financial information of 1.6 million users.*’” Docket No. 70 (emphasis in original).

As such, most of the SAC’s amendments are based on the amended FE statements. Confidential witness statements can create a strong inference of scienter only if the reporting witness has “reliable personal knowledge of the defendants’ mental state.” *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 998 (9th Cir. 2009), *as amended* (Feb. 10, 2009). 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. *Id.* at 994 (citing *In re Daou Sys., Inc.*, 411 F.3d 1006, 1015–16, 1022 (9th Cir. 2005)). Therefore, for the FEs to support the necessary finding of scienter, the FEs’ statements must demonstrate with reliable facts creating a “strong inference” that Mr. Kunze knew of or recklessly disregarded the breach, the magnitude of which could have affected 1.6 million customers.

a. Former Employee 1

FE1 stated she learned of the breach on November 10, 2017, when she received an e-mail around 3:00 p.m., inviting her to a special meeting where she and other employees “were told that someone had access to confidential information for customers.” SAC ¶ 31. Plaintiffs further allege that “FE1 ***was informed*** at the special meeting that someone had accessed the names and addresses for customers as well as employees’ information, including gender, social security numbers, and dates of birth. FE1 also recalled that ***they were informed*** at the meeting that the intruder had accessed confidential customer information, and that ***PayPal said*** someone had tools and had accessed confidential information, which was sitting in the TIO Networks’ servers.” *Id.* (emphasis added). Accordingly, because of this, FE1 “understood the breach had potential to

1 impact all TIO customers and all TIO employees—everyone whose personal information was
2 stored on its servers.” *Id.* (emphasis removed).

3 Like FE1’s statements in the FAC, FE1’s recounting of the events in the SAC still fails to
4 show that **Mr. Kunze knew**, by the November Announcement, that someone had compromised the
5 data of 1.6 million TIO customers. No statement is attributed to Mr. Kunze or any of the other
6 individual defendants. Nor do the alleged statements made at the meeting show that the individual
7 defendants knew the breach had compromised the records of 1.6 million customers. FE1’s
8 statement is made more problematic by the fact that the amended statement is inconsistent with
9 FE1’s prior statement. Previously, FE1 is quoted as stating that “they suspected or saw” that
10 someone had access to customer data (FAC ¶ 32), which is materially different than “they were
11 informed” of the intrusion (SAC ¶ 31). There is a distinct difference in degree of certainty and, by
12 implication, the depth of the company’s knowledge regarding the breach. This discrepancy raises
13 credibility concerns about FE1. *See Zucco*, 552 F.3d at 995 (reliability and personal knowledge
14 must be satisfied in the first prong of the two-part test); *In re Maxwell Techs., Inc. Sec. Litig.*, 18
15 F. Supp. 3d 1023, 1034 (S.D. Cal. 2014) (a court must “examine the witnesses for indicia of
16 reliability and personal knowledge . . .”).

17 In sum, FE1’s statements fail for three reasons. First, that an unknown individual informed
18 FE1 at a special meeting of a breach of confidential information, and that “PayPal said someone
19 had tools and had accessed confidential information” fails to show specifically who at PayPal
20 informed FE1 of the breach or what the individual said. In particular, the SAC fails to connect the
21 dots as to who informed her of the breach at the specially-called meeting, or why the unknown
22 individual felt obliged to report the breach to FE1 in her role as a Support Operations Manager.
23 Second, nearly all the amendments to FE1’s summary relies on hearsay (*e.g.*, she was informed by
24 an unnamed person at PayPal and informed by an unnamed person at the meeting), which the
25 Court must weigh against reliability when considering scienter. *See Zucco*, 552 F.3d at 998, n. 4
26 (hearsay statements relied upon by confidential witnesses may not be sufficiently reliable,
27 plausible, or coherent to warrant further consideration of proving the scienter requirement).
28 Lastly, as discussed in above, FE1’s memory of the meeting in the FAC contradicts her account in

the SAC. *Compare* FAC ¶ 32 (“they suspected or saw that someone had access to customer data . . .” and that “[t]hey shut down service to complete the investigation.”); *with* SAC ¶ (“[we] were informed at the special meeting that someone had accessed the names and addresses for customers as well as employees’ information . . . and that PayPal said someone had tools and had accessed confidential information . . .”).

Plaintiffs argue that this Court previously credited the FEs’ statements as reliable. This is not so—the Court never opined on the reliability of the FE statements. The Court’s prior decision assumed *arguendo* that the statements “at most establish that some of the Defendants may have known that that there was some breach in TIO’s platform. They do not substantiate allegations that Defendants on November 10, 2017, ‘determined that an unknown but unauthorized person or entity was at the time logged into TIO’s networks and had access to personal information of 1.6 million users.’” Docket No. 75 at 11. FE1’s amended statement remain deficient.

In particular, the statement on its face do not show—let alone mention—that Mr. Kunze had knowledge of a breach affecting 1.6 million customers and used that knowledge (or recklessly disregarded it) to deceive the market. Yet, Plaintiffs must allege Mr. Kunze’s scienter because he is the only alleged speaker relative to the November Agreement. *See* Declaration of Ludwig, Exhibit A, at 15:21–22 (“That’s right, Your Honor. And let’s be specific. Scienter has to be to Mr. Kunze, who’s the only alleged speaker.”). FE1’s statements are not sufficiently indicative of scienter.⁶

⁶ Plaintiffs cite *S. Ferry LP #2 v. Killinger*, 687 F. Supp. 2d 1248, 1254 (W.D. Wash. 2009) for the proposition that a complaint may rely on either direct or circumstantial evidence to plead scienter adequately. However, an expanded reading of the passage to which Plaintiffs cite reads “but even the circumstantial allegations in the complaint must be strong and particular enough to withstand the PLSRA’s heightened pleading requirements. *Id.* (citing *In re Silicon Graphics Inc. Sec. Litig.*, 183 F.3d 970, 974 (9th Cir. 1999), *as amended* (Aug. 4, 1999)). Plaintiffs next two cases are case-specific applications of circumstantial evidence. *See In re UTStarcom, Inc. Sec. Litig.*, 617 F. Supp. 2d 964, 975 (N.D. Cal. 2009) (\$400 million in restated revenues can support an inference of scienter because revenues must be earned before it can be recognized.); *In re Alstom SA*, 406 F. Supp. 2d 433, 504 (S.D.N.Y. 2005) (trial court finds pleadings sufficiently show a strong inference that the cost overruns were *widely* known). Here, Plaintiffs do not analogize the alleged security breach with restated revenues, nor does the SAC allege with specificity that the breach was “widely known,” especially given that it was a “special meeting” where FE1 learned of this information. Confidential statements can only create a strong inference of scienter when the reporting witness has reliable personal knowledge of the defendants’ mental state. *See Zucco*, 552, F.3d at 998.

b. Former Employee 2 and 3

FE2's amended statement reiterates the earlier assertion that Mr. Kunze announced, in a closed meeting, that TIO had actually been breached. SAC ¶ 33. Like the FAC, at most, this statement, if believed, may show that there was *some* breach in the TIO platform known to Mr. Kunze. The new statement, however, goes on to state that "immediately after Kunze informed FE2 of the breach, the network team immediately severed the link between the corporate and production side of the network, the latter of which being where sensitive customer information was stored, in an attempt to minimize harm to customers." *Id.* FE2's new statement does not take the extra step of specifically pleading, as the PSLRA and Rule 9(b) require, that Mr. Kunze had knowledge of the magnitude of the breach. Instead, Plaintiffs seek to infer that the subsequent severing of the network is somehow an admission that Mr. Kunze had knowledge of the depth of the breach (reaching 1.6 million customers); but this inference is less cogent and compelling than the inference that the severing of the network was for preventative measures pending further investigation. In essence, FE2's statement remains substantively unchanged between the FAC and SAC. Similarly, FE3's statement remains substantively unchanged between the FAC and SAC. Like FE1's statement, FE3's statement does not even mention Mr. Kunze, and simply claims that it was *her* understanding (rather than Mr. Kunze having knowledge) that there was a breach in November 2017.

The Ninth Circuit requires that confidential witnesses meet the two-prong test of reliability. *See Daou*, 411 F.3d at 1014; *Zucco*, 552 F.3d at 991 (first, the statements must be described with sufficient particularity to establish their reliability and personal knowledge; and second, the statements must themselves be indicative of scienter). None of the FEs' statements, either individually or collectively, meet that test of reliability in demonstrating that Mr. Kunze knew on November 10, 2017, of the magnitude of the breach when he made the November Announcement.

The weakness of any inference of scienter is underscored by the lack of any obvious incentive to mislead. There is no allegation of motivation – *e.g.*, that Defendants sold stock during the Class Period or that any of the individual defendants stood to gain a profit from the alleged

wrongdoing. Nor is there any satisfying explanation of what benefit Defendants hoped to gain by delay disclosure of the full scope of the breach by three weeks. This was not like overestimating financial performance of a company with the hope and possibility that financial fortunes might improve and thereby mask an otherwise misleading statement. If there were a breach causing 1.6 million customer files to be compromised, that fact could not be undone, mooted, or masked by waiting three weeks.⁷

2. Cybersecurity Expert (Mr. Kenny Yeung)

To bolster their showing of scienter, Plaintiffs “engaged the services of a cybersecurity expert in determining what information was likely available to TIO regarding the scope of potential compromise of TIO customers’ data at the time the breach was discovered on November 10.” SAC ¶ 36. Defendants take issue with the use of Mr. Yeung’s conclusions because he has no personal knowledge about what occurred at TIO. Mot. at 12.

Both parties agree that there is authority for the proposition that a plaintiff can support a securities fraud claim with opinions provided by an expert. In *Nursing Home Pension Fund, Local 144 v. Oracle Corporation*, a case alleging false reporting of revenue and misrepresentations regarding sales projections by defendant Oracle, the Ninth Circuit found that documents relating to the billing and payment histories of Oracle’s customers, obtained by plaintiffs and analyzed by their financial expert, appeared to establish improper revenue adjustment. *Nursing Home Pension Fund, Local 144 v. Oracle Corp.*, 380 F.3d 1226, 1232–34 (9th Cir. 2004). The Ninth Circuit credited the use of plaintiff’s expert—a former financial analyst—who (1) had reviewed the billing and payment histories of some of Oracle’s customers; (2) had actually spoken with Oracle employees regarding customer payments; and (3) had provided specific and detailed reporting of the statements of the Oracle employees. *Id.* at 1233. *Nursing Home* concluded that the complaint had described the witnesses (including plaintiff’s

⁷ In their opposition and at the hearing, counsel for Plaintiffs argued a “soft landing” theory—*i.e.*, that Defendants intentionally disclosed only some of the bad news before making the full disclosure so as to soften the negative reaction from the public. Opp. at 16. This theory is not pled in the SAC, is not supported by the FE statements, and appears to be based on speculation only.

expert) “with sufficient particularity to establish that they were in a position to know Oracle’s accounting practices.” *Nursing Home*, 380 F.3d at 1233 (citing *Novak v. Kasak*, 216 F.3d 300, 314 (2d Cir. 2000)). The court added, however, that what was even more important was that the documents in which plaintiff’s expert relied “*themselves* appear to establish improper revenue adjustment.” *Id.* (emphasis added).

Thus, based on *Nursing Home* and *Zucco*, district courts can consider allegations from experts if such factual allegations satisfy the same standard applied to confidential informants. See *Browning v. Amyris, Inc.*, 2014 WL 1285175, at *19 (N.D. Cal. Mar. 24, 2014) (experts are evaluated just as confidential informants). Therefore, Mr. Yeung must meet the two-prong test of *Zucco* such that (1) his statements must be described with sufficient particularity to establish his reliability and personal knowledge; and (2) his statements must themselves be indicative of scienter.

According to the SAC, Mr. Yeung has twenty-three years of experience in information technology (security, audit, risk assessment, and risk management) and IT operations. SAC ¶ 36. He reviewed three categories of information to reach his conclusion: (1) PayPal’s and TIO’s public statements on November 10 and December 1; (2) confidential statements set forth in the SAC, and (3) publicly available information concerning TIO’s breach.” *Id.* Mr. Yeung concluded that “PayPal and TIO’s conduct in response to the breach indicates that they were likely aware that *all* customer data had been potentially compromised as of November 10th.” *Id.* ¶ 37 (emphasis in original). He reached this conclusion because, to him, TIO’s customer’s personal and financial data are its most valuable information and are what criminals who breach such servers would immediately attempt to steal. *Id.*

However, Mr. Yeung’s expert opinion fails to sufficiently strengthen the inference of scienter. There is also no allegation that Mr. Yeung was familiar with, much less had knowledge of, the specific security architecture of Defendants’ privacy network. In fact, the SAC coins Mr. Yeung’s conclusion as “the most reasonable assumption,” which appears to be merely a guess about the structure of Defendants’ network. Unlike the expert in *Nursing Home*, Mr. Yeung did not actually talk to employees at TIO or PayPal, nor did he review documents that—in and of

1 themselves—demonstrate inconsistencies that were available to Mr. Kunze during the November
2 Announcement. *See Nursing Home*, 380 F.3d at 1230 (“[t]he most direct way to show both that a
3 statement was false when made and that the party making the statement knew that it was false is
4 via contemporaneous reports or data, available to the party, which contradict the statement.”).

5 The situation here is similar to a recent decision in this district wherein plaintiffs’ theory of
6 securities fraud relied on the opinion of a non-testifying expert. In *In re OmniVision Techs., Inc.*
7 *Sec. Litig.*, 937 F. Supp. 2d 1090, 1108 (N.D. Cal. 2013, plaintiffs sued defendant for purportedly
8 concealing the fact that it (a designer and supplier of semiconductors) lost a contract with Apple to
9 Sony before the production of a new iPhone. *Id.* at 1094. Apple was the defendant’s largest
10 customer. *Id.* Plaintiffs hired a non-testifying expert consultant to opine as to when Apple’s
11 procurement process would have begun and when Apple would have started looking for
12 alternative suppliers. *Id.* at 1095. Specifically, this expert was used to establish that because this
13 iPhone had an extended product development cycle, Apple would have decided to use Sony
14 components (and not the defendant’s components) on a date prior to the start of the class period.
15 *Id.* at 1107. The *OmniVision* court found that the complaint’s reliance on this expert was
16 “essentially an allegation made on information and belief without disclosing the actual basis” for
17 its findings—*i.e.*, no personal knowledge.

18 Plaintiffs attempt to distinguish *OmniVision* by arguing that, there, the expert witness’s
19 opinions were inadequate because “they were phrased in terms of what Apple ‘would have done’ .
20 . . not facts about what Apple actually did.” *Opp.* at 15. But that is essentially what Mr. Yeung
21 has done here—*i.e.*, he is inferring what likely would have happened in the event of any breach.

22 Even considered holistically with the SAC, Mr. Yeung’s conclusions do not support a
23 finding of scienter. *See Nursing Home*, 380 F.3d at 1234 (“Considered separately, Plaintiffs’
24 allegations may not create a strong inference of scienter. However, we must consider “whether
25 the total of plaintiffs’ allegations, even though individually lacking, are sufficient to create a strong
26 inference that defendants acted with deliberate or conscious recklessness.”) (citing *No. 84*
27 *Employer-Teamster Joint Council Pension Tr. Fund v. Am. W. Holding Corp.*, 320 F.3d 920, 938
28 (9th Cir. 2003)).

Accordingly, Defendants' motion to dismiss is **GRANTED with prejudice**. *See Salameh v. Tarsadia Hotel*, 726 F.3d 1124, 1133 (9th Cir. 2013) ("A district court's discretion to deny leave to amend is 'particularly broad' where the plaintiff has previously amended.").

C. Control Liability 20(a)

For a Section 20(a) claim, Plaintiffs "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). "Section 20(a) claims may be dismissed summarily . . . if a plaintiff fails to adequately plead a primary violation of section 10(b)." *Zucco Partners, LLC*, 552 F.3d at 990. Plaintiffs' Section 20(a) claim relies on the viability of a Section 10(b) claim. As such, Defendants' motion to dismiss Plaintiffs' Section 20(a) claim is **GRANTED with prejudice**.

In sum, the SAC is dismissed with prejudice. This order disposes of Docket No. 79.

The Clerk is instructed to enter Judgment and close the file.

IT IS SO ORDERED.

Dated: September 18, 2019


EDWARD M. CHEN
United States District Judge