UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, Plaintiff, v. YUNFENG SUN, a/k/a "ALPHONSE SUN," and HONGNAM CHEUNG, a/k/a "ZHANG HONGNIM," a/k/a "STANFORD FISCHER," Defendants.	Civil Action No. **COMPLAINT**

INTRODUCTION

1. At all times relevant to this Complaint, Defendants Yunfeng Sun, a/k/a "Alphonse Sun," and Hongnam Cheung, a/k/a "Zhang Hongnim" and "Stanford Fischer," were online application ("app") developers who were engaged in an international online consumer investment fraud scheme (the "Fraud Scheme"). Through that Fraud Scheme, Defendants and other co-conspirators, known and unknown, perpetrated a form of online fraud through which they socially engineered and targeted victims to download from, among other sources, Google Play mobile apps that purportedly offered investments in cryptocurrencies and other products.[1] Members of the Fraud Scheme lured victims in with promises of high returns, and the seemingly legitimate apps were designed to display purported returns on investments in individual victim accounts. Yet the gains conveyed by the apps were illusory. And the scheme did not end there. Instead, when individual victims attempted to withdraw

[1] This type of fraud scheme is frequently referred to by the press and government agencies, such as the Federal Bureau of Investigation, as "pig butchering." Google neither adopts nor endorses the use of this term.

their balances, Defendants and their confederates would double down on the scheme by requesting various fees and other payments from victims that were supposedly necessary for the victims to recover their principal investments and purported gains.

2. Defendants have engaged in a persistent, continuing scheme to defraud consumers, despite Google's efforts to combat the scheme to protect users on its platforms by investigating and suspending offending fraudulent apps that Defendants uploaded to Google Play. As Google has suspended and taken apps offline to shield Google Play users, Defendants have persisted in uploading new apps to Google Play, using varying computer network infrastructure and accounts to obfuscate their identities, and making material misrepresentations to Google in the process. Since at least approximately 2019, Defendants and their confederates have uploaded at least approximately 87 apps to Google Play in furtherance of the Fraud Scheme.

3. Through the course of this continuing pattern of fraudulent and illegal activity, Defendants' Fraud Scheme has caused at least approximately 100,000 individual users to download the apps from Google Play, causing financial loss to consumer victims. The Fraud Scheme also harms Google, by threatening the integrity of its Play platform, compelling Google to spend resources investigating and remediating this misconduct in order to protect its users, and jeopardizing Google's relationship with its current and potential users.

PARTIES

I. PLAINTIFF

4. Plaintiff Google LLC is a corporation organized under the laws of the State of Delaware with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California.

5. As a leading technology company, Google operates a variety of popular online consumer products, platforms, and services, many of which are core to its business and relevant here:

a. ***Google Play.*** Google Play is an online store that provides over 2 million online applications to Google Android and Google Chrome users. Third-party developers upload their apps to Google Play, which enables them to distribute the apps to billions of users around the world. Developers can choose to offer their apps to users to download for free or for a fee.

b. ***Google Workspace.*** Google Workspace is a cloud-based suite of productivity and collaboration tools that provides users with integrated collaboration tools, including Gmail, Google Drive, Google Meet, Google Chat, Google Docs, Google Slides, Google Sheets, Google Forms, and Google Sites.

c. ***Gmail.*** Gmail is a free email service that is hosted on Google's servers and used by more than 1.5 billion people worldwide.

d. ***Google Voice.*** Google Voice is a free call-management service that enables users to place and receive calls from anywhere through a smartphone or the Internet.

e. ***YouTube.*** YouTube is an online video-sharing platform that millions of people use to share and watch videos each day.

6. Google is committed to providing a safe and secure environment for its users by preventing apps that are deceptive and malicious from operating on the Google Play platform. As discussed in greater detail below, Google requires developers who release apps on the Google Play platform to agree to a Developer Agreement that governs their conduct.

Google also deploys substantial resources to detect the abuse of its services by bad actors, including by soliciting reports of inappropriate behavior from Google users, by investigating fraud and other illegal activity on apps released on Google Play, and by taking other steps to enforce the Developer Agreement against developers whom Google detects as breaking the rules.

II. DEFENDANTS

7. Defendants listed in paragraphs 8–9 are individuals who have conspired to engage in an unlawful pattern of racketeering activity by committing hundreds of acts of wire fraud, causing harm to Google and at least approximately 100,000 Google users (the Fraud Scheme).

8. Defendant Yunfeng Sun, a/k/a "Alphonse Sun," is an individual who has developed Google Play apps. He is believed to reside in Shenzhen, China.

9. Defendant Hongnam Cheung, a/k/a "Zhang Hongnim" and "Stanford Fischer," is an individual who has developed Google Play apps. He is believed to reside in Hong Kong, China.

JURISDICTION AND VENUE

10. This Court has federal-question jurisdiction over Google's claim under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), pursuant to 28 U.S.C. § 1331. This Court also has jurisdiction over the causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1332 because complete diversity exists between Plaintiff and Defendants, and because the amount in controversy exceeds $75,000. This Court has supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over Defendants pursuant to 18 U.S.C. § 1965 and N.Y. C.P.L.R. §§ 301 and 302 because Defendants have transacted business and engaged in fraudulent conduct in the United States and in New York, which gives rise in part to Google's claims. Defendants used two companies purportedly located in New York, New York to facilitate the unlawful activity. *See infra* ¶¶ 32, 49. Defendants have also engaged in intentional, wrongful, and illegal acts the effects of which Defendants knew and intended would be felt in the United States and New York. Among other things, Defendants have intentionally caused victims to download their fraudulent apps in New York and throughout the United States, and have intentionally directed victims' machines in New York and throughout the United States to subject them to fraudulent acts.

12. This Court also has pendent personal jurisdiction over Defendants on Plaintiff's state-law claims for breach of contract. *See infra* ¶¶ 82–110. Exercising pendent personal jurisdiction in this case is appropriate, regardless of whether personal jurisdiction is otherwise available, because Plaintiff's RICO claims and breach of contract claims derive from a common nucleus of operative fact.

13. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(c) because Defendants do not reside in the United States and may be sued in any judicial district.

14. Venue is also proper in this judicial district pursuant to 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because a substantial portion of the harm to Google occurred in this district and Defendants transacted their affairs in this judicial district. Defendants engage in conduct availing themselves of the privilege of conducting business in New York, and used instrumentalities located in this judicial district to carry out acts alleged in this Complaint.

FACTUAL ALLEGATIONS

I. GOOGLE AND GOOGLE PLAY

15. Google Play is an online store that provides millions of apps to approximately 2.5 billion monthly active users around the world. Through Google Play, Google offers an app-distribution platform where developers can upload their creations and users can download the content they want. Google Play benefits both developers and users: it allows developers to scale up their businesses by reaching audiences in over 190 countries and allows users to safely connect with an enormous number and diverse variety of apps through Android (a free and open operating system).

16. Before developers can upload their apps to Google Play, they must identify themselves[2] and submit the apps to Google for approval. In their submission, developers must provide the app title, a category and description, and information about the functionality and content of their app. Once a developer submits its app to Google Play, Google uses a combination of human and automatic reviews to review the app to ensure that it comports with Google's Play Developer Program Policies. If the app passes the review, it is published to Google Play and available for users to download. If the app does not pass the review, the developer is provided with the reasons for rejection, and can make the required updates and resubmit the app for approval.

17. Developers' use of Google Play is governed by the Developer Distribution Agreement (the "Developer Agreement"), a legally binding contract between Google and

[2] Developers must provide a contact name and contact details when creating a developer account. *See* Contact Information requirements for developer accounts, https://support.google.com/googleplay/android-developer/answer/10840893?hl=en#zippy=%2Cdeveloper-account-for-organization-or-business%2Cdeveloper-account-for-personal-use, attached as **Exhibit 1**.

developers.[3] It covers developers' use of Google Play to distribute their products, and contains various terms and conditions geared toward protecting Google users from fraud, including but not limited to, the following terms:

a. Section 4.1 of the Developer Agreement requires developers and their products to "adhere to the Developer Program Policies."[4] Among other things, the Developer Program Policies forbid developers to upload to Google Play "apps that expose users to deceptive or harmful financial products and services," including harmful products and services "related to the management or investment of money and cryptocurrencies."[5]

b. Sections 4.6 and 11.4 of the Developer Agreement require developers to use "Google Play only for purposes that are permitted by [the Developer Agreement] and any applicable law [and] regulation," and "represent and warrant that all information that [they] provide to Google or users in connection with [the Developer] Agreement or [their] Products will be current, true, accurate, supportable and complete."[6]

18. Google uses a variety of mechanisms to enforce the Developer Program Policies against apps and developer accounts that violate those policies.[7] As discussed, Google reviews submissions for apps that developers seek to add to Google Play, and if an app does

[3] The Developer Agreement, https://play.google.com/about/developer-distribution-agreement.html, attached as **Exhibit 2**.

[4] Exhibit 2.

[5] Financial Services subsection of Play Console Help, https://support.google.com/googleplay/android-developer/answer/9876821?hl=en, attached as **Exhibit 3**.

[6] Exhibit 2.

[7] *See* the Developer Program Policy, https://support.google.com/googleplay/android-developer/answer/14693005?visit_id=638216912481327759-14, attached as **Exhibit 4**.

not pass Google's review, it will be rejected, meaning that it will not be made available on Google Play. Google may also remove already-published apps from the app store for detected policy violations. Once Google removes an app, users can no longer download that app or any prior version. If an app violates the Developer Program Policies multiple times or in an egregious manner, Google may suspend the app and any prior versions, making them unavailable for download from Google Play. If Google suspends an app from Google Play, that will also count as a strike against the good standing of the app developer's Google Play developer account. Under section 2.2 of the Developer Agreement, developers must be in good standing to distribute their apps through Google Play.[8] If a developer "repeated[ly] or serious[ly]" violates the Developer Agreement, including by committing fraud or acts that harm users, Google can terminate the developer's accounts altogether, meaning that the developer can no longer use Google Play at all.[9] The Developer Policies also assert that any related individual and developer accounts may also be permanently suspended if a user account is terminated.[10]

II. MEANS AND METHODS OF DEFENDANTS' RACKETEERING CONSPIRACY

19. Defendants were involved in a type of online fraud scheme through which fraudsters contact and socially engineer targets through text messaging or other communication platforms, gain their trust, and ultimately convince them to invest in seemingly legitimate investment platforms. Frequently, the fraudsters will guarantee that the investments will yield high returns, and may give the victims doctored reports falsely depicting their

[8] Exhibit 2.

[9] *See* Enforcement Process, https://support.google.com/googleplay/android-developer/answer/9899234?hl=en, attached as **Exhibit 5**.

[10] *Id.*

investment as earning money. When victims attempt to withdraw funds, they cannot do so. The fraudsters frequently respond to attempts to withdraw funds by requesting additional investment, taxes, or fees, promising that these payments will allow victims to access their accounts. But no matter how much money the victim hands over or how many promises the fraudsters make, the moment the victims "invest" the money, it is gone.

20. Since at least in or about 2019 through the present, Defendants have conducted their version of the Fraud Scheme by socially engineering and conning victims into "investing" in apps, available on Google Play and through other means, that purported to be cryptocurrency exchanges and other investment platforms.

21. While Defendants varied their approach from app to app, the means and methods were substantially similar.

22. First, Defendants created fraudulent apps that purported to be legitimate cryptocurrency exchanges and investment platforms, and made them available on Google Play. Defendants made multiple misrepresentations to Google in order to upload their fraudulent apps to Google Play, including but not limited to, misrepresentations about their identity, location, and the type and nature of the application being uploaded.

23. Next, Defendants Yunfeng Sun and Hongnam Cheung (including through their agents) socially engineered and lured victim investors to download their fraudulent apps from Google Play and other sources, primarily through three methods:

a. ***Wayward text-messaging campaigns.*** Defendants or their agents would send text messages using Google Voice to potential victims, primarily in the United States and Canada. The messages were designed to convince the targeted victims that they were sent to the wrong number (for example, "I am Sophia,

do you remember me?" or "I miss you all the time, how are your parents Mike?"). If targeted victims responded (for example, by telling the senders that they must be sending messages to the wrong number), Defendants or their agents would try to strike up a conversation and after exchanging initial messages with the victims,[11] shift the conversations to other messaging platforms such as WhatsApp. Defendants or their agents would then attempt to develop a "friendship" or "romantic relationship" and ultimately try to persuade the victims to download and invest through one of their apps. The "friend" or "romantic partner" would offer to guide the victim through the investment process, often reassuring the victim of any doubts they had about the apps, but then disappear once the victim tried to withdraw funds.

b. ***Online videos.*** Defendants or their agents created online videos, including on YouTube, promoting the fraudulent investment apps. The videos were designed to convince potential investors that the investment platforms and cryptocurrency were legitimate, safe, and effective by providing information about the history of the investment platforms and the cryptocurrency, such as introducing viewers to the "leadership teams" (which, on information and belief, were in fact paid actors). The videos would promise high rates of return, for example, two percent daily investment return.

c. ***Affiliate marketing campaigns.*** Defendants or their agents lured victims using in-person and online marketing programs that convinced users to become "affiliates" of the apps on the promise that they would earn commission by

[11] A number of users reported these text messages as spam to Google.

signing up additional users. Through these affiliate programs, Defendants advertised their apps on social media as a guaranteed and easy way to earn money. Defendants even offered in-person conferences to give "investment advice" and promote the financial benefits of using their apps and trading platforms.

24. Defendants and their agents designed the fraudulent apps that were made available on Google Play to appear legitimate. Their user interfaces sought to convince victims that they were maintaining balances on the app and that they were earning "returns" on their investments. But those statements were false. The apps were not actual trading platforms; they existed only to ingest users' money, with which the fraudsters then abscond.

25. Finally, users could not successfully withdraw their investments or their purported gains. Sometimes, to convince users that the apps were legitimate and that it was safe to invest larger amounts of money, Defendants or their agents would allow users to initially withdraw small amounts. But later attempts to withdraw purported returns simply did not work. Some users received no response at all when they tried to withdraw money, despite repeatedly contacting purported customer-service lines. Worse still, other users were told that they needed to pay a fee or have a minimum balance to withdraw their money—ploys that bilked some victims out of even more money. Various victims of the Fraud Scheme have flagged the apps to Google Play as inappropriate by reporting, in sum and substance and among other things, that requests to withdraw investments and returns have been met with demands that additional funds be submitted to enable them to access their funds, with some demands ranging from 10 to 30 percent to cover purported commissions and/or taxes. Moreover, the

complaints reported that victims still did not receive their withdrawal requests even after these additional fees were paid.

26. Google is committed to ensuring the integrity of Google Play. Upon discovering fraudulent behavior, including but not limited to, discovery through diligent investigation of victim complaints, Google suspends and shuts down fraudulent apps and other Google infrastructure associated with the Fraud Scheme (for example, Workspaces, Google Voice numbers) based on violations of the Developer Agreement or the Google Terms of Service.

27. Despite Google's diligence, the scheme continues to proliferate through new fraudulent apps that Defendants create through a continuing scheme of misrepresentations, including by creating new aliases and infrastructure as part of attempts to obfuscate their connection to suspended fraudulent apps. Google employs a risk-based approach to detecting and removing apps that do not comport with the Play Developer Program Policies, and it does not know of any live apps currently associated with Defendants. In total, Google has been able to identify and disable at least approximately 87 fraudulent apps ("the Fraudulent Apps") associated with Defendants and the Fraud Scheme over at least the past four years, based on business records, including subscriber information, indicating that they are tied by overlapping online infrastructure.

III. APPS INVOLVED IN SCHEME

28. Sections III.a–c below illustrate in more detail how the Fraud Scheme worked, providing illustrative examples of several of the Fraudulent Apps Defendants used to carry out their scheme. Google took steps to remove the Fraudulent Apps in question from Google Play after discovering Play Developer Program Policy violations.

a. Defendants Send Wayward Text Messages to Lure Victims into Investing Through the TionRT App

29. According to business records maintained by Google, the TionRT LTD ("TionRT") app was uploaded to Google Play in July 2022 by a developer account associated with Yunfeng Sun. TionRT purported to be a cryptocurrency exchange.

30. Members of the Fraud Scheme lured victims into investing using the TionRT app through wayward messages, either through text or social media platforms. The texts would purport to be from wrong numbers, but then the texters would strike up conversations with the victims, developing "friendships" and "romantic attachments." After gaining the victims' trust, the fraudsters would convince the victims to download and invest using the TionRT app in order to earn extra money. The "friend" or "romantic partner" would frequently guide the victim through the process, offering reassuring explanations of the financial and technical aspects of investing.

31. After building a relationship with the victims, members of the Fraud Scheme would suggest that the victims invest a small amount and then encourage them to withdraw some of the money once they started seeing returns. After this initial withdrawal succeeded, the reassured users would invest more money.

32. Defendants also made the app seem more legitimate through press releases on newswire service websites, such as "Digital Journal," that partner with public relations firms to distribute press releases for a fee. A Digital Journal press release[12] published July 15, 2022,

[12] *See* "Tionrt Exchange Overtakes Other Exchanges with Strong Trading Performance and Seamless Trading Experience," DIGITAL JOURNAL (July 15, 2022), https://www.digitaljournal.com/pr/tionrt-exchange-overtakes-other-exchanges-with-strong-trading-performance -and-seamless-trading-experience, attached as **Exhibit 6**.

includes TionRT's "cryptocurrency exchange" website and its Manhattan address, which public records confirm is the address of the corporate entity "TionRT LTD."[13]

33. Although the app seemed legitimate, victims eventually realized that it was a scam. Later withdrawals were not successful. When users tried to withdraw larger amounts of their "earnings," they were told to pay more money. When victims complained to the "friend" or "romantic partner" who had so helpfully guided them through the process, the "friend" or "romantic partner" would simply disappear.

34. Victims could not withdraw their funds, and the platform was eventually shut down.

b. Defendants Con "Affiliates" into Using the Starlight App

35. As early as February 2022, a firm known as the "Starlight Project" opened an office in Hohoe, Ghana, and launched a marketing campaign to convince Ghanaians to download and use the Starlight app, according to local press reports.[14] The Starlight Project offered a tantalizing premise: Ghanaians could earn money by watching videos and completing tasks on the app.

36. In at least one instance, the Starlight app promoters appeared to have organized an in-person conference that promoted the Starlight app as a way to make money in order to "solve your difficulties during the pandemic."[15]

---

[13] TionRT Ltd. lists its address as 244 Madison Avenue, Suite 1095, New York, NY 10016. "Tionrt Ltd.," NY Dept. of State, Division of Corporations Entity Information, https://apps.dos.ny.gov/publicInquiry/EntityDisplay, attached as **Exhibit 7**.

[14] *See* "Investments of more than 6,000 Starlight customers in stalemate, Agents at large," GHANA NEWS AGENCY (July 19, 2022) https://gna.org.gh/2022/07/investments-of-more-than-6000-starlight-customers-in-stalemate-agents-at-large/, attached as **Exhibit 8**.

[15] *See* "How to make money online in Ghana with the starlight app," YOUTUBE, https://www.youtube.com/watch?v=ddV76vmk3DY (posted Mar. 28, 2022).

37. Ads and videos soon appeared on various social media platforms, including Facebook, Instagram, and TikTok, encouraging people to download the Starlight app so that they could earn extra cash.

38. The TikTok ad, later uploaded to Instagram, featured two young women explaining that users could earn money by downloading the Starlight app for free, and walked viewers through how to register. A screenshot taken from the Instagram post is depicted below:

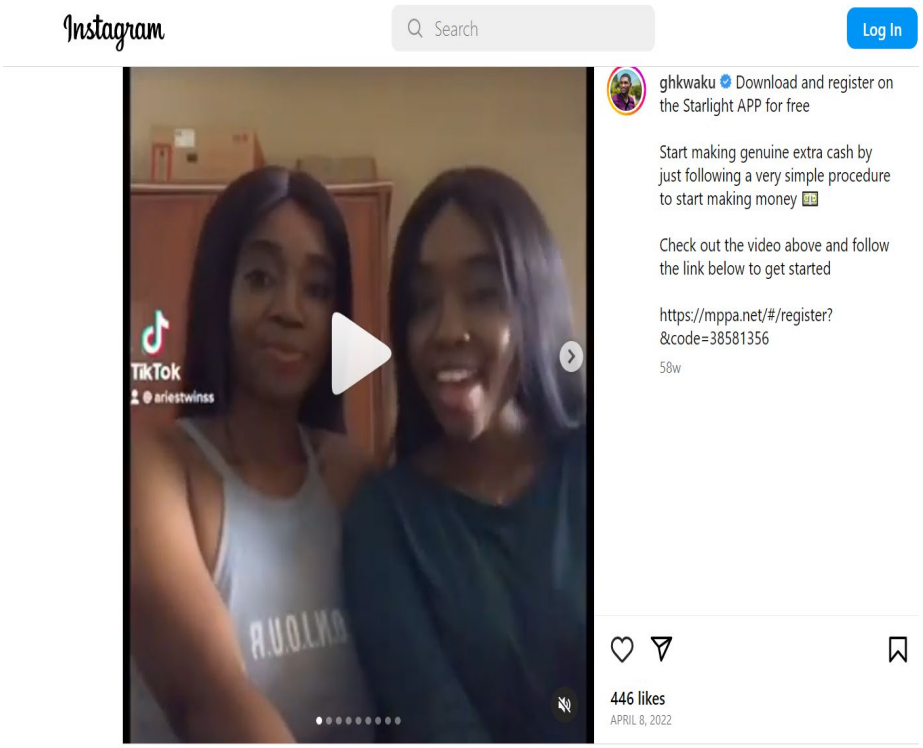

Figure 1
See Instagram, https://www.instagram.com/p/CcF8FDGKXVj/?hl=en (posted Apr. 8, 2022). See original TikTok post here: https://www.tiktok.com/amp/tag/starlightghana.

39. The social media advertisements represented that earning money on the app was simple and risk-free: the ads promised that users could earn commissions by simply watching videos.

40. Through these different channels, Defendants worked to convince victims to download the Starlight app, which they made available on Google Play, among other places.

41. Although Defendants advertised that earning money on the app involved only watching videos on the app and was otherwise free, victims soon discovered that they, as "affiliates," could not begin "earning" money until they invested initial capital through the app.

42. Starlight's promoters promised users that they could withdraw their capital at any time, but when users tried to withdraw their initial capital and earnings, they could not do so.[16] Press reports from Ghana state that when users tried to contact the Starlight Project about their money, their calls went unanswered[17] and that representatives of the firm were nowhere to be found.[18]

43. The Starlight app has been downloaded at least approximately 23,000 times, based on Google records. In abuse reports that victims submitted to Google about the Starlight app, victims said, among other things, that the Starlight Project is a "big scam," calling it a "Ponzi scheme" that has "scammed millions." The Ghana News Agency reported that more than 6,000 Ghanaians were left with nothing to show for their investments.

c. Defendants Use Fake Online Videos to Promote the Fake SkypeWallet App

44. According to business records maintained by Google, the SkypeWallet app was uploaded to Google Play by a developer account associated with Defendant Yunfeng Sun, a/k/a "Alphonse Sun." SkypeWallet purported to be a cryptocurrency exchange.

[16] *See* Exhibit 8.

[17] *Id*.

[18] *Id*.

45. Members of the Fraud Scheme used online videos to convince victims to download the app. To promote SkypeWallet, individuals in a YouTube video[19] claimed to be the leadership team of SkypeCoin, a company that purportedly sponsored a cryptocurrency by the same name. According to the stars of the video, SkypeCoin traded exclusively on SkypeWallet. The video guaranteed users that SkypeCoin would generate high rates of return, claiming that investors would earn at least approximately two percent in daily investment returns.

46. The purported leadership team of SkypeCoin featured in the SkypeWallet YouTube video appears in a similar promotional video for another publicly reported fraud scheme, OTCAI.[20] The OTCAI promotional video features an individual identified as "Romser Bennett," supposedly the "Founder of the OTCAI":

Figure 2
Screen capture of OTCAI promotional video, depicting "Romser Bennett" as OTCAI founder. *See* "This is OTCAI," YOUTUBE, https://www.youtube.com/watch?v=N3bUpnr1XA0 (posted May 11, 2022).

[19] "Skype wallet team video shooting manuscript," YouTube, https://www.youtube.com/watch?v=lOMzGarSSu4 (posted Mar. 17, 2022).

[20] *See* "OTCAI 'click a button' app Ponzi collapses, website gone," BEHIND MLM, https://behindmlm.com/companies/otcai-click-a-button-app-ponzi-collapses-website-gone/ (June 9, 2022), attached as **Exhibit 9**.

The SkypeWallet promotional video also features a Skype Coin "Co-Founder" identified by the same name, but the video features a different individual purporting to be that person:

Figure 3
Screen capture of SkypeWallet promotional video, depicting "Romser Bennett" as SkypeCoin co-founder. *See* "Skype wallet team video shooting manuscript," YOUTUBE, https://www.youtube.com/watch?v=lOMzGarSSu4 (posted Mar. 17, 2022).

The overlap does not end there. Both videos depict a different individual identified as an engineer named "Rodriguez." The OTCAI video's "Rodriguez," allegedly the technical leader of the OTCAI platform, is depicted below:

Figure 4
Screen capture of OTCAI promotional video, depicting "Rodriguez" as technical engineer at OTCAI. *See* "This is OTCAI," YOUTUBE, https://www.youtube.com/watch?v=N3bUpnr1XA0 (posted May 11, 2022).

The SkypeWallet video[21] depicts the same actor depicting "Rodriguez," the engineer from OTCAI, under the name "William Bryant," purportedly the Chief Operating Officer of Skype Coin:

Figure 5
Screen capture of SkypeWallet promotional video, depicting the same individual, but as "William Bryant," the purported Chief Operating Officer of Skype Coin. *See* "Skype wallet team video shooting manuscript," YouTube, https://www.youtube.com/watch?v=lOMzGarSSu4 (posted Mar. 17, 2022).

In addition, both the OTCAI and SkypeWallet promotional videos appear to have been filmed in the same room, based upon, among other things, identical chairs and window fixtures. The striking overlap in these videos demonstrates the brazenness of Defendants' scheme to recruit victims, likely involving paid actors playing different roles with identical pseudonyms.

47. The users Defendants enticed were quickly scammed out of their money. Not only did Defendants fail to make good on the guaranteed returns they had boasted, but users soon discovered that they could not withdraw their money as promised.

[21] The SkypeWallet video depicts a third actor, also identified as "Rodriguez," and described as technical engineer and head of platform technology at SkypeCoin.

48. The SkypeWallet app promoted in videos was fraudulent. Victims reported in abuse reports to Google that their accounts were frozen and that people affiliated with the apps told the victims that they needed to redeposit their account balances to unfreeze the account—to no avail. Victims thus lost not just their initial investments but also the additional funds they paid to try to unfreeze their accounts. The platform eventually shut down, and victims could not recoup their funds. Individual victims reported a range of losses, from thousands, up to 75 thousand dollars.

IV. DEFENDANTS' INVOLVEMENT IN THE SCHEME

49. A particular Google Workspace account ("Workspace Account-1") is associated with several Google Voice numbers that were suspended, based on victim complaints, for sending at least approximately 130 unsolicited spam text messages to recruit victims to the Fraud Scheme. Business records maintained by Google link payments associated with Workspace Account-1 to Defendant Yunfeng Sun. In addition, in the process of verifying Workspace Account-1, the customer provided New York State business records signed by Sun associated with Xiangying, Inc., a company registered in New York, New York.

50. As discussed above, Google has identified at least approximately 87 fraudulent apps linked to the scheme. Although Defendants attempted to obfuscate their connection to the apps by using a variety of different developer accounts and other infrastructure to register subsets of the apps, non-content business records maintained by Google and other publicly available information link the apps together, including by, among other things, overlapping links between registration email addresses and IP addresses used to host websites associated with the apps and their privacy policies.

51. Defendant Yunfeng Sun is an app developer and perpetrator of this scheme. In addition to being associated with payment information for Workspace Account-1, which used associated Google Voice numbers to promote the scheme, subscriber information and other publicly available information link Workspace Account-1 with a YouTube channel registered in his name ("YouTube Account-1"). YouTube Account-1, through which Sun promotes a dating app that he developed, and associated publicly available information indicates that Sun has advertised mobile app development and offers help to developers who have their apps rejected by online app stores. Subscriber records, including records associated with YouTube Account-1, indicate that Sun has control and dominion over a variety of other email accounts and infrastructure that are connected or associated with registering or uploading a substantial number of the Fraudulent Apps, including the Starlight and SkypeWallet apps.

52. Defendant Hongnam Cheung is another app developer and an active perpetrator of this scheme. According to business records maintained by Google and other publicly available information, one of the fraudulent applications that was linked to Defendant Yunfeng Sun, a/k/a "Alphonse Sun," has multiple overlapping Internet infrastructure links with another fraudulent application associated with the Fraud Scheme ("Fraud App-1"). Subscriber information associated with Fraud App-1 indicates that it was registered to and uploaded by an email address associated with Cheung ("Email Address-1"). Subscriber records maintained by Google, including records associated with Email Address-1, indicate that Cheung has control and dominion over other email accounts and infrastructure associated with at least approximately ten apps Defendants used as part of the Fraud Scheme.

V. HARM TO GOOGLE, USERS, AND THE PUBLIC

53. Google is committed to ensuring the integrity of Google Play and protecting its users. Upon discovering fraudulent behavior, Google must expend effort and resources to suspend fraudulent apps and associated Google infrastructure used to facilitate the fraud.

54. Despite Google's diligence, the scheme continues to proliferate, as Defendants have created new apps using new aliases and infrastructure, making repeated material misrepresentations regarding their identity and activities to Google as part of attempts to deceive Google into allowing their new apps into Google Play. So even though Google has removed a number of Defendants' fraudulent apps, Defendants will continue to harm Google and Google Play users.

55. That future harm builds on the substantial harm Defendants have already caused to Google and the users of Defendants' fraudulent apps.

56. The scheme has affected consumers across the globe. Specifically, Google records indicate that at least approximately 100,000 users have downloaded the Fraudulent Apps, including at least approximately 8,700 in the United States.

57. Defendants' Fraud Scheme has caused substantial financial losses to Google users. According to user complaints, financial losses appear to range from one hundred to tens of thousands of dollars per individual victim. Google believes that through the course of the Fraud Scheme, approximately 100,000 Google users have been victims based on download data for the Fraudulent Apps. Though significant, the harms extend far beyond the monetary losses to Google users.

58. Defendants have also caused substantial harm to Google. Defendants' scheme has caused Google to expend substantial resources to detect, deter, and disrupt Defendants' actions and thereby protect Google users and Google's products and services.

59. Google designed Google Play as an app-distribution platform open to all developers, allowing them to reach a wide audience of users. Google also provides content-neutral tools and resources to support developers as they grow their businesses. Google Play's well-earned reputation for successfully supporting developers and providing them with a large customer base makes it attractive to developers.

60. Yet Google Play can continue to be an app-distribution platform that users want to use only if users feel confident in the integrity of the apps. By using Google Play to conduct their Fraud Scheme, Defendants have threatened the integrity of Google Play and the user experience.

61. By using other Google products to support their scheme, Defendants also threaten the safety and integrity of those other products, including YouTube, Workspace, and Google Voice.

62. Defendant's scheme has thus impaired Google users' confidence and trust in Google, its services, and its platforms.

63. Defendants' ongoing scheme also harms the integrity of the Internet ecosystem as a whole by causing the public to lose confidence in utilizing the Internet for investing and other commerce.

CLAIMS FOR RELIEF

CLAIM 1
Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1962(c)–(d)

64. The allegations in paragraphs 1 through 63 of the Complaint are repeated and re-alleged as though fully set forth herein.

65. At all relevant times, Google was a person within the meaning of 18 U.S.C. § 1961(3).

66. At all relevant times, Google was a "person injured in his or her business or property by reason of a violation of" RICO within the meaning of 18 U.S.C. § 1964(c).

67. At all relevant times, each Defendant was a person within the meaning of 18 U.S.C. §§ 1961(3) and 1962(c).

The RICO Enterprise

68. Defendants are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise: creating and publishing more than 80 fraudulent investment platform apps and cryptocurrency exchange apps to deceive users into making investments. *See supra* ¶¶ 7–9.

69. Defendants Yunfeng Sun and Hongnam Cheung, along with their unnamed co-conspirators, controlled and used multiple corporate entities to carry out their fraudulent scheme, including an entity named "Xiangying Inc." whose registered address is in New York, NY.

Pattern of Racketeering Activity

70. At all relevant times, Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of an online consumer investment fraud

scheme through an unlawful pattern of racketeering activity involving hundreds of wire fraud predicate offenses (18 U.S.C. § 1343) within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c), with such conduct and activities affecting interstate and foreign commerce.

71. Since at least in or about 2019, Defendants committed numerous acts of wire fraud in furtherance of a single criminal scheme across at least approximately 87 fraudulent apps, by, among other things, making material misrepresentations to Google and individual victims with the goal to socially engineer and con victims into "investing" on their apps purporting to be cryptocurrency exchanges and investment platforms.

72. Google's injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Google will continue to be harmed by Defendants' ongoing conduct and continued violations.

73. Google is entitled to recover treble damages plus costs and attorneys' fees from Defendants in accordance with 18 U.S.C. § 1964(c).

Wire Fraud Predicate Offenses

74. Defendants committed wire fraud with the intent to defraud and obtain money by means of false or fraudulent pretenses. Defendants transmitted or caused to be transmitted writings, signs, and signals via wire communication in interstate or foreign commerce for the purpose of executing fraudulent schemes, in violation of 18 U.S.C. § 1343. For instance, Defendants carried out their Fraud Scheme by sending text messages, publishing videos on YouTube, and placing ads on social media platforms, including Facebook, Instagram, and TikTok, seeking to solicit funds from victims. Defendants further sent wire communications

to Google to onboard their apps to Google Play. Defendants also used the Fraudulent Apps to transmit wire communications that depicted false returns to victims of the Fraud Scheme.

75. Defendants executed the Fraud Scheme—including by creating, publishing, and promoting fraudulent investment platforms and cryptocurrency exchange apps—with the intent to obtain money from users by means of false and fraudulent pretenses.

76. In submitting their apps to Google for approval, over the course of the Fraud Scheme, Defendants made repeated material misrepresentations to Google so that the apps would be published on Google Play, for purposes of executing their Fraud Scheme.

77. Defendants also made material misrepresentations to Google users by sending SMS messages, operating affiliate programs, and deploying social media content in order to convince them to download and use their fraudulent investment platforms and cryptocurrency exchange apps with the intent to defraud and obtain money by means of false and fraudulent pretenses.

78. Google has suffered injury to its business as a result of these fraudulent schemes.

Conspiracy to Violate RICO

79. Defendants have undertaken the fraudulent acts described above as part of a common scheme. Defendants willfully, knowingly, and unlawfully conspired and agreed to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d). *See supra* ¶¶ 49–52.

80. Defendants knew that they were engaged in a conspiracy to commit multiple wire fraud predicate offenses, and they knew that their predicate acts of wire fraud were committed as part of such racketeering activity. Their agreement to directly or indirectly

participate in the conduct, management, or operation of the scheme was necessary in order to commit this pattern of racketeering activity.

81. Google has suffered injury to its business as a result of these actions.

CLAIM 2
Breach of Contract – Google Play App Signing Terms of Service

82. The allegations in paragraphs 1 through 63 of this Complaint are repeated and re-alleged as though fully set forth herein.

83. Defendant Yunfeng Sun entered into a valid, binding, and enforceable written contract with Google by expressly agreeing to the Google Play App Signing Terms of Service ("Play App ToS").

84. The Play App ToS require developers to represent and warrant that all information they provide to Google or users in connection with their products will be "current, true, accurate, supportable and complete."[22]

85. Defendant Yunfeng Sun breached the Play App ToS by providing false and inaccurate information to Google in connection with the apps he submitted for publication to Google Play. Sun repeatedly made multiple misrepresentations to Google in order to upload fraudulent apps to Google Play. These misrepresentations include, but are not limited to, misrepresentations about his identity, location, and the type and nature of the application being uploaded, as Defendant Sun made false and inaccurate representations to Google, which ultimately exposed approximately one hundred thousand consumer victims worldwide to his deceptive investment platforms and cryptocurrency exchange applications.

[22] The Developer Agreement, Section 11.4, attached as Exhibit 2. In consenting to be bound by the Play App ToS, Defendants consented to be bound by the Developer Agreement, which in turn requires Defendants to make these representations and warranties. *See* Play App ToS, https://play.google/play-app-signing-terms/, attached as **Exhibit 10**.

86. As a result of Defendant Sun's breach, Google has suffered economic damages in excess of $75,000 by incurring expenses to investigate Defendant Sun's breach and expending resources to remediate Defendant Sun's damage to the safety and integrity of Google's platforms.

CLAIM 3
Breach of Contract – Google's Developer Program Policies

87. The allegations in paragraphs 1 through 63 of this Complaint are repeated and re-alleged as though fully set forth herein.

88. Defendants entered into a valid, binding, and enforceable written contract with Google by expressly agreeing to Google's Developer Program Policies, which are incorporated into the Developer Agreement, at Section 4.1.

89. In accordance with these policies, Google does not allow apps or developer accounts that (1) misrepresent or conceal their primary purpose, (2) engage in coordinated activity to mislead users, or (3) coordinate with other apps, sites, developers or other accounts to conceal or misrepresent developer or app identity or other material details.

90. The Developer Program Policies also bar apps that expose users to deceptive or harmful financial products and services, including "those related to the management or investment of money and cryptocurrencies."[23]

91. Defendants misrepresented and concealed the primary purpose of their apps, convincing users that these apps were cryptocurrency exchanges or investment platforms operating as typical platforms for users to invest their funds in cryptocurrency or other investments.

[23] Developer Program Policies, attached as Exhibit 4.

92. Defendants engaged in coordinated efforts to mislead users by sending SMS messages, operating affiliate programs, and deploying social media content to convince users to install and invest in fraudulent cryptocurrency exchanges.

93. Defendants coordinated with their other fraudulent apps, their fraudulent cryptocurrency exchange websites, and other developers and their accounts to misrepresent their identities, the apps' identities, and the primary purpose of their apps—to operate fake cryptocurrency exchange apps in order to defraud users.

94. Google does not allow apps that attempt to deceive users. Google does not allow apps that promote or help create false or misleading information or claims conveyed through imagery, videos, and/or text.

95. Defendants breached Google's Developer Program Policies by attempting to deceive users by conveying false and misleading information through their apps in order to convince Google's users to deposit money through their apps and platforms.

96. As a result of Defendants' breach, Google has suffered economic damages in excess of $75,000 by incurring expenses to investigate Defendants' breach and expending resources to remediate Defendants' damage to the safety and integrity of Google's platforms.

CLAIM 4
Breach of Contract – Google Terms of Service

97. The allegations in paragraphs 1 through 63 of this Complaint are repeated and re-alleged as though fully set forth herein.

98. It is a violation of the Google Terms of Service ("Google ToS") to misuse the service, such as by defrauding others or using the service other than as permitted by law.[24]

[24] Google ToS, https://policies.google.com/terms?hl=en-US, attached as **Exhibit 11**.

99. Defendants misled and defrauded thousands of consumer victims, convincing them to install and invest in Defendants' fraudulent investment platforms and cryptocurrency exchange apps, in direct violation of the Google ToS.

100. As a result of Defendants' breach, Google has suffered economic damages in excess of $75,000 by incurring expenses to investigate Defendants' breach and expending resources to remediate Defendants' damage to the safety and integrity of Google's platforms.

CLAIM 5
Breach of Contract – YouTube Community Guidelines

101. The allegations in paragraphs 1 through 63 of this Complaint are repeated and re-alleged as though fully set forth herein.

102. Defendants' use of YouTube is subject to the YouTube Community Guidelines, incorporated into the YouTube Terms of Service.[25]

103. It is a violation of the YouTube Community Guidelines to post content to scam users by "making exaggerated promises, such as claims that viewers can get rich fast."[26] It is also a violation of the YouTube Community Guidelines to post content "promising money . . . if viewers . . . download an app, or perform other tasks."[27]

104. Defendants breached the YouTube Community Guidelines by creating and publishing videos to promote their fraudulent investment platforms and cryptocurrency exchange applications on YouTube.

[25] *See* YouTube Terms of Service, https://www.youtube.com/static?template=terms, attached as **Exhibit 12.**

[26] YouTube Community Guidelines: Spam, deceptive practices, & scams policies, https://support.google.com/youtube/answer/2801973?hl=en&ref_topic=9282365, attached as **Exhibit 13**.

[27] *Id.*

105. As a result of Defendants' breach, Google has suffered economic damages in excess of $75,000 by incurring expenses to investigate Defendants' breach and expending resources to remediate Defendants' damage to the safety and integrity of Google's platforms.

CLAIM 6
Breach of Contract – Google Voice Acceptable Use Policy

106. The allegations in paragraphs 1 through 63 of the Complaint are repeated and re-alleged as though fully set forth herein.

107. All Google Voice users must agree to the Google Voice Additional Terms of Service.[28] The Google Voice Additional Terms of Service incorporates within its terms the Google Voice Acceptable Use Policy.[29]

108. The Google Voice Acceptable Use Policy prohibits "sending commercial or promotional messages to a large number of users" by "creat[ing] multiple user accounts . . . under false or fraudulent pretenses."[30]

109. Defendants breached the Google Voice Acceptable Use Policy by acquiring numerous Google Voice numbers through their respective Google Workspace accounts and sending a significant number of spam SMS messages from these numbers.

110. As a result of Defendants' breach, Google has suffered economic damages in excess of $75,000 by incurring expenses to investigate Defendants' breach and expending resources to remediate Defendants' damage to the safety and integrity of Google's platforms.

---

[28] About Voice Terms of Service, https://support.google.com/voice/answer/9266964?hl=en&ref_topic=9273222&sjid=8767681408402182274-NC, attached as **Exhibit 14**.

[29] *See* Google Voice Additional Terms of Service, https://support.google.com/voice/answer/9231816?sjid=840138155963502559 8-NA, excerpted as **Exhibit 15.**

[30] Google Voice Acceptable Use Policy, https://support.google.com/voice/answer/9230450?hl=en, attached as **Exhibit 16**.

DEMAND FOR JURY TRIAL

111. Google respectfully requests a jury trial pursuant to Rule 38(b) of the Federal Rules of Civil Procedure for all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Google respectfully requests:

(a) That the Court enter a judgment against Defendants finding that Defendants have:

i. Engaged in acts or practices that violate the Racketeer Influenced and Corrupt Organizations Act; and

ii. Breached their contracts with Google in violation of California law.

(b) That the Court issue a permanent injunction enjoining and restraining Defendants and their officers, directors, principals, agents, servants, employees, successors, assigns, and all other persons and entities acting in participation with or conspiring with them or who are affiliated with the Defendant from:

i. Accessing or attempting to access Google's services, including but not limited to, Google Play, YouTube, and Google Voice;

ii. Creating or maintaining any Google accounts;

iii. Using any Google products or services to promote any of Defendants' apps, websites, or products;

iv. Engaging in any activity that violates Google's terms and any policies incorporated therein, including but not limited to, the Google Play App Signing Terms of Service, Google's Developer Program Policies, the YouTube Terms of Service, the Google Terms of Service, the Google

Voice Additional Terms of Service, or any related and/or incorporated policies; and

v. Assisting, aiding, or abetting any other person or entity in engaging in or performing any of the activities complained of in this Complaint.

(c) That the Court award Google all general, actual, and special damages that Google has sustained and will sustain as a consequence of Defendants' unlawful acts in an amount to be proved at trial;

(d) That the Court award Google all reasonable costs incurred in prosecuting this action, including reasonable attorneys' fees;

(e) That the Court award Google pre- and post-judgment interest; and

(f) That the Court grant Google such further relief as the Court considers just and equitable.

Dated: April 4, 2024

Respectfully submitted,

/s/ Timothy T. Howard

Timothy T. Howard
Scott A. Eisman
Photeine Lambridis
FRESHFIELDS BRUCKHAUS DERINGER US LLP
3 World Trade Center
175 Greenwich Street, 51st Floor
New York, New York 10007
T: +1 212 277 4000
timothy.howard@freshfields.com
scott.eisman@freshfields.com
photeine.lambridis@freshfields.com

Elvira Sihvola (*pro hac vice* application forthcoming)
FRESHFIELDS BRUCKHAUS DERINGER US LLP
700 13th St, NW, 10th Floor
Washington, D.C. 20005
T: +1 202 777 4500
elvira.sihvola@freshfields.com

Counsel for Plaintiff Google LLC