

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
28UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

RIPPLE LABS INC., et al.,

Plaintiffs,

v.

YOUTUBE LLC,

Defendant.

Case No. 20-cv-02747-LB

**ORDER GRANTING MOTION TO
DISMISS**

Re: ECF No. 26

INTRODUCTION

The plaintiffs, Ripple Labs and its CEO Bradley Garlinghouse (collectively, “Ripple”), developed a cryptocurrency called XRP. Scammers impersonated Ripple on YouTube (in part by using Ripple’s federally registered trademarks and publicly available content such as interviews with Mr. Garlinghouse) to make it look like they were Ripple and thus perpetuated a fraudulent “giveaway,” promising that if XRP owners sent 5,000 to one million XRP to a “cryptocurrency wallet,” then the XRP owners would receive 25,000 to five million XRP. In fact, the XRP owners who responded to the scam lost their XRP and received no XRP in return. The plaintiffs sued defendant YouTube for not doing enough to address the scam (including by failing to respond to multiple takedown notices), claiming the following: (1) contributory trademark infringement in violation of the Lanham Act, 15 U.S.C. § 1114(1) (by allowing use — and therefore infringement — of Ripple’s trademarks); (2) misappropriation of Ripple’s CEO’s identity and thus his right of

1 publicity, in violation of Cal. Civil Code § 3344 and California common law; and (3) a violation
2 of California’s unfair competition law (“UCL”), Cal. Bus. & Prof. Code § 17200, predicated on
3 the trademark and state-law claims.¹

4 YouTube moved to dismiss (1) the Lanham Act claim in part on the ground that the plaintiffs
5 did not plausibly plead its knowledge of the trademark infringement, and (2) the state-law claims
6 on the ground that it is immune from liability under § 230(c)(1) of the Communications Decency
7 Act (“CDA”), 47 U.S.C. § 230(c)(1), because it is not a content provider.² The court grants the
8 motion (with leave to amend).

9 **STATEMENT**

10 Ripple is an “enterprise blockchain company” that developed and manages the cryptocurrency
11 XRP, which can be used in place of traditional currencies to facilitate cross-border payments.³
12 Banks, corporations, and individuals buy XRP.⁴

13 YouTube is a video-sharing platform.⁵

14 Ripple and XRP owners were the target of a fraud — the XRP Giveaway Scam — whereby
15 the fraudsters hijacked other users’ channels on YouTube and used the channels to impersonate
16 Ripple and its CEO. (Fraudsters can hijack a legitimate YouTube channel through a spear-
17 phishing attack: the fraudsters send an email to the channel’s creator, and when the creator
18 responds, he inadvertently discloses his YouTube credentials, thereby allowing the fraudsters to
19 take over his channel and populate its content.) After hijacking the channels, the fraudsters
20 populated the channels with content that included Ripple’s trademarks (such as its logo and name),
21 Mr. Garlinghouse’s name and likeness, and publicly available content (such as interviews with
22 Mr. Garlinghouse or other members of Ripple’s leadership team). Masquerading as Ripple, the

23
24
25
26
27
28

¹ Compl. – ECF No. 1 at 17–21 (¶¶ 61–99). Citations refer to material in the Electronic Case File (“ECF”); pinpoint citations are to the ECF-generated page numbers at the top of documents.

² Mot. – ECF No. 26.

³ Compl. – ECF No. 1 at 4 (¶¶ 12, 19), at 5 (¶¶ 20–21).

⁴ *Id.* at 4–5 (¶¶ 19–20).

⁵ *Id.* at 6 (¶ 27).

1 fraudsters promised XRP owners that if they sent between 5,000 to one million XRP to a digital
2 wallet, then they would receive between 25,000 to five million XRP. After XRP owners sent XRP
3 to the digital wallet, the currency disappeared, and the XRP owners received nothing in return.⁶

4 Ripple and YouTube users alerted YouTube about the scam, but YouTube allegedly did not
5 respond by taking down the offending content in a reasonable time frame. A Forbes article in
6 November 2019 reported the scam, the hijacking of popular YouTube creator MarcoStyle’s
7 channel, the conversion of his channel to Mr. Garlinghouse’s profile, the hacker’s running of a
8 livestream promoting the scam, and the stealing of \$15,000 from viewers’ Ripple wallets.⁷
9 MarcoStyle alerted YouTube, and YouTube acknowledged the issue that day but took a week to
10 resolve it.⁸ During this time, YouTube verified the hijacked channel as authentic (even though it
11 was masquerading as Mr. Garlinghouse’s account).⁹

12 After the Forbes article, Ripple alleges that it sent YouTube more than 350 takedown notices:
13 49 related directly to the scam and 305 related to accounts and channels that were impersonating
14 Mr. Garlinghouse or infringing on Ripple’s brand, likely to monetize the scam.¹⁰ Ripple alleges
15 that it sent multiple takedown notices for the same conduct because YouTube did not take down
16 the fraudulent channels for days, weeks, or months after notice.¹¹ New instances of the scam
17 “continued to appear, often amassing thousands of views and creating more victims by the day.”¹²

18
19 ⁶ *Id.* at 7–9 (¶ 35).

20 ⁷ *Id.* at 10 (¶ 40); Paul Tassi, *A YouTuber with 350,000 Subscribers Was Hacked, YouTube verified His*
21 *Hacker*, Forbes (Nov. 14, 2019), <https://www.forbes.com/sites/paultassi/2019/11/14/a-youtuber-with-350000-subscribers-was-hacked-youtube-verified-his-hacker/?sh=23bd01a76fe6>, Ex. 8 to Compl. –
22 ECF No. 1-1 at 141–42. The court considers the documents attached to the complaint under the
incorporation-by-reference doctrine. *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542,
1555 n.19 (9th Cir. 1989); *see also Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

23 ⁸ Forbes Article, Ex. 8 to Compl. – ECF No. 1-1 at 142

24 ⁹ Compl. – ECF No. 1 at 10 (¶ 40).

25 ¹⁰ *Id.* at 12 (¶ 47).

26 ¹¹ *Id.* (¶ 48) (14 takedown notices (starting November 12, 2019) about hijacked channel purporting to
be Mr. Garlinghouse’s channel that resulted in a takedown months later, on February 19, 2020;
January 2, 2020 takedown notice that took three weeks to resolve; nine takedown notices (starting
27 January 21, 2020) about channel promoting the scam that remained active until March 18, 2020;
January 27, 2020 notice about hijacked channel promoting the scam resolved on February 3, 2020).

28 ¹² *Id.* (¶ 49).

1 For example, on March 20, 2020, a YouTube user told YouTube about a channel using Ripple’s
2 marks and Mr. Garlinghouse’s image to promote the scam, YouTube did not take action, and by
3 the next day, 85,000 users viewed the fraudulent video.¹³

4 YouTube allegedly profited from the scam because it sold ads to the fraudsters that featured
5 Mr. Garlinghouse’s name, infringed on Ripple’s trademarks, and promoted the scam.¹⁴

6 According to its guidelines and policies, YouTube removes offending content when it learns
7 about it, including “scams and other deceptive practices.”¹⁵

8 The parties do not dispute that the court has federal-question jurisdiction over the Lanham Act
9 contributory trademark-infringement claim and supplemental jurisdiction over the state-law
10 claims.¹⁶ 28 U.S.C. §§ 1331, 1367. All parties consented to magistrate jurisdiction.¹⁷

11 12 **STANDARD OF REVIEW**

13 A complaint must contain a “short and plain statement of the claim showing that the pleader is
14 entitled to relief” to give the defendant “fair notice” of what the claims are and the grounds upon
15 which they rest. Fed. R. Civ. P. 8(a)(2); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A
16 complaint does not need detailed factual allegations, but “a plaintiff’s obligation to provide the
17 ‘grounds’ of his ‘entitlement to relief’ requires more than labels and conclusions, and a formulaic
18 recitation of the elements of a cause of action will not do. Factual allegations must be enough to
19 raise a claim for relief above the speculative level[.]” *Twombly*, 550 U.S. at 555 (cleaned up).

20 To survive a motion to dismiss, a complaint must contain sufficient factual allegations, which
21 when accepted as true, “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556
22 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). “A claim has facial plausibility when
23

24 _____
25 ¹³ *Id.* at 14 (¶ 52).

26 ¹⁴ *Id.* at 10 (¶ 37).

27 ¹⁵ *Id.* at 6–7 (¶¶ 30–33); YouTube Policies, Ex. 1 to Compl. – ECF No. 1-1 at 2–6; YouTube
28 Community Guidelines Enforcement, Ex. 4 to Compl. – ECF No. 1-1 at 114–122.

¹⁶ *Id.* at 4 (¶¶ 15–16); Mot. – ECF No. 26.

¹⁷ Consents – ECF Nos. 13–14.

1 the plaintiff pleads factual content that allows the court to draw the reasonable inference that the
2 defendant is liable for the misconduct alleged.” *Id.* “The plausibility standard is not akin to a
3 ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted
4 unlawfully.” *Id.* (citing *Twombly*, 550 U.S. at 557). “Where a complaint pleads facts that are
5 merely consistent with a defendant’s liability, it stops short of the line between possibility and
6 plausibility of ‘entitlement to relief.’” *Id.* (cleaned up) (quoting *Twombly*, 550 U.S. at 557).

7 If a court dismisses a complaint, it should give leave to amend unless the “pleading could not
8 possibly be cured by the allegation of other facts.” *United States v. United Healthcare Ins. Co.*,
9 848 F.3d 1161, 1182 (9th Cir. 2016) (cleaned up).

11 ANALYSIS

12 YouTube moved to dismiss the trademark and state-law claims under Rule 12(b)(6) for failure
13 to state a claim. The court grants the motion with leave to amend.

15 1. Contributory Trademark Infringement

16 “To be liable for contributory trademark infringement, a defendant must have (1) intentionally
17 induced the primary infringer to infringe, or (2) continued to supply an infringing product to an
18 infringer with knowledge that the infringer is mislabeling the particular product supplied.” *Perfect*
19 *10, Inc. v. Visa Int’l Serv. Ass’n*, 494 F.3d 788, 807 (9th Cir. 2007) (cleaned up). If the alleged
20 infringer supplies a service (as opposed to a product), then “the court must consider the extent of
21 control exercised by the defendant over the third party’s means of infringement.” *Id.* A plaintiff
22 must show that the defendant “continued to supply its services to one who it knew or had reason to
23 know was engaging in trademark infringement.” *Louis Vuitton Malletier, S.A. v. Akanoc Sols, Inc.*,
24 658 F.3d 936, 942 (9th Cir. 2011).

25 Contributory trademark infringement claims about conduct on an online platform often involve
26 the sale of infringing goods in an online marketplace. In that context, courts have held that “a
27 service provider must have more than a general knowledge or reason to know that its service is
28 being used to sell counterfeit goods. Some contemporary knowledge of which particular listings

1 are infringing or will infringe . . . is necessary.” *Spy Phone Labs LLC v. Google Inc.*, No. 15-cv-
 2 03756-PSG, 2016 WL 1089267, at *3 (N.D. Cal. Mar. 21, 2016) (quoting *Tiffany (NJ) Inc. v. eBay*
 3 *Inc.* 600 F.3d 93, 107 (2d Cir. 2010)). Also, “notice of certain acts of infringement does not imply
 4 generalized knowledge of — and liability for — others.” *Id.* (citations omitted). Thus, in *Spy*
 5 *Phone*, the court held that an app developer’s complaint to Google about competing apps’
 6 violations of Google’s anti-spyware policy was not the same as a trademark complaint. *Id.* at *2,
 7 4. A trademark complaint was a notice of infringement, but a spyware complaint was not. *Id.* at
 8 *4. Absent notice of trademark infringement in the form of a trademark complaint, Google was
 9 not liable for not removing infringing apps preemptively. *Id.*

10 The plaintiffs allegedly notified YouTube of the trademark infringement through takedown
 11 notices and allege that You Tube “ignored or failed to address many of the[ir] takedown
 12 demands.”¹⁸ The examples — in subparagraphs to that general allegation — are about delay in
 13 taking down the offending channels (not a failure to do so altogether), all in the face of a persistent
 14 fraud that apparently had near daily new occurrences.¹⁹ The examples include (1) a takedown
 15 notice, 13 subsequent takedown notices, and a hacked channel’s remaining active for more than
 16 two months until YouTube “took corrective action,” (2) a three-week delay before YouTube
 17 “addressed” a hacked channel after notice, (3) a takedown notice, eight more takedown notices,
 18 and slightly less than two months before YouTube addressed a channel promoting the scam, and
 19 (4) a week’s delay before YouTube addressed a hacked channel.²⁰

20 The issue thus is whether the plaintiffs’ allegations about YouTube’s delay in taking down the
 21 scam and the hijacked channels — which used Ripple’s trademarked content — plausibly plead a
 22 claim for contributory trademark infringement.

23
 24
 25 _____
 26 ¹⁸ Compl. – ECF No. 1 at 12–13 (¶¶ 48–49).
 27 ¹⁹ *Id.* at 12 (¶ 48); *see* Statement.
 28 ²⁰ Compl. – ECF No. 1 at 12 (¶ 48) (referring to YouTube’s taking “corrective action” eventually). The
 court cannot tell whether “taking corrective action” involves removing the channels or instead
 involved other corrective action. The court thus uses the proxy that YouTube “addressed” the issue.

1 Courts have found that delays of several days (after receipt of a trademark complaint) do not
2 plausibly establish a contributory trademark infringement claim, but delays of at least six months
3 can. *Spy Phone*, No. 15-cv-03756-KAW, 2016 WL 6025469, at *5 (N.D. Cal. Oct. 14, 2016)
4 (collecting cases, including those involving a six-month delay and a six-to-nine-month delay). In
5 *Spy Phone*, a contributory trademark claim survived a Rule 12(b)(6) motion when Google took 18
6 and 27 days to address two trademark complaints. The length of time alone did not plausibly
7 establish a claim, but other fact issues about Google’s response to the trademark complaints —
8 such as whether it unjustifiably or purposefully delayed its investigation (and thereby provided
9 services to a known infringer) — meant that the claim survived at the pleadings stage. *Id.*

10 Under these cases, the plaintiffs have not plausibly pleaded a claim for contributory trademark
11 infringement.

12 The plaintiffs allegedly complained about trademark infringement, and they also complained
13 about the misuse of Mr. Garlinghouse’s identity.²¹ Applying the analysis in *Spy Phone*, the first
14 category is a notice of trademark infringement that required YouTube’s response, and the second
15 is not. *Id.*, No. 15-cv-03756-PSG, 2016 WL 1089267 at *4. The complaint lumps the two
16 categories together. The plaintiffs must identify their complaints of trademark infringement
17 (tethered to a specific YouTube user’s account) and YouTube’s failure to respond or delayed
18 response to the specific complaints.

19 Without a delineation between the two categories, the court cannot evaluate whether YouTube
20 had contemporaneous knowledge of the infringing conduct and continued to supply its services.
21 *Id.*; *Louis Vuitton*, 658 F.3d at 942. As a result, the court cannot “draw the reasonable inference
22 that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. Also, the alleged
23 delays here — a week, several weeks, around two months — are shorter than the delays that courts
24 generally have found actionable. (*Spy Phone* had shorter delays of 18 and 27 days, but the delays
25 themselves did not establish a plausible claim; instead, disputed facts about Google’s reasons for
26 the delay did. No. 15-cv-03756-KAW, 2016 WL 6025469 at *5 (collecting cases).

27
28

²¹ *Id.* (¶ 47).

1 At the hearing, the plaintiffs argued that requiring this specificity imposes a pleading standard
2 that exceeds Rule 8)(a)'s "fair notice" requirement and is the equivalent of pleading the claims
3 with particularity under Rule 9(b), meaning, the who, what, where, when, and how of the
4 misconduct. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). The court is not
5 imposing a Rule 9(b) standard. The plaintiffs do not need to plead all of their evidence.

6 Representative examples — similar to those in paragraph 48 of the complaint but identifying the
7 specific trademark complaints and YouTube's response to those complaints — are sufficient.

8 The plaintiffs' remaining theories for contributory trademark infringement fail for the
9 following reasons.

10 The plaintiffs contend that YouTube had constructive knowledge that the scam was persistent
11 and the tools to eliminate the scam from its platform.²² This claim turns on the actual notice to
12 YouTube. *Tiffany*, 600 F.3d at 109; *Spy Phone*, No. 15-cv-03756-PSG, 2016 WL 1089267 at *3–
13 4, *id.*, No. 15-cv-03756-KAW, 2016 WL 6025469 at *6. As discussed above, the allegations in the
14 plaintiffs' complaint do not sufficiently differentiate between the trademark notices and the other
15 notices. Thus, the plaintiffs do not plausibly plead a claim.

16 The plaintiffs also contend that YouTube was willfully blind to the scam and failed to prevent
17 it.²³ See *Global-Tech Appliances, Inc. v. S.E.B. SA.*, 563 U.S. 754, 769 (2011); *Spy Phone*, No. 15-
18 cv-03756-KAW, 2016 WL 6025469 at *6. The facts alleged here do not establish a duty to
19 preemptively address the scam based on YouTube's knowledge of the infringements. *Spy Phone*,
20 No. 15-cv-03756-KAW, 2016 WL 6025469 at *6 (analyzing cases and holding that Google did
21 not have a generalized duty — based on knowledge that a vendor was selling counterfeit goods —
22 to preemptively police online vendors). The result in *Spy Phone* applies with greater force here
23 because YouTube is not an online marketplace policing its vendors and instead is a social-media
24 platform hosting its users. Its ability to react to and police hackers is different than an online
25 marketplace's ability to react to and police its vendors.

26
27 _____
28 ²² Opp'n – ECF No. 29 at 16–20.

²³ *Id.* at 20–21.

1 To illuminate the point, consider the cases that the parties cite: they all involve online
2 marketplaces. (The parties did not cite any case involving similar allegations of trademark
3 infringement on a hijacked social-media platform, and the court did not find any.) The cases
4 establish that an online marketplace is responsible for contributory trademark infringement when
5 — after notice that a vendor is selling infringing products — it allows the vendor to keep selling
6 the infringing products. For example, in *Spy Phone*, Google allegedly allowed a vendor to release
7 an infringing app after notice that the vendor’s released app was infringing *Spy Phone*’s
8 trademark. No. 15-cv-03756-KAW, 2016 WL 6025469 at *6. In *Spy Optic, Inc. v. Alibaba, Inc.*,
9 on one occasion, the Alibaba marketplace allowed the infringing vendor to post “multiple
10 infringing products” after the plaintiff identified the trademark infringement. 163 F. Supp. 3d 755,
11 766 (C.D. Cal. 2015). By contrast, in *Tiffany (NJ) v. eBay Inc.*, eBay took down challenged
12 listings promptly, warned sellers and buyers, canceled fees it earned, and directed buyers not to
13 consummate the sale of the disputed item. 600 F.3d at 106.

14 The cases illustrate an online marketplace’s duty (and ability) to remove a known vendor from
15 the online platform when it knows about the trademark infringement. *Louis Vuitton*, 658 F.3d at
16 942. Thus, it might be reasonable to hold eBay to a tight time period to discontinue its services to
17 someone selling fake Tiffany or Louis Vuitton products: eBay and its vendors have a business
18 relationship, and eBay can terminate a vendor easily. eBay also derives revenue from the
19 relationship. And if eBay delays an investigation and a takedown, there might be fact issues about
20 whether it purposefully or unjustifiably did so, presumably for self-serving reasons. *Cf. Spy*
21 *Phone*, No. 15-cv-03756-KAW, 2016 WL 6025469 at *5. That ability to police its vendors
22 arguably makes it more accountable when it does not take action.

23 An online social-media platform’s delay in investigating and removing scams like the one here
24 is not obviously analogous to the marketplace’s delay. Investigating a scam — involving phishing
25 and hijacked user credentials — is (at minimum) different and likely more complicated. For one,
26 YouTube does not control a hacker in the same way that a marketplace controls a vendor’s ability
27 to sell on the platform. *See Perfect 10*, 494 F.3d at 807. Also, YouTube’s investigation involves
28

1 legitimate YouTube users and a persistent, evolving scam creating “more victims by the day.”²⁴ Its
2 investigation differs in scope from the marketplace’s investigation of its vendor. The impact of
3 notice (or in the language of the cases, “contemporary knowledge” of infringement) is different
4 too. *Spy Phone*, No. 15-cv-03756-PSG, 2016 WL 1089267 at *3. When a marketplace knows
5 about infringing products, it can terminate the infringing vendor. The only thing that matters is
6 notice of the trademark infringement. But when YouTube learns about hacked content that
7 includes trademarked content, the scope of its inquiry also is about protection of data and its users
8 and eliminating the scam.

9 Moreover, YouTube does not provide services to or profit from a hacker in the same way that
10 a marketplace provides services to and profits from a vendor. *Id.* In some ways, it too is a victim
11 of the hijacking. Its revenues from ads are not obviously equivalent to revenues resulting from a
12 business contract between a marketplace and a vendor.

13 Ultimately, it may be that the sufficiency of YouTube’s response involves factual disputes that
14 are not amenable to resolution on a Rule 12(b)(6) motion, at least as to whether YouTube had
15 contemporaneous knowledge of the infringing conduct and continued to supply its services. *Louis*
16 *Vuitton*, 658 F.3d at 942.

17 For now, the court dismisses the contributory trademark claim with leave to amend.
18

19 **2. Section 230 Immunity**

20 Absent a federal claim, the court does not have supplemental jurisdiction over the state claims.
21 28 U.S.C. § 1367(a). Even assuming that there is a viable federal claim, YouTube is immune
22 under § 230(c)(1) of the Communications Decency Act for the state claims: (1) misappropriation
23 of Ripple’s CEO’s identity and his right of publicity, in violation of Cal. Civil Code § 3344 and
24 California common law, and (2) a violation of the UCL based on the predicate state-law and
25 federal claims.²⁵

26
27 _____
28 ²⁴ Compl. – ECF No. 1 at 12–13 (¶¶ 48–49).

²⁵ *Id.* at 18–21 (¶¶ 75–99).

1 Under the Communications Decency Act, (1) website operators generally are immune from
2 liability for third-party content posted on their websites, but (2) they are not immune if they create
3 or develop the information, in whole or in part. 47 U.S.C. §§ 230(c)(1) & (f)(3). “Immunity from
4 liability exists for (1) a provider or user of an interactive computer service, (2) whom a plaintiff
5 seeks to treat, under a state law cause of action, as a publisher or speaker of (3) information
6 provided by another information content provider.” *Dyroff v. Ultimate Software Grp., Inc.*, 934
7 F.3d 1093, 1097 (9th Cir. 2019) (cleaned up).

8 YouTube is an interactive-computer service.²⁶ It is undisputed that it did not create any ads:
9 YouTube ads are third-party content, and the at-issue “ads were presented to YouTube by the
10 scammers” here.²⁷ It is not “responsible, in whole or in part, for the creation or development of the
11 information,” and thus, it is immune from liability for the third-party content. 47 U.S.C. §
12 230(f)(3); *cf. Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 801–03 (N.D. Cal. 2011) (Facebook
13 created ads, including content, based on users’ browsing history, and thus it was not immune
14 under the Act for violating the plaintiffs’ statutory right of publicity, among other things).

15 The plaintiffs nonetheless contend that YouTube materially contributed to the scam (and
16 created content) by awarding a “verification badge” — by giving the MarcoStyle hacked channel a
17 badge that it allegedly reserves for “authentic” channels — thereby “communicating to hundreds
18 of thousands of viewers and subscribers that these hacked accounts and channels were ‘the official
19 channel of a creator, artist, company, or public figure.’”²⁸ A website helps to develop unlawful
20 content if it “contributes materially to the alleged illegality of the content.” *Fair Hous. Council v.*
21 *Roommates.com, LLC*, 521 F.3d 1157, 1167–68 (9th Cir. 2008). The badge did not materially
22 contribute to the content’s illegality here. *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 n.4 (9th Cir.

23
24
25
26 _____
27 ²⁶ Opp’n – ECF No. 29 at 21–26; Reply – ECF No. 33 at 7.

28 ²⁷ Compl. – ECF No. 1 at 10 (¶ 37).

²⁸ Opp’n – ECF No. 29 at 22 (quoting Compl. – ECF No. 1 at 3 (¶ 10)).

1 2016). What made the content illegal was that the scammers hijacked users' content and tricked
2 them into sending their XRP to a digital wallet.²⁹

3 The plaintiffs also contend that YouTube materially contributed to the fraudulent
4 advertisements for the scam by allowing advertisers to display "views" that the video received.³⁰
5 Displaying views does not create content, and the plaintiffs' argument thus does not alter the
6 conclusion that YouTube has immunity under § 230(c) for the state-law claims. *Dyroff*, 934 F.3d
7 at 1096; *Kimzey*, 836 F.3d at 1270; *Roommates*, 521 F.3d at 1169.

8
9 **CONCLUSION**

10 The court grants the motion to dismiss with leave to amend within 21 days. This disposes of
11 ECF No. 26.

12 **IT IS SO ORDERED.**

13 Dated: November 20, 2020



14 LAUREL BEELER
15 United States Magistrate Judge

16
17
18
19
20
21
22
23
24
25
26
27 _____
28 ²⁹ The complaint's allegations do not establish that verification of YouTube accounts promotes the
scam either. *See, e.g.*, Compl. – ECF No. 1 at 11 (¶ 43).

³⁰ Opp'n – ECF 29 at 25 (citing Compl. – ECF No. 1 at 10 (¶ 37)).