Wilmer Cutler Pickering Hale and Dorr LLP
Brendan R. McGuire (*pro hac vice*)
brendan.mcguire@wilmerhale.com
Phone: (212) 295-6278 / Fax: (212) 230-8888
Hallie B. Levin (*pro hac vice*)
hallie.levin@wilmerhale.com
Phone: (212) 295-6710 / Fax: (212) 230-8888
7 World Trade Center
250 Greenwich Street
New York, New York 10007

David Gringer (*pro hac vice pending*)
david.gringer@wilmerhale.com
Phone: (202) 663-6674 / Fax: (202) 663-6363
1875 Pennsylvania Avenue NW
Washington, DC 20006

Rebecca A. Girolamo, CA Bar No. 293422
becky.girolamo@wilmerhale.com
Phone: (213) 443-5343 / Fax: (213) 443-5400
350 South Grand Avenue, Suite 2100
Los Angeles, CA 90071

Attorneys for Defendants Global Risk Advisors LLC and Kevin Chalker

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

BROIDY CAPITAL MANAGEMENT LLC and ELLIOTT BROIDY,

Plaintiffs,

v.

STATE OF QATAR, STONINGTON STRATEGIES LLC, NICOLAS D. MUZIN, GLOBAL RISK ADVISORS LLC, KEVIN CHALKER, DAVID MARK POWELL, MOHAMMED BIN HAMAD BIN KHALIFA AL THANI, AHMED AL-RUMAIHI, and DOES 1-10,

Defendants.

Case No.: 2:18-CV-02421-JFW

The Honorable John F. Walter

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF GLOBAL RISK ADVISORS LLC'S AND KEVIN CHALKER'S MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

Hearing Date: Aug. 27, 2018
Time: 1:30 PM
Courtroom: 7A
Judge: John F. Walter
Am. Complaint Filed: May 24, 2018

Table of Contents

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES, RULES, AND REGULATIONS

PRELIMINARY STATEMENT

In a 70-page First Amended Complaint ("FAC"), stuffed with political intrigue and personally motivated attacks, Plaintiffs' have added Global Risk Advisors LLC ("GRA") and Kevin Chalker (together the "GRA Defendants") to this case without making a single relevant factual allegation. Despite the supposed extensive forensic analysis of Plaintiff Elliott Broidy's "advanced cyber unit," the initial iteration of Plaintiffs' tale did not mention the GRA Defendants once. Two months later, after this Court denied their request for a temporary restraining order (following Plaintiffs' motion that also did not mention the GRA Defendants once), Plaintiffs decided to write the GRA Defendants into the story. Grasping at straws to further Mr. Broidy's agenda and salvage this case, the Plaintiffs have alleged nothing more than a conspiracy ***theory***.

However, even Plaintiffs' conspiracy theory apparently supports only seven allegations in their FAC's "statement of facts" that reference GRA Defendants. And all but one rest solely on "information and belief." Plaintiffs never explain the basis for their purported belief, nor do they provide additional facts to support their "information and belief" assertions. The sole exception is an allegation that contains information in a publicly-filed business record, which establishes the known and irrelevant fact that GRA opened a subsidiary in Qatar months before the alleged conspiracy began. From this fact, and this fact alone, Plaintiffs ask the Court to make the implausible inference that the GRA Defendants participated in a global conspiracy that included "unknown threat actors," 10 John Does, two unnamed companies, and a retired diplomat. There are no proper allegations made to exclude the obvious alternative explanation to Plaintiffs' tale: the GRA Defendants were engaged in lawful activity to grow their business and did not play any role in the alleged hack of Plaintiffs' emails. Because *Twombly* and *Iqbal* require far more, the case must be dismissed.

Dismissal is appropriate for several additional independently-sufficient reasons. *First*, the FAC alleges that the GRA Defendants acted as an agent of a foreign state within the scope of its agency. This entitles the GRA Defendants to immunity, either derivatively from Qatar's immunity under the Foreign Sovereign Immunities Act, or under the long-standing common law doctrine of foreign official immunity. *Second*, the FAC's threadbare allegations do not include any suit-related contacts between any of the GRA Defendants and the State of California. Accordingly, the court lacks personal jurisdiction. *Third*, the FAC's conclusory allegations not only fail to state a claim against the GRA Defendants under Rule 8, but because the FAC alleges a unified course of fraudulent conduct, its claims sound in fraud, Rule 9(b)'s heightened pleading standard applies, and the allegations against the GRA Defendants are woefully short of meeting that strenuous standard. Each of the individual causes of action is also not properly pled, compelling dismissal.

BACKGROUND

A. The GRA Defendants

Global Risk Advisors LLC is headquartered in New York, New York (FAC ¶ 5), with an alleged subsidiary, Global Risk Advisors (EMEA) Limited ("GRA EMEA"), based in Doha, Qatar. FAC ¶ 25. GRA EMEA is licensed to engage in "advisory/consulting and IT consultancy work" and also to provide "cybersecurity, defense and security consultancy services."[1] GRA EMEA received its license to operate in Qatar before the alleged conspiracy commenced. *See* Ex. A to Mot. for Judicial Notice.

[1] Mot. for Judicial Notice Exs. A and B.

GRA's founder and CEO is Kevin Chalker. FAC ¶ 23. Mr. Chalker is a citizen of the United States and lives in New York State. *Id*. Before founding GRA, he served the United States through his work for the Central Intelligence Agency. *Id*. ¶ 5. After these initial references, Mr. Chalker is not mentioned by name again.[2]

B. Procedural History

On March 26, 2018, Plaintiffs, along with Ms. Robin Rosenzweig, filed their original Complaint, which did not reference the GRA Defendants. Dkt. 1. Six days later, Plaintiffs moved for a preliminary injunction. Dkt. 31. The motion and its accompanying exhibits did not reference the GRA Defendants. *Id.* This Court promptly denied Plaintiffs' motion, stating that it had "serious concerns" regarding its jurisdiction over Qatar, and holding that Plaintiffs had failed to establish a likelihood of success on the merits. Dkt. 37 at 2.

Plaintiffs filed the FAC on May 24, 2018. The FAC dropped Ms. Rosenzweig as a plaintiff without explanation, and added the GRA Defendants, among others. Dkt. 47.

C. Broidy Allegations

The seven allegations in the FAC's statement of facts that reference the GRA Defendants, save for one, are made solely on "information and belief." *See, e.g.*, FAC ¶ 7. The FAC does not supply the factual basis for any of these information-and-belief allegations.

Plaintiffs do allege that GRA EMEA received a license to operate in Qatar months before the alleged conspiracy began and the license they received included the word "cyber." FAC ¶ 95; Exs. A and B. This is the only allegation in the statement of facts that references the GRA Defendants that is *not* based solely on information and belief.

[2] Defendant David Powell has not been served. This motion is therefore limited to GRA and Mr. Chalker.

The FAC contains ***no factual allegations*** that explain why the fact that GRA EMEA was licensed to operate in Qatar to perform IT and cybersecurity work supports an inference that the GRA Defendants participated in the alleged conspiracy.

What the FAC does allege is that beginning in June 2017, the State of Qatar was subject to crippling economic sanctions orchestrated by Saudi Arabia and the United Arab Emirates. FAC ¶¶ 2, 52. The FAC alleges that Qatar responded to these sanctions by launching an "effort" to "influence public opinion" in the United States. FAC ¶ 2.

According to the FAC, "Qatar" decided to intrude into Broidy's email server and Google's servers, and then disseminate "the contents to U.S. news organizations." FAC ¶¶ 7, 9. The FAC alleges that the purpose of the hack of Broidy was to promote Qatar's "economic and commercial interests," *id*. ¶ 31, provide "retribution" for Broidy's public and private critiques of Qatar, *id*. ¶ 128, and to diminish Broidy's "influence within the United States." *Id*. ¶ 40.

Based only on "information and belief," the FAC alleges the GRA Defendants "personally supervised" aspects of an "information operation against Plaintiffs." *Id*. ¶ 6. The FAC does not state which aspects of the operation the GRA Defendants supervised, who from GRA supervised the "information operation," nor does it say what such supervision entailed. The FAC also alleges on information and belief that unspecified "Qatari Defendants" retained the GRA Defendants "to coordinate and implement the hack." *Id*. It does not state when this happened, where it happened, or what the supposed coordination and implementation entailed. Later, the FAC partially contradicts itself by claiming that the State of Qatar, *potentially through other [unnamed] Agent Defendants*, retained the GRA Defendants to "coordinate" the hack. *Id*. ¶ 93. The FAC then contradicts the allegation that the GRA Defendants "implement[ed]" the hack, by limiting the GRA Defendants' role in the alleged conspiracy—again on information and belief

exclusively—to introducing "Defendant State of Qatar" to unspecified "cyber mercenaries," *id*. ¶¶ 6-7, in "various [but unspecified] countries." *Id.*

Internal contradictions notwithstanding, the FAC supplies no detail regarding what the GRA Defendants did to coordinate or implement the hack. Critically, the FAC also does not allege that any of the supposed and unnamed "cyber threat actors" actually carried out the alleged hack on Broidy's emails.

The FAC contains no allegations in its statement of facts that identify any role played by the GRA Defendants in disseminating the materials obtained through the alleged hack. The FAC does allege—on information and belief—that "the State of Qatar, acting through [] Agent Defendants," was responsible for disseminating the emails and documents allegedly stolen from the Plaintiffs. FAC ¶ 126. The FAC does not allege that any emails were ever possessed—let alone disseminated—by the GRA Defendants.

ARGUMENT

I. The GRA Defendants Are Immune From Suit

The GRA Defendants are entitled to immunity under two related but distinct doctrines: (1) derivative sovereign immunity under the FSIA and (2) common law foreign official immunity.

A. Derivative Sovereign Immunity

Under the FSIA, "a foreign state is presumptively immune from the jurisdiction of United States courts … unless a specified exception applies." *Saudi Arabia v. Nelson*, 507 U.S. 349, 355 (1993). Qatar is indisputably a "foreign state" within the meaning of the FSIA, *see* FAC ¶ 19, and, for the reasons stated in Qatar's brief, *see* Dkt. 112-1, at 10-20, no specified exceptions apply here.

The GRA Defendants are entitled to sovereign immunity "derivative" of Qatar's immunity. The Supreme Court first recognized derivative sovereign immunity in *Yearsley v. W.A. Ross. Const. Co.*, which held that private contractors, as government

agents, are entitled to derivative sovereign immunity for work "authorized and directed by the Government of the United States." 309 U.S. 18, 20 (1940); *see also Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 673 (2016) (reaffirming *Yearsley* immunity). Pursuant to derivative immunity, "[w]hen a contractor acts under the authority and direction of the United States, it shares in the immunity enjoyed by the Government," *Zinck v. ITT Corp.*, 690 F. Supp. 1331, 1333 (S.D.N.Y. 1988); *see also Nielsen v. George Diamond Vogel Paint Co.*, 892 F.2d 1450, 1456 (9th Cir. 1990) (recognizing doctrine).

Courts have applied the agency principles underlying derivative immunity to foreign sovereign immunity claims. *See Butters v. Vance Int'l, Inc.*, 225 F.3d 462, 466 (4th Cir. 2000). The Fourth Circuit elucidated that "[i]t is but a small step to extend [*Yearsley* immunity] to the private agents of foreign governments." *Id.* Thus, an individual or entity is entitled to sovereign immunity deriving from a foreign state's immunity under the FSIA where the entity or individual is a contractor of a foreign sovereign and acts within the scope of the contracted duties. *See id*. Notably, the entitlement to derivative immunity is distinct from whether an individual qualifies for direct immunity under the FSIA and, as a result, derivative immunity is not dependent on whether the individual or entity qualifies as a "foreign state" or "agent or instrumentality" under the FSIA's text. *See id*.[3]

B. Foreign Official Immunity

The GRA Defendants are equally entitled to foreign official immunity under the common law, which extends more broadly than FSIA statutory immunity. *See, e.g.*, *Dogan v. Barak*, No. 2:15-CV-08130-ODW (GSJx), 2016 WL 6024416, at *5 (C.D. Cal.

[3] For that reason, the Supreme Court's decision in *Samantar v. Yousuf* (*Samantar I*), 560 U.S. 305 (2010), did not abolish derivative sovereign immunity. The *Samantar* Court made clear that it did "not doubt that in some circumstances the immunity of the foreign state extends to an individual for acts taken in his official capacity." *Id.* at 322.

Oct. 13, 2016); *see also Yousuf v. Samantar* (*Samantar II*), 699 F.3d 763, 774 (4th Cir. 2012) ("'[T]he immunity of a foreign state . . . extends to . . . any . . . public minister, official, *or agent of the state* with respect to acts performed in his official capacity if the effect of exercising jurisdiction would be to enforce a rule of law against the state.'" (quoting Restatement (2d) of Foreign Relations Law § 66(f)) (second, third, and fourth alterations in original) (emphasis added)).

Foreign official immunity is warranted where an agent of a foreign state is alleged to have acted "within the scope of said role and/or relationship [with the government entity]." *Farhang v. Indian Inst. of Tech.*, 655 F. App'x 569, 571 (9th Cir. 2016) (dismissing claims against individual defendant based on foreign official immunity).[4] Thus, common law foreign official immunity extends to entities or individuals who are not "foreign officials" themselves but who act on behalf of a foreign sovereign under the sovereign's direction. *See, e.g.*, *Wultz v. Bank of China Ltd.*, 32 F. Supp. 3d 486, 497-498 (S.D.N.Y. 2014); *Giraldo v. Drummond Co., Inc.*, 808 F. Supp. 2d 247, 249-250 (D.D.C. 2011), *aff'd*, 493 F. App'x 106 (D.C. Cir. 2012). Thus, an individual or entity need not be a government official to receive foreign official immunity. *See Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272, 277-278 (S.D.N.Y. 2015) (extending immunity to "non-governmental official" because "the scope of a foreign official's immunity . . . focuses on the official's acts, and not the official's status"); *Rishikof*, 70 F. Supp. 3d at 13 (holding immunity inquiry focuses on "the act itself and whether the act was performed on behalf of the foreign state," not "[t]he rank of the agent who performed the act"). Accordingly, individuals or entities employed by or working on behalf of a foreign state

---

[4] *See also Mireskandari v. Mayne*, No. CV 12-3861 JGB (MRWx), 2016 WL 1165896, at *16-17 (C.D. Cal. Mar. 23, 2016) (recognizing "the international law principle that sovereign immunity extends to an individual official acting on behalf of the foreign state"). Such immunity is often referred to as "conduct-based immunity." *See, e.g.*, *Samantar II*, 699 F.3d at 769; *Rishikof v. Mortada*, 70 F. Supp. 3d at 11-12.

qualify for foreign official immunity protection. *See Moriah*, 107 F. Supp. 3d at 275-276, 280; *Rishikof*, 70 F. Supp. 3d at 10, 12-13. Furthermore, because foreign official immunity is not a direct extension of the sovereign's immunity, it may apply even if the foreign sovereign is not immune under the FSIA. *See Rishikof*, 70 F. Supp. 3d at 17; *Weiming Chen v. Ying-jeou Ma*, No. 12-CV-5232 (NRB), 2013 WL 4437607, at *4 (S.D.N.Y. Aug. 19, 2013).

C. The GRA Defendants Are Entitled to Sovereign Immunity

Under either doctrine, the GRA Defendants are immune from suit. Applying the common law principles underlying both derivative and foreign official immunity, this Court has held that defendants were immune from suit based on allegedly unlawful actions while acting under the direction of a foreign state. *See, e.g.*, *Mayne*, 2016 WL 1165896, at *16-17. In *Mayne*, for instance, the Court held that the defendants (individuals employed by a regulatory agency) were entitled to immunity because the complaint alleged that the challenged conduct was undertaken at the direction of government officials and that the government officials "orchestrated and implemented" the purported unlawful conduct. *See id.* at 18; *see also, e.g.*, *Lewis v. Mutond*, 258 F. Supp. 3d 168, 173-174 (D.D.C. 2017) (holding defendants were entitled to foreign official immunity because they were agents of the Democratic Republic of Congo and the alleged actions were part of their official duties); *Moriah*, 107 F. Supp. 3d at 275-276, 280 (granting foreign official immunity to independent advisor that acted "at the request of and at the direction of" government officials); *Rishikof*, 70 F. Supp. 3d at 12-15 (holding delivery driver defendant was entitled to foreign official immunity because he was an agent of the Swiss Confederation and "acting within the scope of his employment" when traffic accident occurred).

Here, the FAC alleges that the GRA Defendants engaged in the challenged conduct solely at Qatar's direction. For instance, the FAC alleges that Qatar "orchestrate[d] and

execute[d]" the alleged hacking and subsequent dissemination of the materials, FAC ¶ 1, that the Qatari Defendants "retained and used the GRA Defendants" to coordinate the alleged hacking, *id.* ¶ 6, and that the GRA Defendants were "retained to [act] . . . on behalf of Defendant State of Qatar," *id.* ¶ 96. In addition, the GRA Defendants are not alleged to have had any motivation independent of Qatar's alleged interests for engaging in the conduct, nor are they alleged to have exceeded the bounds of their agency on behalf of Qatar.

Thus, it is clear that the GRA Defendants are alleged to have acted at Qatar's direction, and within the scope of their agency, which places the GRA Defendants' alleged conduct squarely within the parameters of both derivative and foreign official immunity. *See, e.g.*, *Farhang*, 655 F. App'x at 571; *Samantar II*, 699 F.3d at 775.

Furthermore, Plaintiffs' own legal theories to invoke jurisdiction under the FSIA depend on this Court finding that the GRA Defendants (and the other Agent Defendants) were acting at the direction of Qatar. The noncommercial tort exception to the FSIA requires a finding "that the tortious acts of individual employees of the sovereign were undertaken within the scope of employment." *Rishikof*, 70 F. Supp. 3d at 14. If the GRA Defendants were not acting at Qatar's direction, then their actions could not be imputed to Qatar and "the tortious activity exception would not apply." *Id.*; *see also* FAC ¶ 3 (alleging "Qatar (which as a principal is bound by the actions and knowledge of its agents) hired numerous United States agents"); *id.* ¶ 30 (alleging this Court has jurisdiction over Qatar based on the Defendants' tortious conduct). Similarly, Plaintiffs seek to rely on Qatar's alleged "commercial contracts" with the Defendants to establish jurisdiction under the FSIA's commercial activity exception. *See* FAC ¶ 31. Even assuming that this exception applies (and it does not), Plaintiffs allege that the GRA Defendants were following Qatar's direction pursuant to "the contract."

Immunity is especially warranted here given that Plaintiffs' allegations rest entirely on core sovereign functions and implicate politics and diplomatic relations between foreign states. *See, e.g.*, FAC ¶¶ 2, 4, 27, 54-55, 57-60 (alleging Defendants endeavored to reverse a "Trump-endorsed blockade by [Qatar's] Arab neighbors"). As this Court has explained, immunity is particularly apt where actions on behalf of the foreign state were "inextricably intertwined with politics, diplomacy, foreign policy, and even economics." *Dogan*, 2016 WL 6024416, at *9; *see also Kirschenbaum v. 650 Fifth Ave.*, 257 F. Supp. 3d 463, 532 (S.D.N.Y. 2017) (holding foreign sovereign has a national interest in maintaining access to U.S. markets where the "government has been under trade embargos for decades").

II. There is No Personal Jurisdiction Over The GRA Defendants

Plaintiffs have the burden of establishing that the Court has personal jurisdiction over the GRA Defendants. *Boschetto v. Hansing*, 539 F.3d 1011, 1015 (9th Cir. 2008). Plaintiffs seek to invoke specific personal jurisdiction over the GRA Defendants. FAC ¶ 35. Their efforts are unavailing.

Because the GRA Defendants are nonresidents and Plaintiffs are asserting intentional tort claims, the Plaintiffs must establish that (1) the GRA Defendants "purposefully direct[ed] [their] activities toward [California]" (the "purposeful direction" test) and (2) "the claim [is] one which arises out of or relates to the [GRA Defendants' California]-related activities." *Axiom Foods, Inc. v. Acerchem UK Ltd.*, 874 F.3d 1064, 1068 (9th Cir. 2017). "If the plaintiff fails to satisfy either of these prongs, personal jurisdiction is not established[.]" *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004).

Plaintiffs have failed to establish—as they must—that the first prong of the test has been satisfied. *Axiom*, 874 F.3d at 1069. Plaintiffs do allege, in wholly conclusory fashion, that the "Agent Defendants," which may or may not include the GRA

Defendants (the FAC is consistently unclear) supposedly "targeted Plaintiffs in California and directed their tortious conduct towards Plaintiffs in California, with knowledge and intent that Plaintiffs suffer harm in California." FAC ¶ 35. This threadbare recital of supposed facts is little more than a set of legal conclusions and cannot support personal jurisdiction, even if the allegations are read to include the GRA Defendants. *See Ashcroft v. Iqbal*, 556 U.S. 662, 686 (2009) ("[T]he Federal Rules do not require courts to credit a complaint's conclusory statements without reference to its factual context.").

Even if Plaintiffs' allegation that Defendants targeted Plaintiffs "in California" were credited, it is insufficient to establish specific personal jurisdiction. "The foreseeability of injury in a forum is not a sufficient benchmark for exercising personal jurisdiction." *Axiom*, 874 F.3d at 1070 (internal quotation marks and citation omitted). Nor are sufficient contacts established merely because a defendant "directed his conduct at plaintiffs" whom he knew resided in the forum state. *Walden v. Fiore*, 571 U.S. 277, 289 (2014). Such tests would "impermissibly allow[] a plaintiff's contacts with the defendant and forum to drive the jurisdictional analysis." *Id.*

Instead, plaintiffs are required to show that the alleged suit-related conduct of the defendant creates a "substantial connection" to California. *Id.* at 284. But the GRA Defendants ***are not alleged to have any connections in California related to the lawsuit***. *See* FAC ¶¶ 93-95. Even as told by the Plaintiffs, their conspiracy theory focuses on GRA EMEA's supposed operations in Qatar, and introductions made by unidentified GRA Defendants to unspecified individuals around the world, none of whom are alleged to be in California. *See* FAC ¶¶ 94-95. Furthermore, there is nothing "California-centric" about the allegations, nor is there any harm felt by the plaintiffs unique to conduct allegedly engaged in by the GRA Defendants in California (or even any conduct allegedly engaged in by the so-called "agent defendants"), both of which the law requires. *See Walden*, 571 U.S. at 289-290.

Plaintiffs instead rest their assertion of personal jurisdiction on the happenstance that *they* (and their computers) reside in California and that Defendants knew where Plaintiffs lived. *See* FAC ¶¶ 128-129. Again, this is insufficient. *See, e.g.*, *Republic of Kazakhstan v. Ketebaev*, No. 17-CV-00246-LHK, 2017 WL 6539897, at *7 (N.D. Cal. Dec. 21, 2017) (hacking email servers that happened to be located in California "not enough to confer personal jurisdiction" over defendant); *NexGen HBM, Inc. v. ListReports, Inc.*, No. 16-CV-3143 (SRN/FLN), 2017 WL 4040808, at *1-5, 10-14 (D. Minn. Sept. 12, 2017) (finding purposeful direction test not satisfied in forum where defendants were located where plaintiff allegedly misappropriated trade secrets by accessing plaintiff's website). Further distancing themselves from any California contacts, Plaintiffs now contend that the alleged hack took place in ***Vermont***. *See* Dkt. 133 at 9.

To be consistent with due process, specific personal jurisdiction must be predicated on contacts that the "'defendant *himself*' creates with the forum State," and "not the defendant's contacts with persons who reside there." *Walden*, 571 U.S. at 284-285 (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985)). Plaintiffs fail to meet this requirement under the law "and [accordingly] the case must be dismissed." *Boschetto*, 539 F.3d at 1016

Plaintiffs also cannot show that their claims "arise" out of any California-specific contacts of the GRA Defendants. This prong is satisfied only if Plaintiffs would not have been injured "but for" the GRA Defendants' conduct *in California*. *Rio Props. Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1021 (9th Cir. 2002). As explained, Plaintiffs have failed to allege any such conduct on the part of the GRA Defendants. But even if such conduct had been alleged, Plaintiffs' claims arise out of contacts the GRA Defendants are alleged to have had in Qatar or in the location of the "known or unknown" threat actors whom the GRA Defendants allegedly introduced to Qatar. Neither is alleged to have

occurred in California. Accordingly, Plaintiffs have not shown that their injuries would have been suffered but-for the GRA Defendants' suit-related conduct in California.

III. Plaintiffs Fail to State a Claim Under Rule 8

To survive a motion to dismiss under Rule 8, a complaint must "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face'." *Iqbal*, 556 U.S. at 678. "While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations." *Id* at 679–683. The FAC offers little more than a conclusory "formulaic recitation of the elements" of the alleged causes of action and should accordingly be dismissed under Fed. R. Civ. P. 12(b)(6). *Id*. at 681.

A. The FAC's Conclusory Allegations Fail to State a Claim

At its core, the FAC rests on the allegation that an IP address in Qatar was used to access BCM's server in California and Plaintiffs' suspicion that Qatar wished to target them. FAC ¶ 115. As this Court has already recognized in its order denying a temporary restraining order, that allegation and inference are insufficient to support the conclusion that the State of Qatar ordered or authorized hacks on Plaintiffs. *See* Dkt. 37.

Even if these allegations were somehow sufficient to *state a claim* against Qatar, they are plainly insufficient to do so against the GRA Defendants. The GRA Defendants' involvement in the case appears to stem solely from the unremarkable fact that GRA opened an office in Qatar approximately two months before the alleged hacks began. FAC ¶ 95; Ex. 1. Based on that fact alone—the only allegation in the FAC's statement of facts made against the GRA Defendants not premised on "information and belief"—the FAC asserts legal conclusions and implausible inferences regarding the GRA Defendants' alleged culpability. *See* FAC ¶¶ 93-96.

As a threshold issue, if the FAC's allegation regarding GRA launching a subsidiary in Qatar—the sole creditable allegation made against the GRA Defendants—were

sufficient to state a claim, *any* lawsuit against a business with an operating subsidiary in Qatar would survive a motion to dismiss for conduct alleged to have been undertaken at the direction of Qatar. Such an absurd result would not stand pre-*Twombly* and *Iqbal*, and certainly does not hold today. *See, e.g.*, *Teledyne Risi, Inc. v. Martin-Baker Aircraft Co. Ltd.*, No. CV 15-07936 SJO (GJSx), 2016 WL 8857029, at *4 (C.D. Cal. Feb. 2, 2016) (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)) (dismissing complaint for failure to state a claim where sole factual allegations linking defendant to unlawful conduct were plaintiff's location of incorporation and status as a corporate affiliate of co-defendant).

Plaintiffs ask the Court to infer that because GRA opened an office in Qatar before the alleged conspiracy commenced they coordinated the hacking scheme. Plaintiffs never explain why this inference is plausible; it is not. GRA publicly disclosed its Qatari subsidiary pursuant to Qatari law. It is completely implausible to believe that if the GRA Defendants established a subsidiary to facilitate a hacking scheme they would have publicly broadcast the opening of the subsidiary; it is even more implausible that Qatar would have compelled that they do so. The mere fact that the GRA Defendants opened a subsidiary with operations in Qatar before the alleged hacks began cannot—to put it mildly—support a plausible inference that the GRA Defendants engaged in the alleged unlawful conduct. *See, e.g.*, *In re Century Aluminum Co. Sec. Litig.*, 729 F.3d 1104, 1108 (9th Cir. 2013) ("When faced with two possible explanations, only one of which can be true and only one of which results in liability, plaintiffs cannot offer allegations that are 'merely consistent with' their favored explanation but are also consistent with the alternative explanation. Something more is needed, such as facts tending to exclude the possibility that the alternative explanation is true, in order to render plaintiffs' allegations plausible."). Plaintiffs allege no such facts.

The FAC's few other stray references to the GRA Defendants are vague and conclusory, are also alleged on information and belief, should not be credited even on a motion to dismiss (*see Iqbal*, 556 U.S. at 681), and even if they were credited, fail to push the FAC across the line of plausibility. The FAC alleges, for example, (perforce on information and belief) that the GRA Defendants "supervised" and "were responsible" (FAC ¶ 94) for the hacks. But the FAC fails to supply any factual details to describe what this supervision and responsibility allegedly entailed, when it took place, or how it was effectuated. Without more, these are mere legal conclusions. The FAC states on information and belief that the GRA Defendants "introduced [the] Defendant State of Qatar to known and unknown threat actors to execute the attacks," but includes no facts as to when and how these introductions took place, nor whom they involved. *Id.* The FAC also vaguely alleges that GRA Defendants "made it clear" within "the small community of former U.S. government offensive cyber operatives" that they had been "retained to conduct or coordinate offensive cyber operations on behalf of Defendant State of Qatar." *Id.* ¶ 96. Not only is the statement that the GRA Defendants were "retained to conduct . . . offensive cyber operations" wholly conclusory, vague and lacking in factual support, but the GRA Defendants are left to guess as to who made the statement, to whom the statement was made, when the statement was made, and how the GRA Defendants allegedly "made [this] clear." Moreover, even if taken as true, the statement on its own terms makes no reference to Plaintiffs. In sum, none of the allegations about the GRA Defendants, even taken as true, are inconsistent with the "obvious alternative explanation" that the GRA Defendants' work for Qatar was wholly unrelated to Plaintiffs and completely lawful. *See, e.g.*, *Iqbal*, 555 U.S. at 682 (allegations are implausible where complaint fails to allege facts sufficient to dispel more likely inferences).

B. The FAC's Allegations on "Information and Belief" Are Insufficient

The GRA Defendants must also be dismissed from the case because all but one of the allegations in the FAC's statement of facts pertaining specifically to the GRA Defendants (the previously discussed allegation regarding opening an office in Qatar (FAC ¶¶ 25, 95)) are based "on information and belief." Post-*Iqbal*, where a complaint is premised solely on allegations based on information and belief, without additional factual support, the complaint is "insufficient as a matter of law." *Tarantino v. Gawker Media, LLC*, No. CV 14-603-JFW (FFMx), 2014 WL 2434647, at *5 (C.D. Cal. Apr. 22, 2014) (Walter, J.); *see also Vivendi SA v. T–Mobile USA Inc.*, 586 F.3d 689, 694 (9th Cir. 2009) (finding insufficient allegations based "upon information and belief" where no further facts were alleged); *Simonyan v. Ally Fin. Inc.*, No. CV 12-8495-JFW (FMOx), 2013 WL 45453, at *2 (C.D. Cal. Jan. 3, 2013) (Walter, J.) (noting that "factual allegations ... based on 'information and belief' and contain[ing] nothing more than a rote recitation of the required elements of each respective claim ... fall well short of the requirements set forth in *Iqbal*."); *United States v. Ctr. for Diagnostic Imaging, Inc.*, 787 F. Supp. 2d 1213, 1221 (W.D. Wash. Apr. 4. 2011) (holding that "[a] plaintiff relying on 'information and belief' must state the factual basis for the belief.").

Plaintiffs supply no basis for their "information and belief" allegations. For example, the FAC alleges "[o]n information and belief, the GRA Defendants introduced Defendant State of Qatar to known and unknown threat actors to execute the attacks, and supervised this work and were responsible for the overall execution of the project." FAC ¶ 94. This is the key allegation linking the GRA Defendants to the alleged hacks and yet it is premised on "information and belief" with no additional explanation for the belief.

As deficient as the FAC is with regard to the GRA Defendants generally, the allegations pertaining to the two named GRA employees, Kevin Chalker and David Powell, are even thinner. With respect to Kevin Chalker, the FAC alleges (without basis)

only that he "is a former CIA cyber-operative who runs GRA." *Id.* ¶ 5. The FAC does not supply any detail about Mr. Chalker's role in the purported conspiracy, nor does it define the term "cyber-operative," which is not even a real word. Similarly, with respect to David Powell, the FAC identifies him as a conspirator because he allegedly established GRA's office in Qatar "weeks prior to the commencement of the attack on Plaintiffs." *Id.*

C. The FAC's Civil Conspiracy Allegations Also Fail

To establish a conspiracy, the FAC relies solely on the allegation that Qatar retained the GRA Defendants to join the conspiracy. Such an allegation is nothing more than a thinly veiled legal conclusion. *See Villegas v. Wells Fargo Bank, N.A.*, No. C 12-02004 LB, 2012 WL 4097747, at *5 (N.D. Cal. Sept. 17, 2012) (dismissing conspiracy claim where "Plaintiffs merely state conclusory allegations of cooperation and an agency relationship between [alleged co-conspirators]"); *Carpenter v. Thrifty Auto Sales*, No. EDCV09-02233 DMG (DTBx), 2010 WL 11595928, at *5 (C.D. Cal. July 30, 2010) (same). It should not be credited as fact.

With no factual allegation from which to plausibly infer the formation of a conspiracy involving the GRA Defendants, the FAC then states that the Defendants "while in the United States, conspired to unlawfully access [plaintiffs' communications] and that they "carried out that conspiracy . . . in both the United States and abroad." FAC ¶¶ 128-129. These conclusory allegations are insufficient to connect the GRA Defendants to any illegal conspiracy. *See Kendall v. Visa U.S.A., Inc.*, 518 F.3d 1042, 1048 (9th Cir. 2008) (upholding dismissal of conspiracy claims where Plaintiffs alleged only "ultimate facts, such as conspiracy, and legal conclusions.").

Even if the factual allegations could support the legal theories alleged—and as to the GRA Defendants they cannot—the FAC's "shotgun pleading" dooms Plaintiffs' claims. The FAC lumps together all Defendants and recites the elements of the causes of

action against them without any factual allegation to demonstrate each individual Defendant's alleged culpability. Courts have repeatedly rejected such "shotgun pleadings" at the dismissal stage. *See, e.g.*, *Nissen v. Lindquist*, No. C16-5093 BHS, 2017 WL 26843, at *1–2 (W.D. Wash. Jan. 3, 2017) ("The unifying characteristic of all types of shotgun pleadings is that they fail to one degree or another, and in one way or another, to give the defendants adequate notice of the claims against them and the grounds upon which each claim rests."); *Mason v. Cty. of Orange*, 251 F.R.D. 562, 563 (C.D. Cal. 2008) ("typical shotgun pleading" is inadequate).

The FAC asserts all ten causes of action against all fourteen Defendants, without any distinction in the recitation of the elements of each claim as to the specific actions taken by the individual Defendants. The FAC includes no detail as to each Defendant's alleged actions and culpability in the various claims asserted by Plaintiffs. Instead, for each cause of action, the FAC includes a formulaic recitation of the elements of that claim, lumping together fourteen Defendants, including ten "John Doe" Defendants. *See, e.g.*, FAC ¶ 143 ("Defendants engaged in deliberate spearfishing attacks"); *id*. ¶ 156 ("Defendants knowingly and unlawfully accessed or caused to be accessed computers…"). These shotgun allegations fail to put the GRA Defendants on notice of the alleged conduct for which they are being sued and should be dismissed accordingly. *See McFadden v. Deutsche Bank Nat'l Trust*, No. 2:10-CV-03004 JAM KJN PS, 2011 WL 3606797, at *7 (E.D. Cal. Aug. 16, 2011) (failure to differentiate among defendants "leaving each defendant to guess about its own allegedly unlawful conduct . . . requires dismissal"); *Mankuyan v. Cach*, No. 12-CV-08356 RGK, 2012 WL 6199938, at *3 (C.D. Cal. Dec. 11, 2012) ("A court should dismiss a complaint that makes undifferentiated allegations against multiple defendants[.]").

IV. Rule 9(b)'s Heightened Pleading Standard Applies

Even if the Court somehow held the FAC satisfied Rule 8, it fails the more stringent standard in Rule 9, which applies here. Fed. R. Civ. P. 9(b) provides that "[i]n alleging fraud . . ., a party must state with particularity the circumstances constituting fraud[.]" Because the FAC alleges a "unified course of fraudulent conduct," Rule 9(b)'s heightened pleading standard applies. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1104 (9th Cir. 2003). Plaintiffs do not meet this standard.

In the Ninth Circuit, it is the allegation of fraudulent conduct—and not the title of the claim—that compels application of Rule 9(b). Hence, when a claim is "grounded in fraud" or "sound in fraud," the "pleading of that claim as a whole must satisfy the particularity requirement of Rule 9(b)." *Id*. at 1103-1104. A claim can sound in fraud "even if the word 'fraud' is not used." *Id*. at 1105; *see also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009); *Tae Hee Lee v. Toyota Motor Sales, U.S.A.*, 992 F. Supp. 2d 962, 971 (C.D. Cal. 2014) (Walter, J.) ("Rule 9(b) applies not only where fraud is an essential element of a claim, but where a claim is 'grounded in fraud' or 'sounds in fraud'"). This precedent controls here.

Plaintiffs allege two fraud claims titled as such, invoking both the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030(a)(2)(C) & (a)(5) (emphasis added), and the California Comprehensive Computer Data Access and Fraud Act ("CCCDAFA"), Cal. Pen. Code § 502, both of which are subject to Rule 9(b). *See, e.g.*, *Oracle America, Inc. v. Service Key, LLC*, No. C 12-00790 SBA, 2012 WL 6019580, at *6-7 (N.D. Cal. Dec. 3, 2012) (applying Rule 9(b) to CFAA claim alleging defendants fraudulently obtained third-party passwords and used them to access defendant's website).

But Rule 9(b)'s heightened pleading standard applies to the entire FAC because it alleges that the Defendants engaged in a unified course of fraudulent conduct. Indeed, the FAC is premised on allegations that the Defendants effectuated a hack of Plaintiffs'

email servers by "***fraudulently*** registering online website domains," in order to "***deceive*** several persons in the United States into providing their email login credentials." FAC ¶ 15 (emphasis added). This alleged course of conduct plainly sounds in fraud and therefore triggers Rule 9(b)'s more stringent standard. *See, e.g.*, *Vess*, 317 F.3d at 1103; *FTC v. Lights of America, Inc.*, 760 F. Supp. 2d 848, 852-855 (C.D. Cal. 2010) (applying Rule 9(b) to allegations of deception); *Satmodo, LLC v. Whenever Commc'ns, LLC*, No. 17-CV-0192-AJB NLS, 2017 WL 1365839, at *2-3 (S.D. Cal. Apr. 14, 2017) (applying Rule 9(b) to allegations that Defendants "improperly accessed Plaintiff's computers without authorization" (emphasis omitted)); *United States v. Scan Health Plan*, No. CV 09-5013-JFW (JEMx), 2017 WL 4564722, at *7 (C.D. Cal. Oct. 5, 2017) (Walter, J.) ("Because claims under the False Claims Act sound in fraud, they must meet Rule 9(b)[.]").

Rule 9(b) demands that the circumstances constituting the alleged fraud be "specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Bly-Magee v. California*, 236 F.3d 1014, 1019 (9th Cir. 2001). To comply with the specificity requirement of Rule 9(b), a complaint may not "lump multiple defendants together." *UMG Recordings, Inc. v. Glob. Eagle Entm't, Inc.*, 117 F. Supp. 3d 1092, 1108 (C.D. Cal. 2015) (quoting *Swartz v. KPMG LLP*, 476 F.3d 756, 764-765 (9th Cir. 2007)). Rather, plaintiffs must "differentiate their allegations when suing more than one defendant . . . and inform each defendant separately of the allegations surrounding his alleged participation in the fraud." *Id.*; *see also Scan Health*, 2017 WL 4564722, at *7 (dismissing complaint under Rule 9(b) that failed to "identify the role of each defendant in the alleged fraudulent scheme").

The FAC repeatedly violates this rule, consistently lumping together various formulations of the "Agent Defendants" and "Defendants" generally in lieu of allegations

specific to each Defendant. *See, e.g.*, FAC ¶ 152 ("Defendants have violated § 502(c)(4) by knowingly accessing and without permission altering Plaintiffs' data, which resided in Plaintiffs' and Google's computers, computer systems or computer networks, all of which were located in California. . . ."); *id.* ¶ 190 ("Defendants willfully and intentionally accessed without authorization a facility through which an electronic communication service is provided. . . ."). The Ninth Circuit has repeatedly rejected under Rule 9(b) shotgun allegations like those made here. *See, e.g.*, *Swartz*, 476 F.3d at 764; *Scan Health*, 2017 WL 4564722, at *7.

Moreover, the FAC fails to supply the requisite "'who, what, when, where and how of the misconduct charged.'" *Vess*, 317 F.3d at 1106. There are simply no creditable facts alleged against the GRA Defendants that provide any of the necessary detail, including who from GRA was involved, what that involvement consisted of, and how the GRA Defendants "coordinated" the hacking. Plaintiffs just allege a hack occurred and that it was "coordinated" by the GRA Defendants. Nothing more. At minimum, Plaintiffs were required to "'identif[y] the role of [each] defendant[ ] in the alleged fraudulent scheme.'" *Swartz*, 476 F.3d at 765. As to the GRA Defendants, the Plaintiffs have failed to do so.

Furthermore, while Plaintiffs' "information and belief" allegations doom the FAC under Rule 8, their deficiencies are more pronounced under Rule 9(b). Factual allegations based solely on information and belief—like those made here—"usually do not satisfy the particularity requirements under Rule 9(b)." *Moore v. Kayport Package Exp., Inc.*, 885 F.2d 531, 540 (9th Cir. 1989); *see also Simonyan*, 2013 WL 45453, at *2 (dismissing complaint based on information and belief allegations containing nothing more than a rote recitation of each claim's elements). Because these information-and-belief allegations are no different, the FAC must be dismissed.

V. The Individual Counts Fail to State A Claim Against The GRA Defendants

A. The FAC Does Not Allege GRA Defendants Themselves Accessed Plaintiffs' Computers or Servers

Plaintiffs have failed to support their "information and belief" allegations with any creditable factual allegations that the GRA Defendants themselves unlawfully or improperly accessed Plaintiffs' computers or servers. Accordingly, Counts I, II, IV, VI, and VIII should be dismissed.

Counts I & II. Claims brought under the CFAA must be alleged with particularity, *Oracle*, 2012 WL 6019580, at *6-7, which plaintiffs have not done. Furthermore, Plaintiffs' CFAA claim fails because they do not adequately allege the GRA Defendants accessed Plaintiffs' computer servers. "[T]he CFAA requires that the individual *actually access* the information, not merely receive it from a third party." *See Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc.*, 953 F. Supp. 2d 1290, 1297 (S.D. Ga. 2013) (emphasis added); *see also Flynn v. Liner et al.*, No. 3:09-CV-00422-PMP-RAM, 2011 WL 2847712, at *3 (D. Nev. July 15, 2011) (no "aiding and abetting liability" under CFAA). Plaintiffs baldly state in Count I of the FAC that "the GRA Defendants, accessed or caused to be accessed Plaintiffs' servers." FAC ¶ 141. However, this statement is nothing more than a "formulaic recitation of a cause of action's elements," *Twombly*, 550 U.S. at 545 , and absent further factual allegations (allegations not made in the FAC), fails to state a claim.

As with Count I, CCCDAFA claims are subject to a heightened pleading standard, as its statutory language mimics the CFAA. Cal. Penal Code § 502(e)(1). Accordingly, Count II fails for the same reasons as Count I: Plaintiffs have failed to allege with sufficient particularity that the ***GRA Defendants*** accessed Plaintiffs' computers.

Count IV. "A claim for intrusion upon seclusion has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a

reasonable person." *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016). As with Counts I and II, Plaintiffs have failed to adequately allege that the GRA Defendants intruded into a private place or matter because they do not allege that the GRA Defendants themselves accessed Plaintiffs' computers or servers.

Count VI. Plaintiffs allege that the "Defendants," violated the Stored Communications Act ("SCA"). A defendant is civilly liable under the SCA for "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it is in electronic storage in such system[.]" 18 U.S.C. § 2701(a)(1). Plaintiffs' allegations are insufficient for two reasons. *First*, Plaintiffs do not allege the GRA Defendants directly accessed Plaintiffs' computers or servers. *See Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1006 (9th Cir. 2006) (no secondary liability under SCA). *Second*, SCA liability is limited to "facilit[ies] through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1). As the Stonington Defendants correctly argue, Dkt. 129-1 at 16, Plaintiffs do not allege that BCM's computer systems are a "facility" under the SCA.

Count VII. The DMCA prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under th[e] [Act]." 17 U.S.C. § 1201(a). Plaintiffs fail to allege sufficient facts to state a DMCA claim for three independently sufficient reasons.

First, the GRA Defendants did not commit any act of circumvention on their own, and instead allegedly "coordinated" the hack or "introduced" Qatar to unknown threat actors. FAC ¶¶ 7, 93-94. Neither of those acts demonstrates circumvention as required by the statute. *Second*, as the Stonington Defendants correctly argue, Plaintiffs have failed to allege sufficient detail to support the legal conclusion that copyrighted material was hacked. Dkt. 129-1 at 17. And *finally*, the DMCA does not cover phishing schemes

like the one alleged here. *See Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 692 (D. Md. 2011).

B. Plaintiffs Have Insufficiently Alleged That The GRA Defendants Received, Possessed, Or Distributed Stolen Emails

Plaintiffs do not make any specific allegations that GRA Defendants actually received, possessed, or distributed any stolen emails. Because Counts III, V, VIII, and IX each require such allegations, they must be dismissed.

Count III. In order to sufficiently allege a cause of action for receipt of stolen property, Plaintiffs must demonstrate "that *the accused* received, concealed or withheld [stolen property] from the owner thereof." *Finton Construction, Inc. v. Bidna & Keys, APLC*, 190 Cal. Rptr. 3d 1, 12 (Cal. Ct. App. 2015) (emphasis added). Plaintiffs have not alleged any facts to support the claim that the GRA Defendants "received, concealed or withheld" stolen property from the Plaintiffs.

Count V. To state a conversion claim under California law, a plaintiff must allege a defendant "assumed control or ownership over the property." *Graham-Suit v. Clainos*, 756 F.3d 724, 749 (9th Cir. 2014). Because Plaintiffs do not allege that the GRA Defendants "received" stolen property from the Plaintiffs, it necessarily follows that the GRA Defendants could not have taken any action to convert or dispose of that property.

Counts VIII and IX. Both the California Uniform Trade Secrets Act and the Defend Trade Secrets Act prohibit the "misappropriation" of trade secrets. *See* Cal. Civ. Code § 3426.2(a); *see also* 18 U.S.C. § 1836(b). Plaintiffs have not alleged that GRA Defendants "acquired, disclosed, or used" any of Plaintiffs' property, including any purported trade secrets, which the law requires. *See, e.g., Becton, Dickinson & Co. v. Cytek Biosciences Inc.*, No. 18-CV-00933, 2018 WL 2298500, at *3-*4 (N.D. Cal. May 21, 2018).

Additionally, Plaintiffs do not allege with sufficient particularity that the information and documents allegedly hacked were "trade secrets." *See, e.g.*, *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 522 (9th Cir. 1993) (a plaintiff must identify the trade secret with reasonable particularity). The broad categories of information cited by Plaintiffs, FAC ¶ 205, are generic categorizations routinely held insufficient as a matter of law. *See Becton*, 2018 WL 2298500, at *3.

C. Plaintiffs' Civil Conspiracy Claim Must Be Dismissed

In addition to the other pleading failures discussed *supra*, under California law, "there is no separate tort of civil conspiracy and no action for conspiracy to commit a tort unless the underlying tort is committed and damage results therefrom." *See MH Pillars Ltd. v. Realini*, 277 F. Supp. 3d 1077, 1096 (N.D. Cal. 2017). Plaintiffs have failed to sufficiently allege any of the substantive torts underlying their conspiracy claim, and without a substantive tort there can be no civil conspiracy claim. *See id.*

D. Plaintiffs' Common Law Tort Claims Are Preempted

In addition to the foregoing, Counts III, IV, V, and X fail because they are preempted by CUTSA, which preempts common law claims "if they are based on the same nucleus of facts as the misappropriation of trade secrets claim for relief." *Chang v. Biosuccess Biotech Co., Ltd.*, 76 F. Supp. 3d 1022, 1041 (C.D. Cal. 2014). Plaintiffs' common law tort claims arise out of the same nucleus of facts: the alleged hacking of Plaintiffs' computers and computer servers. Accordingly, Counts III, IV, V, and X are preempted and must be dismissed.

Count X (Civil Conspiracy) is additionally preempted by the CFAA, which provides for co-conspirator liability under 18 U.S.C. § 1030(b)—a provision under which Plaintiffs failed to plead. *See DHI Group, Inc. v. Kent*, No. H-16-1670, 2017 WL 1088352, at *12 (S.D. Tex. Mar. 3, 2017) ("the CFAA, by creating a statutory conspiracy claim, excludes common law conspiracy claims").

CONCLUSION

For the foregoing reasons, the FAC should be dismissed. Having failed twice to allege even a remotely plausible conspiracy, and with the allegations running squarely into Defendants' sovereign immunity, the Court should not give the Plaintiffs a third chance. Dismissal should be with prejudice.

Dated: July 23, 2018

WILMER CUTLER PICKERING HALE AND DORR LLP

By: /s/ Brendan R. McGuire

Brendan R. McGuire (*pro hac vice*)
7 World Trade Center
250 Greenwich Street
New York, NY 10007
Email: brendan.mcguire@wilmerhale.com
Telephone: + 1 212-295-6278
Facsimile: + 1 212-230-8888

Attorney for Defendants Global Risk Advisors LLC and Kevin Chalker