

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FARHAD AZIMA)	
)	
)	
Plaintiff,)	
)	
v.)	No. 16-cv-01948 (KBJ)
)	
RAK INVESTMENT AUTHORITY)	
)	
Defendant.)	
)	

MEMORANDUM OPINION

Plaintiff Farhad Azima (an American citizen and resident) is an international businessman who has worked for many years with Defendant Ras Al Khaimah Investment Authority (“RAKIA”), which is an investment organ of one of the emirates within the United Arab Emirates. Like many longstanding business relationships, the partnership between Azima and RAKIA has had its ups and downs. Not surprisingly, this lawsuit concerns one of the downs: Azima maintains that RAKIA commissioned the repeated surreptitious hacking of his personal and business laptops from October 2015 to August 2016, and then published disparaging material that was illicitly gleaned from Azima’s computers during the hacking. Azima filed the instant lawsuit on September 30, 2016, claiming that RAKIA has violated the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, *et seq.*, and that RAKIA has also engaged in common law conversion and unfair competition.

Before this Court at present is RAKIA’s motion to dismiss Azima’s first amended complaint pursuant to Federal Rule of Civil Procedure 12(b)(1) and the

doctrine of *forum non conveniens*. (See Mem. in Supp. of Def.’s Mot. to Dismiss (“Def.’s Mot.”), ECF No. 31-2, at 7–9.)¹ In its motion, RAKIA argues that this Court lacks subject matter jurisdiction over this case because the Foreign Sovereign Immunities Act (“the FSIA”), 28 U.S.C. § 1604, *et seq.*, confers sovereign immunity upon RAKIA, and because none of the FSIA’s limited exceptions apply. (See Def.’s Mot. at 21–35.) In particular, RAKIA asserts it enjoys immunity because it is an “agency or instrumentality of a foreign sovereign” (*id.* at 21), and neither the FSIA’s commercial activity exception or non-commercial tort exception confers jurisdiction over RAKIA under the instant circumstances (*id.* at 24–35). RAKIA further contends that, even if this Court has jurisdiction under the FSIA, the United Kingdom is the proper forum to hear this lawsuit, not the District of Columbia, given the forum-selection clause that Azima and RAKIA executed as part of a March 2016 Settlement Agreement (*see id.* at 35–37), and the fact that the balance of public and private interests favor litigating this matter in London (*see id.* at 37–40).

For the reasons explained fully below, RAKIA’s motion to dismiss Azima’s complaint will be **DENIED**. This Court concludes that it has subject matter jurisdiction over this case, because Azima has alleged that RAKIA engaged in foreign commercial activities in connection with an act that had a direct effect within the United States, such that this matter falls within the commercial activity exception to the FSIA. And because RAKIA has failed to demonstrate that the United Kingdom is an adequate and available forum to litigate Azima’s claims, the Court also rejects RAKIA’s contention

¹ Page-number citations to the documents that the parties have filed refer to the page numbers that the Court’s electronic filing system automatically assigns.

that the doctrine of *forum non conveniens* requires that this case be brought in London. A separate Order consistent with this Memorandum Opinion will follow.

I. BACKGROUND²

A. The Commercial Dealings Of Azima And RAKIA

Azima is an American businessman who resides in Kansas City, Missouri (*see* Am. Compl., ECF No. 28, ¶ 7), while RAKIA is a commercial investment entity that is part of the government of Ras Al Khaimah, one of the emirates in the United Arab Emirates (*see id.* ¶¶ 8–9). Azima and RAKIA have worked together on a number of business matters over the past decade (*see id.* ¶ 64), and throughout their association with one another, Azima and RAKIA have repeatedly discussed possible joint ventures in the aviation, hospitality, logistics, munitions, and steel industries (*see id.* ¶ 21). These discussions have sometimes come to fruition; Azima and RAKIA have engaged in “multiple business ventures” through which RAKIA has paid Azima more than seven million dollars. (*Id.* ¶ 18.)

In one such venture, one of Azima’s businesses—known as “HeavyLift International Airline”—entered into a joint venture with RAK Airways to build and operate a flight training academy in Ras Al Khaimah. (*See id.* ¶ 19.) RAKIA became involved with this arrangement as a guarantor, because it agreed to guarantee RAK Airways’s performance in the event that RAK Airways failed to meet its contractual

² The facts contained within this section are derived from Azima’s amended complaint and the exhibits that RAKIA and Azima have attached to the briefings in this case. The facts revealed in those exhibits are relevant here, because there is a factual dispute that is pertinent to the Court’s resolution of the instant motion. *See SACE S.p.A. v. Republic of Para.*, 243 F. Supp. 3d 21, 32 (D.D.C. 2017) (explaining that, while normally a court at the motion to dismiss stage must take all facts in the light most favorable to the plaintiff, jurisdictional issues such as sovereign immunity require consideration of facts outside the four corners of the complaint). The background provided below describes and references the affidavits and other materials that the parties have submitted.

obligations. (*See id.*) A subsequent dispute arose with respect to this joint venture, when Azima claimed that RAK Airways owed HeavyLift for “investments HeavyLift made[.]” (Settlement Agreement, Ex. L to Def.’s Mot., ECF No. 31-15, at 3.)

HeavyLift eventually turned to RAKIA as RAK Airways’s guarantor, and the three principals (RAKIA, HeavyLift, and Azima) entered into a settlement agreement in March of 2016 to resolve that dispute. (*See id.*) Significantly for present purposes, the March 2016 Settlement Agreement contained the following forum-selection clause:

This Settlement Agreement and any dispute or claim arising out of, or in connection with, it or its subject matter or formation (including, without limitation, any contractual or non-contractual disputes, claims or obligations) is governed by and shall be construed in accordance with English law and the Parties agree to the exclusive jurisdiction of the courts of England and Wales.

(Settlement Agreement at 5–6.)

Notably, Azima contends that, in addition to doing business with RAKIA with respect to the HeavyLift joint venture and other business arrangements, he has also served as a mediator for RAKIA, helping it resolve disputes with other commercial entities. (*See* Am. Compl. ¶ 21.) RAKIA purportedly employed Azima in that capacity during the 2015 and 2016 calendar years, as RAKIA attempted to negotiate a settlement with its former CEO. (*See id.* ¶ 23.) According to Azima’s complaint, RAKIA asked Azima to step in as a mediator for this particular dispute, and Azima fully anticipated that RAKIA would compensate him for his services and expenses. (*See id.*) But Azima alleges that RAKIA never paid him for the services he provided when he mediated between RAKIA and its former CEO, and that RAKIA ultimately terminated his services in July of 2016. (*See id.* at ¶ 34.)

For its part, RAKIA vehemently contends that it never asked Azima to mediate between RAKIA and its former CEO. (*See* Decl. of James Buchanan, Attachment to Def.’s Mot., ECF No. 31-21, ¶¶ 6–7.) Instead, RAKIA recalls that Azima approached RAKIA and offered to serve as “an honest broker”—as distinguished from a neutral mediator—in the dispute between RAKIA and its former CEO. (*See id.*) Furthermore, RAKIA says that it did not offer to pay Azima for these services, nor did it enter into a contract with him for these services. (*See id.* ¶ 8.) Indeed, throughout Azima’s time as an “honest broker,” RAKIA allegedly perceived him to be acting as an advocate for RAKIA’s former CEO. (*See id.* ¶ 12.)

Thus, there is a disagreement between the parties regarding whether or not RAKIA actually hired Azima to mediate a conflict in or around 2015. However, it is beyond dispute that the aforementioned March 2016 Settlement Agreement—which both Azima and RAKIA signed—specifically references the fact that Azima had “recently provided negotiation assistance to RAKIA on an informal basis[,]” and lists this service as one of the reasons for the payout that Azima received through that settlement. (Settlement Agreement at 3.)

B. The Hacking And Its Aftermath

Azima’s complaint alleges that, during the time that Azima was allegedly mediating between RAKIA and its former CEO, computer hackers repeatedly accessed Azima’s business and personal computers. (*See* Am. Compl. ¶¶ 26, 33, 78.) These digital assaults purportedly began on October 14, 2015, when the hackers accessed Azima’s computers using two IP addresses; one that was based in Florida, and one that was based in New York. (*See id.* ¶ 26.) Unbeknownst to Azima, the hackers then repeatedly accessed his computers over the next ten months, monitoring Azima’s

communications, deleting his data, and sending fake emails from his accounts. (*See id.* ¶ 30.) And because Azima did not learn that hackers were accessing his computers until August of 2016 (*see id.* ¶ 31), he continued to communicate with RAKIA and its former CEO electronically (*see id.* ¶¶ 25, 31), and discuss privileged matters with his attorneys concerning his “commercial interactions with RAKIA” (*id.* ¶ 31). Thus, Azima has alleged that the hackers were watching while Azima engaged in sensitive and important business affairs. The hackers also allegedly left behind malware, which infected Azima’s computers (*see id.* ¶ 33), and ultimately damaged Azima’s “U.S.-based business and personal laptops” (*id.* ¶¶ 75, 78).

At the same time that the hackers were infiltrating Azima’s computers, the negotiations between RAKIA and its former CEO started to break down. (*See id.* at ¶¶ 34–35.) Azima alleges that, in July of 2016, RAKIA threatened him directly, by saying that he would become “collateral damage” in the all-out war that RAKIA planned to wage against its former CEO at that time. (*Id.*) Then, a short time later, multiple websites disparaging Azima appeared on the internet. (*See id.* ¶ 38.) The websites featured negative claims about Azima that RAKIA had allegedly made in the past (*see id.*), and also included links to BitTorrent sites that contained private documents from Azima’s computer and information contained in Azima’s iCloud account, including text messages, call history, calendar, photos, and voicemail recordings (*see id.* ¶ 39).³

³ The parties differ starkly with respect to their description of how BitTorrent websites work. Both sides agree that these websites are sometimes used for illegal activity, such as downloading illegally appropriated files. (*See* Am. Compl. ¶ 45; Decl. of James Hung, Attachment to Def.’s Mem. in Opp’n to Mot. for Protective Order, ECF No. 24-1, ¶ 12 (incorporated into 2nd Decl. of James Hung, ECF No. 31-22).) But RAKIA insists that members of the public can access these websites through a legal and non-surreptitious process (*see* Hung Decl. ¶ 16), while Azima maintains that only the BitTorrent creator or one of their affiliates can access the BitTorrent website (*see* Am. Compl. ¶¶ 40–41, 43, 46). This

On September 23, 2016, Azima’s counsel in Washington D.C. received a letter from RAKIA demanding \$4,162,500 if Azima wished to avoid a lawsuit. (*See id.* ¶ 49.) That demand letter based its claims on information that RAKIA had “recently obtained . . . via publicly available internet sources.” (*Id.*) RAKIA attached several of the documents taken from Azima’s computer to this demand letter, and those documents contained confidential information that Azima kept only on his computers. (*See id.* ¶ 50.) RAKIA has since admitted to possessing around 30 GB of Azima’s information (*see id.* ¶ 57), but it claims that it accessed the data legally through publicly available BitTorrent websites.

C. Procedural History

Azima filed the instant action on September 30, 2016. His three-count complaint claimed that RAKIA (or one of its agents) hacked his personal and business computers, stole his data, and used that information both to blackmail him and to harm his reputation. (*See id.* ¶ 60.) On December 12, 2016, RAKIA filed a motion to dismiss Azima’s action on the grounds that (1) the FSIA deprives this Court of subject matter jurisdiction to hear Azima’s case; (2) Azima has failed to state a claim upon which relief could be granted; and (3) the doctrine of *forum non conveniens* requires the dismissal of the lawsuit. (*See* Def.’s Mot. to Dismiss, ECF No. 13.) This Court held a motion hearing on April 24, 2017, and thereafter both denied RAKIA’s motion without prejudice and granted Azima leave to file a First Amended Complaint. (*See* Order, ECF No. 27.)

Azima has now filed an Amended Complaint, in which he repeats the assertion

dispute is immaterial to the Court’s resolution of the instant motion.

that RAKIA hacked his computers and used the resulting data to disparage and extort him in order “to gain an advantage in RAKIA’s commercial relationship with Mr. Azima.” (Am. Compl. ¶ 65; *see also id.* ¶¶ 66–68.) The amended complaint contains three counts, which claim that RAKIA’s conduct violated the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, *et seq.* (Count I), and also constituted common law conversion (Count II) and unfair competition (Count III). (*See id.* ¶¶ 77–103.) To overcome the FSIA bar that would ordinarily block a claim against an arm of a foreign state, Azima has invoked two of the FSIA’s provisions that authorize suits against sovereigns under specified circumstances: the commercial activity exception, 28 U.S.C. § 1605(a)(2), and the non-commercial tort exception, 28 U.S.C. § 1605(a)(5). (*See id.* ¶¶ 63–76.) Therefore, Azima argues that RAKIA is not immune to the instant lawsuit, and he seeks statutory, compensatory, and punitive damages, as well as an injunction that requires RAKIA to return all of his data and to refrain from similar conduct in the future. (*See id.*, Prayer for Relief.)

In response to Azima’s Amended Complaint, RAKIA has once again filed a motion to dismiss. (*See* Def.’s Mot.) RAKIA argues that this Court lacks subject matter jurisdiction under the FSIA, and that the Court should dismiss the action based on the doctrine of *forum non conveniens*. (*See id.* at 24–40.) This Court held a motion hearing on October 27, 2017, and RAKIA’s motion is now ripe for decision. (*See* Pl.’s Mem. in Opp’n to Def.’s Mot. to Dismiss (“Pl.’s Opp’n”), ECF No. 33; Reply Mem. of Law in Further Support of Mot. to Dismiss (“Def.’s Reply”), ECF No. 35.)

II. STATUTORY FRAMEWORK AND LEGAL STANDARDS

A. Sovereign Immunity Under The FSIA

When it enacted the FSIA, Congress made clear that foreign states are “immune

from the jurisdiction of the courts of the United States . . . unless one of [the FSIA’s] several statutorily defined exceptions applies.” *Republic of Arg. v. Weltover, Inc.*, 504 U.S. 607, 610–11 (1992) (citation omitted). The FSIA defines a “foreign state” to include “a political subdivision of a foreign state or an agency or instrumentality of a foreign state.” 28 U.S.C. § 1603(a). And because the courts of the United States must “respect the independence and dignity” of foreign states, *Bolivarian Republic of Venez. v. Helmerich & Payne Int’l Drilling Co.*, 137 S. Ct. 1312, 1319 (2017) (citation omitted), the FSIA’s presumption of immunity serves to cut off litigation against foreign states at the earliest possible moment, *see id.* at 1324.

Notably, however, a foreign sovereign is not entitled to immunity when it acts in a *commercial* capacity, as opposed to a sovereign one. *See id.* at 1320 (citation omitted) (“[W]e consequently began to limit our recognition of sovereign immunity, denying that immunity in cases ‘arising out of a foreign state’s strictly commercial acts[.]’”); *see also Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 487 (1983) (noting that the FSIA codifies the general presumption of foreign state immunity, which falls away if liability is based upon commercial activity). This general principle is expressly codified in a number of exceptions that appear in 28 U.S.C. § 1605(a), two of which purportedly bear on this case. The FSIA’s commercial activity exception provides that

[a] foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case . . . in which the action is based upon a commercial activity carried on in the United States by the foreign state; or upon an act performed in the United States in connection with a commercial activity of the foreign state elsewhere; or upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States[.]

28 U.S.C. § 1605(a)(2). For its part, the non-commercial tort exception states in relevant part that

[a] foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case . . . not otherwise encompassed in [the commercial activity exception], in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment[.]

Id. § 1605(a)(5). If the circumstances set forth in either of these two statutory provisions—or in any of the other FSIA’s statutory exceptions, for that matter—apply, then the defendant foreign sovereign will not be immune and the plaintiff’s lawsuit can proceed. But any court grappling with these issues must bear in mind that these exceptions are “narrowly drawn[.]” *McKesson Corp. v. Islamic Republic of Iran*, 672 F.3d 1066, 1075 (D.C. Cir. 2012) (citations omitted), and should be construed as such, *see Schermerhorn v. State of Isr.*, 876 F.3d 351, 354 (D.C. Cir. 2017) (emphasizing that the noncommercial tort exception must be construed “narrowly”).

B. Motions To Dismiss Actions That Implicate The FSIA

“The established standard for evaluating a motion to dismiss under Rule 12(b)(1) in a case that implicates the FSIA is a nuanced one.” *SACE S.p.A. v. Republic of Para.*, 243 F. Supp. 3d 21, 32 (D.D.C. 2017). “By moving to dismiss, the defendant can challenge either [1] the legal sufficiency” of the allegations that appear on the face of the complaint “or [2] the factual underpinning of [the] exception” upon which the plaintiff relies. *Phoenix Consulting v. Republic of Angl.*, 216 F.3d 36, 40 (D.C. Cir. 2000). “A facial challenge attacks ‘the factual allegations of the complaint’ that lie on ‘the face of the complaint,’ while a factual challenge targets the underlying facts

contained in the complaint.” *Al–Owhali v. Ashcroft*, 279 F. Supp. 2d 13, 20 (D.D.C. 2003) (quoting *Loughlin v. United States*, 230 F. Supp. 2d 26, 35–36 (D.D.C. 2002)).

A facial challenge functions for all practical purposes as a Rule 12(b)(6) motion to dismiss. With regard to such a challenge, the Court must accept as true the complaint’s factual allegations and view all reasonable inferences in the light most favorable to the plaintiff, as it would in ruling on a Rule 12(b)(6) motion. *See Price v. Socialist People’s Libyan Arab Jamahiriya*, 294 F.3d 82, 93 (D.C. Cir. 2002); *SACE S.p.A*, 243 F. Supp. 3d at 32–33. The court is permitted to consider “the facts alleged in the complaint, documents attached as exhibits or incorporated by reference in the complaint, or documents upon which the plaintiff’s complaint necessarily relies even if the document is produced not by the plaintiff in the complaint but by the defendant in a motion to dismiss.” *Patterson v. United States*, 999 F. Supp. 2d 300, 306 (D.D.C. 2013) (citation omitted). If these allegations and inferences together establish that an FSIA exception plausibly applies, then the plaintiff’s complaint will survive a facial challenge. *See Agrocomplect, AD v. Republic of Iraq*, 524 F. Supp. 2d 16, 21 n.8 (D.D.C. 2007).

But where the defendant has made a *factual* challenge, the motion more closely resembles a motion to dismiss brought under Rule 12(b)(1). Thus, a court may consider material outside the pleadings in order to determine whether it has subject matter jurisdiction over the challenged claims. *SACE S.p.A*, 243 F. Supp. 3d at 33. Additionally, factual challenges relating to the FSIA employ a burden-shifting framework for determining whether or not an FSIA exception applies: “[t]he plaintiff bears the initial burden to overcome [this presumption] by producing evidence that an

exception applies[,]” *Bell Helicopter Textron, Inc. v. Islamic Republic of Iran*, 734 F.3d 1175, 1183 (D.C. Cir. 2013) (citation omitted), and once the plaintiff meets this burden of production, “the [defending] sovereign bears the ultimate burden of persuasion to show the exception does not apply,” *id.*

C. Motions To Dismiss For *Forum Non Conveniens*

“The principle of *forum non conveniens* is simply that a court may resist imposition upon its jurisdiction even when jurisdiction is authorized by the letter of a general venue statute.” *Gulf Oil Corp. v. Gilbert*, 330 U.S. 501, 507 (1947), *superseded by statute on other grounds*. Federal courts retain the discretion to dismiss a suit for *forum non conveniens* if a defendant demonstrates that (1) an adequate alternative forum is available to hear plaintiff’s claims, and (2) based on “a balancing of public and private interest factors[,]” the alternative forum is the strongly preferred location for the litigation. *See Agudas Chasidei Chabad of U.S. v. Russian Fed’n*, 528 F.3d 934, 950 (D.C. Cir. 2008) (citing *Piper Aircraft Co. v. Reyno*, 454 U.S. 235, 255 n.22 (1981)).

As the movant, the defendant bears the burden of proof on all points and must demonstrate why the “substantial presumption in favor of plaintiff’s choice of forum” should not apply. *Id.* (citation omitted). And because this inquiry is one concerning whether or not a court should exercise its jurisdiction as a discretionary matter, the court can look to materials outside the pleadings. *See, e.g., MBI Grp., Inc. v. Credit Foncier Du Cameroun*, 616 F.3d 568, 574–75 (D.C. Cir. 2010) (analyzing facts and events not contained within the pleadings that were relevant to the *forum non conveniens* analysis).

III. ANALYSIS

In the instant case, the parties have fiercely debated whether RAKIA is immune

from suit under the FSIA, primarily because they disagree over whether the FSIA's commercial activity or noncommercial tort exceptions apply. Notably, Azima and RAKIA hotly contest several different aspects of the FSIA's commercial activity exception as applied to the instant record: (1) where the alleged hacking of Azima's computers took place (i.e., inside or outside the United States); (2) whether RAKIA has engaged in a pertinent "commercial activity" outside of the United States; (3) whether RAKIA's alleged hacking of Azima's computers was undertaken in connection with that foreign commercial activity; and (4) whether the alleged hacking of Azima's computers had a direct effect within the United States. (*See* Def.'s Mot. at 28–35; Pl.'s Opp'n at 29–39; Def.'s Reply at 8–16.)

For the reasons explained below, this Court has concluded that Azima has adequately alleged (and proven to the extent that RAKIA makes a factual challenge) that RAKIA's hacking of Azima's computers was undertaken in connection with a foreign commercial activity and caused a direct effect within the United States, and thus that the commercial activity exception provides the Court with subject matter jurisdiction over this case. That holding renders it unnecessary for the Court to further opine as to the applicability of the FSIA's noncommercial tort exception. But the Court has proceeded to reach, and resolve, the parties' additional dispute regarding the prudential doctrine of *forum non conveniens* (*see* Def.'s Mot. at 35–40; Pl.'s Opp'n at 42–54; Def.'s Reply at 20–23), and it concludes that RAKIA has failed to carry its burden of establishing that England provides an adequate alternative forum. Therefore, both aspects of RAKIA's motion—to dismiss for lack of subject matter jurisdiction and to dismiss for *forum non conveniens*—will be denied.

A. This Court Has Subject Matter Jurisdiction Over Azima's Claims Under The FSIA's Commercial Activity Exception

As mentioned above, the FSIA's commercial activity exception contains three clauses that provide independent bases for a court to exercise subject matter jurisdiction over a foreign sovereign. *See* 28 U.S.C. § 1605(a)(2). Two of those clauses are relevant here. They authorize a court to exercise jurisdiction where a plaintiff claims that the sovereign committed an injurious act that was performed either within the United States in connection with commercial activity outside the United States, or outside of the United States in connection with commercial activity outside the United States if the act has a direct effect within the United States. *Id.* In the instant case, it is undisputed that if RAKIA can be said to have engaged in a commercial activity at all, such activity took place outside the United States. But the parties debate whether RAKIA's extraterritorial commercial activity is pertinent to the instant lawsuit, and whether the alleged hacking (the injurious act) can be said to have been performed in connection with that commercial activity. (*See* Def.'s Mot. at 28–32; Pl.'s Opp'n at 30–36; Def.'s Reply at 8–13.) The parties are also at odds over whether the alleged hacking had a direct effect within the United States, as well as whether the hacking itself took place inside or outside the United States. (*See* Def.'s Mot. at 28, 32–35; Pl.'s Opp'n at 36–39; Def.'s Reply at 14–16.)

Because this Court concludes that Azima has adequately alleged—and, as necessary, has established—that the hacking that is the basis of the instant lawsuit was performed in connection with RAKIA's commercial activity outside of the United States and had a direct effect within the United States, as explained below, the FSIA's commercial activity exception applies without regard to whether the alleged hacking

occurred inside or outside the United States.

1. The Record Demonstrates That RAKIA Engaged In Extraterritorial “Commercial Activity” For FSIA Purposes

The FSIA defines the phrase “commercial activity” as “either a regular course of commercial conduct or a particular commercial transaction or act.” 28 U.S.C.

§ 1603(d). Generally speaking, such transactions or acts are “the type of actions by which a private party engages in trade and traffic or commerce[.]” *Weltover*, 504 U.S. at 614 (emphasis, internal quotation marks, and citation omitted). Therefore, a foreign state engages in commercial activity for the purpose of the FSIA when it conducts itself “in the manner of a private player in the market.” *Saudi Arabia v. Nelson*, 507 U.S. 349, 360 (1993) (internal quotation marks and citations omitted). For example, courts have held that retaining an attorney, contracting to buy goods or services, or repudiating a contract for goods and services all qualify as “commercial activities” under the FSIA. *See, e.g., Weltover*, 504 U.S. at 614 (“[A] contract to buy army boots or even bullets is a ‘commercial’ activity[.]”); *Nnaka v. Fed. Republic of Nigeria*, 238 F. Supp. 3d 17, 28 (D.D.C. 2017) (agreeing that an attorney’s “retention agreement with Nigeria is ‘commercial activity’ within the meaning of the FSIA”). By contrast, uniquely sovereign activities, such as state-authorized abductions or the nationalization of a business entity through a country’s legal or political systems, do not trigger the commercial activity exception, and lawsuits claiming injury for acts undertaken in connection with such activities do not avoid the FSIA’s sovereign immunity bar. *See, e.g., Rong v. Liaoning Province Gov’t*, 452 F.3d 883, 889–90 (D.C. Cir. 2006) (holding that the government’s legislated takeover of a business was an act of state and not a commercial activity); *Cicippio v. Islamic Republic of Iran*, 30 F.3d 164, 168 (D.C. Cir.

1994) (concluding that state-sponsored hostage taking is not a commercial activity even if it is financially motivated).

Notably, drawing the line between commercial and sovereign activities for FSIA purposes can sometimes be quite difficult. *Compare Rong*, 452 F.3d at 889–90 with *Foremost-McKesson, Inc. v. Islamic Republic of Iran*, 905 F.2d 438, 449–50 (D.C. Cir. 1990). To deal with this ambiguity, the Supreme Court has emphasized that a court must look to whether “a foreign government acts . . . in the manner of a private player within the [market],” and the court must look only to the nature of that activity, *not* the sovereign’s reasons for engaging in it. *Weltover*, 504 U.S. at 614. These two precepts necessarily guide the Court’s inquiry here.

Azima maintains that the commercial activity aspect of the FSIA exception set forth at section 1605(a)(2) is satisfied because RAKIA is engaged in ongoing business dealings with him outside of the United States as a general matter, and also because RAKIA specifically engaged him to mediate the dispute between RAKIA and its former CEO. RAKIA’s motion to dismiss rejects the arguments that pertain to the parties’ longstanding relationship because it claims that those activities are not in connection with the acts in this case (*see* Part III.A.2, *infra*), and, as a factual matter, RAKIA also challenges Azima’s contention that he served as a mediator between RAKIA and its CEO (*see* Def.’s Mot. at 29). In regard to RAKIA’s factual challenge, this Court must examine the entire record in order to ascertain whether Azima has “come[] forward with sufficient evidence to carry [his] burden of production” regarding RAKIA’s participation in a commercial activity, and, if he has, the Court must then assess whether RAKIA, who “shoulder[s] the burden of persuasion[,]” has demonstrated that

no such commercial activity actually occurred. *SACE S.p.A*, 243 F. Supp. 3d at 32 (internal quotation marks and citation omitted).

The instant record is more than sufficient to persuade this Court that RAKIA has engaged in pertinent commercial activity outside of the United States, within the meaning of the FSIA's commercial activity exception, for several reasons. First of all, the information that the parties have presented makes crystal clear that RAKIA and Azima have had an ongoing and active business relationship for many years. There is no dispute that RAKIA is an investment organ of Ras al Khaimah, and it appears that RAKIA's commercial relationship with Azima began no later than 2007, with the HeavyLift joint venture agreement (*see* Buchanan Decl. ¶ 19), and continued until at least the summer of 2016, when Azima and RAKIA discussed investing in a munitions factory (*see id.* ¶ 14). Indeed, the record establishes that between October 14, 2015, and August 2016 (i.e., the period in which the alleged hacking occurred), Azima and RAKIA were engaged in several business-related activities; specifically, they engaged in discussions in the fall of 2015 about a possible "Intelligence, Surveillance, and Reconnaissance" joint venture between RAKIA and a company Azima owns (*id.*); undertook discussions in summer of 2016 about RAKIA and Azima investing in a munitions factory (*see id.*); and continued participating in a joint venture relating to a flight training academy in the United Arab Emirates and between Azima's HeavyLift company and RAK Airways, whose performance RAKIA agreed to guarantee (*see id.* ¶ 19; *see also* Am. Compl. ¶ 64; Settlement Agreement at 2).

Thus, the question here is whether RAKIA's involvement in these business negotiations constituted commercial activity as defined in *Weltover*. It is clear to this

Court that they do. To begin with, these negotiations were generally commercial in nature, and in fact, by agreeing to serve as a guarantor for RAK Airways's performance with respect to the HeavyLift joint venture agreement, RAKIA undertook the *quintessential* role of a commercial actor in the context of a new business enterprise. No less an authority than *Black's Law Dictionary* defines a "joint venture" as "[a] business undertaking by two or more persons engaged in a single defined project[.]" *Black's Law Dictionary* 967 (10th ed. 2014), and in becoming a "guarantor," RAKIA specifically "ma[de] a guaranty or g[ave] security for a debt[.]" *id.* at 821; *see also* 23 *Williston on Contracts* § 61:1 (4th ed. 2017) (describing a 'guaranty' as a contractual promise to compensate the obligee in the event that the principal obligor fails to do so). Contractual promises of this nature are undoubtedly the "type of action[] by which a private party engages in 'trade and traffic or commerce[.]'" *Weltover*, 504 U.S. at 614 (emphasis and citations omitted); *see also De Csepel v. Republic of Hung.*, 714 F.3d 591, 599 (D.C. Cir. 2013). RAKIA cannot deny that it has been party to various business agreements with Azima—either directly or through other business entities—and the Courts of Appeals have acknowledged that a broad array of contractual agreements constitute commercial activity under the FSIA. *See, e.g., De Csepel*, 714 F.3d at 599 (bailment contract); *Embassy of the Arab Republic of Egypt v. Lasheen*, 603 F.3d 1166, 1171 (9th Cir. 2010) (indemnification agreement); *Southway v. Cent. Bank of Nigeria*, 198 F.3d 1210, 1218 (10th Cir. 1999) (assignment contracts).

The trickier (and more hotly contested) question pertaining to RAKIA's alleged commercial activity is a question of fact: whether or not RAKIA specifically engaged Azima's services as a mediator between the summer of 2015 and July 2016. The parties

vehemently disagree as to exactly what role Azima served in the negotiations between RAKIA and its former CEO, and on its face, both parties have provided plausible accounts of the role Azima played. All things considered, this Court finds that Azima has met his burden of production regarding his contention that he worked as a mediator between RAKIA and its CEO between the summer of 2015 and July 2016 and that this activity took place outside the United States, and it finds that RAKIA has not carried its burden of persuasion with respect to this same issue.

The emails that Azima has submitted clearly demonstrate that he functioned as one of the “middle men, the messengers” (7/23/16–7/25/16 Email Chain, Ex. B to Pl.’s Opp’n, ECF No. 33-3, at 4), with respect to the dispute that RAKIA had with its former CEO, and that Azima served in a “Henry Kissinger role” (11/28/15–11/30/15 Email Chain, Ex. D to Pl.’s Opp’n, ECF No. 33-5, at 4). He coordinated meetings between RAKIA and its former CEO in Milan and Geneva (*see id.*; 1/28/16–1/31/2016 Email Chain, Ex. E to Pl.’s Opp’n, ECF No. 33-6, at 2–3), and on at least one occasion, Azima met personally with RAKIA outside the United States (*see* Buchanan Decl. ¶ 11; *see also* Am. Compl. ¶ 24 (noting that only “some” of Azima’s meetings in this matter took place within the United States)). Azima has also provided an email from one of RAKIA’s attorneys indicating that RAKIA entered into the March 2016 Settlement Agreement, at least in part, “in recognition of” Azima’s negotiations services. (12/30/15–1/5/2016 Email Chain, Ex. F to Pl.’s Opp’n, ECF No. 33-7, at 2.) Thus, even if Azima did not receive direct compensation for his negotiation assistance, the record shows that RAKIA perceived his services as having value and intended to reward them. (*See* 12/30/15–1/5/2016 Email Chain at 2 (“[A]ny settlement is more in recognition of

the support and assistance [] Azima is offering to RAK in settling matters with KM and SI[,] as well as[] potential new business ventures currently under discussion.”).)

Nothing that RAKIA has offered undercuts the strong inference that Azima was, in fact, engaged as a mediator with respect to the CEO dispute. RAKIA’s primary piece of evidence in this regard—the declaration of James Buchanan, Azima’s primary contact with RAKIA during the mediation—emphasizes that RAKIA believed Azima was acting as *the CEO’s* advocate with respect to the negotiations, and also that RAKIA never entered into an agreement to compensate Azima for his assistance (*see* Buchanan Decl. ¶¶ 7–8), but these assertions do not rebut Azima’s clear demonstration that he was actively involved in mediating the dispute. What is more, the other documents that RAKIA has submitted actually provide further confirmation of Azima’s mediator role. For example, as noted, the March 2016 Settlement Agreement expressly states that the \$2.6 million settlement was tendered to Azima, at least in part, to acknowledge that “Azima has recently provided negotiation assistance to RAKIA on an informal basis which RAKIA recognises and appreciates.” (Settlement Agreement at 3.) In addition, the Buchanan Declaration asserts that Azima sought to capitalize on his mediation role by proposing new joint ventures, some of which RAKIA did not immediately dismiss. (*See* Buchanan Decl. ¶ 14.) In this Court’s view, whether or not any such venture ultimately materialized is irrelevant because the acknowledgment that Azima was in a position to *make* such suggestions belies RAKIA’s current contention that Azima was merely a biased, uncompensated interloper with respect to the CEO dispute.

Therefore, based on the evidence presented, the Court finds that Azima has established that he served as a mediator in the out-of-country negotiations between

RAKIA and its former CEO, and that his work in these negotiations led, in part, to the agreement that RAKIA and Azima reached with respect to the outstanding dispute over the HeavyLift joint venture. Moreover, and significantly, RAKIA's engagement of Azima's services with respect to the negotiations constituted commercial activity for the purpose of the FSIA. Cf. Lydia Nussbaum, *Mediation As Regulation: Expanding State Governance Over Private Disputes*, 2016 Utah L. Rev. 361, 369–370 (2016) (“[M]ediation now has widespread application in a range of disputes: small claims, family, business . . . [a]nd in the private sector, businesses now include mediation clauses in contracts with each other, with their customers, and with their employees[.]”). Courts have long held that contracts for legal services to resolve disputes are commercial in nature, *see, e.g., Dentons U.S. LLP v. The Republic of Guinea*, 134 F. Supp. 3d 5, 9 (D.D.C. 2015); *Reichler, Milton & Medel v. Republic of Liber.*, 484 F. Supp. 2d 1, 2 (D.D.C. 2007); *see also Nnaka*, 238 F. Supp. 3d at 28 (“[R]etaining an attorney is the type of activity by which private parties engage in commerce.”), and so, too, is the engagement of a mediator by private parties, who routinely turn to mediators in an effort to reach a negotiated resolution of their differences, *see, e.g., Hensel Phelps Constr. Co. v. Cooper Carry Inc.*, 861 F.3d 267, 270 (D.C. Cir. 2017) (noting the frequent use of mediators); *Demissie v. Starbucks Corporate Office and Headquarters*, 118 F. Supp. 3d 29, 31–32 (D.D.C. 2015) (same).

The fact that Azima and RAKIA did not formalize Azima's role through a written or oral contract (*see* Def.'s Mot. at 29), and that RAKIA did not pay Azima directly for his mediation services at the time that they were rendered (*id.*), is of no moment. Azima's mediation work still amounts to commercial activity under the FSIA

because “[e]ngaging in a commercial act does not require the receipt of fair value, or even compliance with the common-law requirements of consideration.” *Weltover*, 504 U.S. at 616. Nor does it matter that RAKIA’s reason for engaging in mediation was “to recover stolen assets from [its former CEO],” which RAKIA labels a “distinctly sovereign activity.” (Def.’s Mot. at 29.) In this regard, RAKIA has confused the *purpose* of its activity with the activity itself; rather, with respect to the FSIA’s commercial activity exception,

the question is not whether the foreign government is acting with a profit motive or instead with the aim of fulfilling uniquely sovereign objectives. Rather, the issue is whether the particular actions that the foreign state performs (whatever the motive behind them) are the *type* of actions by which a party engages in “trade and traffic or commerce[.]”

Weltover, 504 U.S. at 614 (emphasis in original); *see also El-Hadad v. U.A.E.*, 496 F.3d 658, 668 (D.C. Cir. 2007) (noting that “[w]e cannot attend to whether a foreign government aims to make a profit or protect its borders”); *Cicippio*, 30 F.3d at 167 (“[W]e cannot consider the alleged motive of the Iranian government in determining whether appellants’ claim if true would involve commercial activity.”).

In sum, because the relevant activity here is the business negotiations and mediation that RAKIA authorized Azima to orchestrate and participate in during the timeframe of the alleged hacking, this Court concludes that those activities did constitute commercial activity taking place outside of the United States for the purposes of the FSIA.

2. RAKIA’s Alleged Hacking Of Azima’s Computers And Disparagement Of Him Were Acts Undertaken “In Connection With” Its Foreign Commercial Activities

RAKIA has raised a facial challenge to the portion of Azima’s complaint that alleges that RAKIA’s hacking and disparagement were acts done in connection with

either the commercial relationship between Azima and RAKIA or Azima's role as a mediator. (*See* Def.'s Mot. at 22.) But this Court does not, and cannot, conclude that the complaint's allegations are insufficient, implausible, or otherwise lacking in this regard.

Although the D.C. Circuit has yet to opine on the meaning of the phrase "in connection with" as it appears in section 1605(a)(2), the Courts of Appeals that have spoken to this issue have typically held that this phrase has a narrow meaning in the FSIA context. *See Garb v. Republic of Pol.*, 440 F.3d 579, 587 (2d Cir. 2006); *Adler v. Fed. Republic of Nigeria*, 107 F.3d 720, 726 (9th Cir. 1997). As most of those courts read it, that phrase demands that "the acts complained of must have some substantive connection or a causal link to the commercial activity," *Adler*, 107 F.3d at 726 (citing *Fed. Ins. Co. v. Richard I. Rubin & Co.*, 12 F.3d 1270, 1289–91 (3d Cir. 1993)), and thus a mere tangential or attenuated connection between the act and the commercial activity will not suffice, *Garb*, 440 F.3d at 587.⁴ In applying the FSIA's in connection with language narrowly, the Second Circuit concluded that even though "the expropriation of property" is an act that "is, in some sense, 'connected' to any subsequent commercial treatment of that property or its proceeds . . . [but] such a connection . . . is simply too 'attenuated,' and not substantive enough, to satisfy § 1605(a)(2)[.]" *Garb*, 440 F.3d at 587. Similarly, the Third Circuit has concluded that the mismanagement of a building inside the United States should not automatically be considered to be an act in connection with the extraterritorial execution of the loan transaction that was used to finance the building. *See Fed Ins. Co.*, 12 F.3d at 1291.

⁴ But *see Conn. Bank of Commerce v. Republic of Congo*, 309 F.3d 240, 255 (5th Cir. 2002) (examining merely whether the act was "related to" the commercial activity).

Accepting for the moment these courts’ interpretation of the “in connection with” phrase, this Court concludes that Azima has nevertheless made sufficient factual allegations to overcome even that relatively stringent standard. To be specific, the complaint in the instant case alleges that RAKIA “took the acts alleged herein *in order to* gain an advantage over Mr. Azima in his commercial dealings with RAKIA and to inflict commercial and financial harm on Mr. Azima.” (Am. Compl. ¶ 68 (emphasis added).) In this way, Azima’s complaint draws a direct causal relationship between the hacking and online disparagement of which Azima complains and the commercial activity that RAKIA and Azima had been engaged in overseas. And the complaint goes further: it alleges that the information RAKIA supposedly obtained during the hacking of Azima’s computers was actually *used* in conjunction with the demand letter that RAKIA sent to Azima to accuse him of defrauding RAKIA in past commercial activities, including the HeavyLift joint venture. (*See id.* ¶¶ 49, 64.) Thus, the complaint draws a direct line between the hacking and the parties’ commercial dealings, and in so doing, satisfies the FSIA’s in-connection-with requirement.

Azima has also successfully pled a plausible theory that links the alleged hacking to the mediation services that Azima had been providing with respect to the CEO dispute. Azima starts off noting that the hacking of his computer began in October of 2015 and continued through the summer of 2016—a time period that roughly corresponds with the time in which Azima served as a mediator between RAKIA and its former CEO. (*Compare id.* ¶¶ 26, 29 (identifying the start and end points of the hack) *with id.* ¶¶ 23, 34 (identifying the start and end points of the mediation).) That alleged overlap alone supports an inference that there was some connection between the two,

but RAKIA's alleged actions during the final stretch of the mediation further underscores the alleged link between the hacking and Azima's role as a mediator. According to Azima, when it became clear that RAKIA and its former CEO were unlikely to reach an agreement, RAKIA upped the pressure by threatening to make Azima "collateral damage" in the all-out war that RAKIA planned to wage against its former CEO. (*See id.* ¶ 35 (internal quotation marks omitted).) The complaint then asserts that it was *only after* mediation had finally broken down that the hackers published Azima's private information on a number of BitTorrent websites, presumably to punish Azima for his role in the failed mediation in accordance with RAKIA's threat. (*See id.* ¶ 60.)

These allegations are sufficient to support a reasonable inference that RAKIA's alleged hacking had "a substantive connection or a causal link to the commercial activity" in this case. *See Adler*, 107 F.3d at 726 (internal quotation marks and citation omitted). That is, Azima has plausibly alleged that RAKIA's engagement in certain commercial activity—using Azima as a mediator and partnering with him in foreign business ventures—caused RAKIA to commit the hacking for the purpose of influencing the ongoing mediation, punishing Azima if anything went wrong with those negotiations, and ultimately "gain[ing] leverage and coercive influence" over Azima. (Am. Compl. ¶ 67.) Such an alleged link satisfies the in-connection-with requirement of the FSIA. *Cf. Adler*, 107 F.3d at 726 (finding that a sovereign's wrongful behavior surrounding a contract was in connection with that contract).

3. RAKIA's Alleged Hacking Of Azima's Computer Had A "Direct Effect" Within The United States

Finally, this Court must determine whether the allegations in the complaint, read

in the light most favorable to Azima, support the contention that RAKIA's conduct caused a direct effect in the United States. 28 U.S.C. § 1605(a)(2) (noting that a foreign sovereign loses its sovereign immunity when it commits "an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States"). (*See also* Def.'s Mot. at 32–35 (raising a facial challenge to Azima's direct effect allegations).) To do so, the Court must ask whether the alleged effect in the United States "follow[ed] as an immediate consequence of the defendant's . . . activity." *Weltover*, 504 U.S. at 618 (internal quotation marks and citation omitted). In other words, does the alleged effect of the challenged act "flow[] in a straight line without deviation or interruption" from its supposed cause? *Princz v. Fed. Republic of Ger.*, 26 F.3d 1166, 1172 (D.C. Cir. 1994) (internal quotation marks and citation omitted).

To answer *that* question, courts in this jurisdiction first determine whether the plaintiff's claims against the foreign sovereign are grounded in contract law or tort law, because the D.C. Circuit has developed two separate tests for whether these types of claims involve a direct effect within the United States. *See Odhiambo v. Republic of Kenya*, 764 F.3d 31, 38 (D.C. Cir. 2014) (noting that in contract cases a court looks to the contract's specified "place of performance"); *Bell Helicopter Textron, Inc.*, 734 F.3d at 1184 (explaining that in a tort case the court determines where the "locus of the tort" occurred (internal quotation marks and citation omitted)). Where, as here, the claims primarily sound in tort, the direct effect focus is on "the locus of the tort[.]" *Bell Helicopter Textron, Inc.*, 734 F.3d at 1184 (quoting *Antares Aircraft, L.P.*, 999 F.2d at 34); *see also Nnaka*, 238 F. Supp. 3d at 29–30 (concluding that a plaintiff had

demonstrated a direct effect because defendant’s defamation of plaintiff occurred in the United States); *Princz*, 26 F.3d at 1173 (holding that a plaintiff’s suffering from forced labor in Germany and Poland caused a direct effect in Poland and Germany, not the United States). “A tort’s locus is the place where the last event necessary to make an actor liable for an alleged tort takes place[,]” and that last event is typically the injury that the plaintiff suffers. *Nnaka*, 238 F. Supp. 3d at 29 (internal quotation marks omitted) (citing *Atlantica Holdings v. Sovereign Wealth Fund Samruk-Kazyna JSC*, 813 F.3d 98, 109 (2d Cir. 2016)); *see also* Stuart M. Speiser, et al., 1 *American Law of Torts* § 1.1 (Mar. 2018 Update) (“A tortious act has been defined as the commission or omission of an act . . . whereby another receives some injury[.]”). Therefore, the direct effect question often reduces to whether or not the plaintiff sustained his cognizable injury in the United States. *See Atlantica Holdings*, 813 F.3d at 109.

However, notably, even if a court determines that the locus of the tort at issue is the United States, it must also conclude that the effect felt therein was “more than purely trivial.” *Princz*, 26 F.3d at 1172 (internal quotation marks and citation omitted). Of course, this does *not* mean that the effect has to be “substantial or foreseeable.” *Id.* (internal quotation marks and citation omitted); *see also Weltover*, 504 U.S. at 617–18. But purely trivial effects, such as harm to a U.S. citizen’s commercial reputation, *see Bell Helicopter Textron, Inc.*, 734 F.3d at 1183–84, or a U.S. citizen’s having suffered a “financial loss from a foreign tort[,]” *id.* at 1184 (quoting *Antares Aircraft, L.P.*, 999 F.2d at 34), will not suffice to qualify as a direct effect within the United States.

Azima’s complaint asserts several facts that persuade this Court that the alleged hacking of Azima’s computers had a direct effect in the United States. First of all, the

complaint alleges that Azima is an American citizen and a successful businessman who resides in Kansas City, Missouri and conducts many of his business affairs from within the United States. (*See* Am. Compl. ¶¶ 7, 22; *id.* ¶ 24 (“In the [f]all of 2015 . . . Azima frequently communicated with Mr. Buchanan and Mr. Gerrard, through emails and phone calls from and to Mr. Azima in the United States[.]”); *id.* ¶ 31 (referencing business events Azima had in New York); *see also id.* ¶¶ 50–51 (noting that RAKIA has threatened to seek enforcement proceedings in the United States against Azima and his business).) Azima’s complaint contends that it is precisely because Azima often conducts business when he is inside the United States that Azima has a set of “*U.S.-based* business and personal laptops” (*id.* ¶ 78) (emphasis added), and according to the complaint, these were the laptops that were hacked in the fall of 2015 and repeatedly thereafter (*id.*).

Because hacking and the installation of malware affects the targeted computer systems, and the allegations of Azima’s complaint pertaining to where he works and resides support an inference that at least one of Azima’s U.S.-based personal and business laptops was in the United States when the hacking occurred, this Court confidently concludes that Azima has pled that a direct effect occurred within the United States. To find otherwise, as RAKIA insists that one must, would be to require Azima’s complaint to account for the whereabouts of *all* of his computer equipment at each moment when Azima’s computers were hacked, and to infer that if any of his computers could have left the United States with him when he traveled during the nine-month period where these hackings took place, then the complaint fails to allege that the hacking necessarily had a direct effect on his computers inside the United States.

(*See* Hr’g Tr. at 31:9–32:8.) Not only is such an inference procedurally improper, *see Price*, 294 F.3d at 93 (explaining that a facial challenge requires the court to read the allegations in the light most favorable *to the plaintiff* and take all plausible inferences in the plaintiff’s favor), but the Court also finds that the suggestion that a U.S. citizen who lives and works in the United States must pinpoint the dates of an allegedly extensive computer hacking and affirmatively assert that he was inside the United States with all of his computer equipment at the time the hacking occurred in order to be able proceed with an action against a foreign state under the CFAA and the FSIA (*see* Def.’s Mot. at 33–34; Def.’s Reply at 15 & n.7) is, itself, unreasonable.⁵

Thus, this Court finds that Azima’s complaint sufficiently alleges that RAKIA’s supposed hacking had a direct effect inside the United States. The relevant portions of the CFAA provide that a defendant is liable if it “intentionally accesses a protected computer without authorization” and causes the plaintiff to suffer a loss worth at least \$5,000. 18 U.S.C. §§ 1030(a)(5), (c)(4)(A)(i)(I), (g). Azima has pointed out that the hackers not only accessed his computerized files, but they also damaged his U.S.-based personal and business computers and installed malware on those machines. (*See* Am. Compl. ¶¶ 33, 78.) Given the facts alleged in Azima’s complaint, it is reasonable to infer that at least some of the damage to his data and to the computers themselves occurred when his computers were inside the United States, and therefore, Azima’s

⁵ This is not to say that Azima’s complaint could not have more clearly pled the allegations relating to the direct effect prong. Indeed, it would have been far preferable if Azima had included an express contention that the hacked computers were inside the United States at some point during the relevant timeframe, even if his assertion could only be made “upon information and belief.” But ultimately, the Court finds that such an inference can reasonably be drawn from the allegations that do appear in the pleading. And, of course, RAKIA is free to make a factual challenge to this contention, and to provide evidence that Azima’s computers were actually elsewhere during the relevant period, as this litigation proceeds.

plausible allegation of a cognizable injury due to a CFAA violation also establishes a direct effect in the United States. Azima further claims that RAKIA's alleged hacking, as well as the resulting disparagement of him when RAKIA weaponized the information that it had stolen, violated the common law of unfair competition, and these allegations also suffice to establish direct effects in the United States, because the gravamen of the unfair competition claim likewise appears to be that RAKIA's conduct "interfer[ed] with [Azima's] *business* computers." (*Id.* ¶ 98.)

Azima's conversion claim presents a more challenging inquiry, but, ultimately, the Court concludes that Azima has alleged sufficient facts that this claim, too, survives RAKIA's motion to dismiss. With respect to torts against property, it is well established that the locus of the tort is typically "where the force takes effect on the thing[.]" *See* Restatement of Conflict of Laws § 377 note 3 (Am. Law. Inst. 1934). Some courts have understood this to mean that the tort of conversion occurs "where any wrongful retention of plaintiff's property and subsequent injury occurs." *RaceRedi Motorsports, LLC v. Dart Mach., Ltd.*, 640 F. Supp. 2d 660, 666 (D. Md. 2009); *see also Charash v. Oberlin Coll.*, 14 F.3d 291, 297 (6th Cir. 1994) ("A conversion occurs when someone exercises dominion over the property without the owner's consent or authority."). And it is clear that outright theft is not the only way that a tortfeasor retains (exercises dominion and control over) another's property as a matter of law; property can also be deemed converted under D.C. law if it is damaged or destroyed while in the tortfeasor's possession. *See, e.g., Maalouf v. Butt*, 817 A.2d 189, 190 (D.C. 2003).

Assume for the moment that the conversion of digital data is legally possible.⁶ Under that circumstance, the direct effects inquiry with respect to the conversion claim here necessitates an evaluation of *where* Azima's digital data was when RAKIA exercised control over it, and also where the data existed when it was later harmed or wrongfully retained. Azima's complaint helpfully speaks to this point, because it specifically alleges that the harmful hacking activity included the deletion of data from *Azima's U.S.-based business and personal laptops*. (See Am. Compl. ¶ 90.) Given this Court's previous finding that Azima has plausibly alleged that at least one of the hacked computers was inside the United States when the hacking occurred (*see supra*), the hacker's erasure of such data, also plausibly occurred inside the United States.

To the extent that RAKIA's rebuttal includes the observation that Azima had his computers replaced after the malware attack, and thus is the one who destroyed his computers or data (*see* Def.'s Mot. at 34), RAKIA completely misses the point. Azima maintains that he decided, upon the advice of experts, to replace his computers because those computers *had already been damaged* by the hackings in this case (*see* Am. Compl. ¶ 33), and that threshold damage constitutes a direct effect for the purpose of the FSIA. Therefore, Azima's actions were not an "intervening element" between the hacking and the effect felt within the United States. *Princz*, 26 F.3d at 1172.

Finally, the Court rejects RAKIA's contention that Azima did not suffer a direct effect in the United States due to the theft of his data. While it is true that "loss to an

⁶ Many courts, including one in this district, have concluded that a party fails to state a claim for conversion when it asserts that the defendant converted digital data. *See, e.g., 3D Global Solutions, Inc. v. MVM, Inc.*, 552 F. Supp. 2d 1, 10 (D.D.C. 2008) ("Neither District of Columbia nor Virginia law recognizes a cause of action for conversion of intangible property.") (citations omitted). However, RAKIA has not pursued this argument in the present motion, and the Court will not address it.

American individual and firm resulting from a foreign tort” is not sufficient to cause a direct effect within the United States (Def.’s Mot. at 34 (quoting *Antares Aircraft, LP*, 999 F.2d at 36)), in making that statement, the Second Circuit was referencing a *financial* loss, and not the theft of a tangible or intangible object, *see Antares Aircraft*, 999 F.2d at 36. In this Court’s view, the alleged destruction of data on Azima’s computers while these computers were plausibly inside the United States is a sufficiently significant direct effect inside the United States to support this Court’s jurisdiction over Azima’s conversion claim.

4. The Court Need Not Decide Whether The Alleged Hacking Occurred Inside Or Outside The United States, Nor Is It Concerned That The Instant Ruling Will Open The Floodgates To A Wave Of Foreign-State Computer Hacking Lawsuits

This Court’s conclusion that Azima has plausibly alleged that RAKIA hacked his personal computers in connection with commercial activity outside of the United States causing a direct effect inside the United States renders unnecessary any assessment of whether the alleged hacking of Azima’s personal computers is an act that took place inside the United States. (*Compare* Def.’s Mot. at 18 (maintaining that the location of the hacking is the location of the hackers at the moment they broke into Azima’s computers, and arguing that “there is no allegation that the hackers were in the United States at the time”) *with* Pl.’s Opp’n at 29 & n.9 (asserting that, for the purpose of the commercial activity exception, a hacking occurs at the location of the IP addresses used to hack into the target computer, and the IP addresses used for to hack into Azima’s computers were in the United States). While an analysis of the location of the foreign sovereign’s allegedly tortious act is ordinarily a threshold consideration when a plaintiff contends that a federal court has jurisdiction over a foreign sovereign under the

FSIA's commercial activity exception, the location of the challenged act is obvious in the typical case, and the parties' dispute centers on whether the other elements of the applicable prong of the commercial activity exception have been satisfied. *See, e.g., de Cespel*, 714 F.3d at 598 (acknowledging that a Hungarian-based contract "obviously occurred outside the territory of the United States"); *Princz*, 26 F.3d at 1172–73 (taking for granted that the torture of the plaintiff in Germany took place overseas).

Not so with computer hacking. As the D.C. Circuit observed in *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (2017), the "intentional intrusion" that is generally required to commit a hacking tort "plainly lay[s] abroad" if the hackers themselves are not inside the United States, and so does the "tortious act[] of computer programming" that constitutes the actus reus. *Id.* at 10. But the "placement of [a virus] on [the plaintiff's] computer" injures the victim when he "open[s] the infected email attachment," *id.*, and thus occurs inside the United States if the plaintiff is inside the United States when the attachment is opened. Consequently, it "cannot be said that the entire tort occurred in the United States[.]" *id.*, which means that, as far as the FSIA's commercial activity exception is concerned, both parties can ordinarily make credible arguments regarding the location of a hack. (*See, e.g.,* Def.'s Mot. at 18; Pl.'s Opp'n at 29 & n.9.)

Nevertheless, this Court finds that there is no need to resolve the instant parties' vigorous dispute over the location of the hacking under the circumstances presented here. This is because the text, structure, and purpose of the FSIA's commercial activity exception all point to the conclusion that, rather than mandating identification of the location of the foreign sovereign's allegedly tortious act, Congress's primary concern is

ensuring that a lawsuit can be maintained if the foreign sovereign acts in a commercial capacity and undertakes a harmful act that occurs in, or impacts, the United States. *See Bolivarian Republic of Venez.*, 137 S. Ct. 1320 (explaining that 28 U.S.C. § 1605(a)(2) is designed to allow jurisdiction when a foreign nation “act[s] in a commercial capacity like other commercial entities”); *see also Verlinden*, 461 U.S. at 488 (acknowledging the same). And, it is entirely possible to conclude that the facts of a particular case satisfy the commercial activity exception without making a definitive determination regarding the location of the allegedly tortious act.

The plain text of 28 U.S.C. § 1605(a)(2) is the first clue that jurisdiction is properly exercised in this case under the FSIA’s commercial activity exception whether or not the tortious act at issue occurred inside the United States. Read as a whole, this provision authorizes federal courts to entertain a lawsuit against a foreign sovereign for commercial acts that occur either inside the United States (clauses 1 and 2) *or* outside the United States (clause 3). *See* 28 U.S.C. § 1605(a)(2); *see also Odhiambo*, 764 F.3d at 36–38.⁷ Thus, far from being a barrier to maintaining a legal action in federal court, the location-of-the-act determination simply determines what a plaintiff must show to establish that a plaintiff’s claims have some connection to the United States, as is necessary to invoke the jurisdiction of the federal courts. If the tortious act took place in the United States or it took place elsewhere yet still has a direct effect in the United States, *either* clause two or three of the commercial activity exception is applicable, and a court need not necessarily decide which circumstance applies, like in the instant case.

⁷ The fact that the commercial activity exception expressly authorizes federal courts to exercise jurisdiction over acts of a foreign sovereign that occur outside the United States distinguishes this exception from the FSIA’s noncommercial tort exception. *See Doe*, 851 F.3d at 9–10 (discussing the noncommercial tort exception’s phrasing and the important role that phrasing plays).

To conclude otherwise, and thereby require Azima to establish where, exactly, the hacking occurred as a threshold matter, as RAKIA suggests (*see* Def.'s Mot. at 18–19), would be to elevate the form of section 1605(a)(2) over its substance in a manner that contravenes the purpose of that statutory provision. It is difficult to pinpoint the one location where a hacking occurs, as explained above, but it is indisputable that the hacking of Azima's computers took place either inside the United States or outside the United States, and where the statute Congress enacted makes clear that either circumstance can suffice to establish jurisdiction, it simply cannot be the case that the complaint fails even if it contains sufficient allegations to support both. Moreover, because the facts alleged satisfy the more stringent of these two jurisdictional tests (*see* Part III.A.3, *supra* (finding that Azima has sufficiently pleaded that RAKIA's hacking had a direct effect inside the United States)), it is well established that the Court need not decide which legal test is the applicable one. *Cf. Yah Kai World Wide Enterps. v. Napper*, No. 11-cv-2174, 2018 WL 1000836, at *12 n.14 (D.D.C. Feb. 21, 2018) (explaining that when a plaintiff has met a potentially applicable, but more challenging standard, the court need not decide whether that standard or an easier standard actually applies).

For what it's worth, this Court is confident that its decision to eschew ruling on the location issue under the circumstances presented here will not automatically expand the FSIA to any and every case in which a foreign state or organ of the foreign state is accused of hacking into computers used in the United States. This is because Congress has made clear that the effect in the United States has to be direct in order to satisfy the jurisdictional requirement, and in the instant case, Azima has alleged actual damage to

his computers as a result of the hack, which makes it significantly easier to find that the effect of the alleged hacking activity here was not “‘purely trivial.’” *Princz*, 26 F.3d at 1172 (quoting *Weltover*, 504 U.S. 618); *see also Bell Helicopter Textron, Inc.*, 734 F.3d at 1183–84 (explaining that neither reputational harm nor financial loss constitutes a direct effect in the United States). Moreover, Congress has commanded that an act that causes direct effects inside the United States must have been undertaken in connection with some commercial activity of the foreign sovereign, *see* 28 U.S.C. § 1605(a)(2), which means that only hacking that impacts a computer inside the United States *in order to further foreign commercial activity* qualifies under the FSIA. Therefore, unless a foreign sovereign defendant commits a hacking offense in a manner that is similar to what Azima alleges RAKIA did in this case, the FSIA’s commercial activity exception will not permit a federal court to entertain a lawsuit.

B. RAKIA Has Failed To Prove That London, England Is An Adequate Alternative Forum For This Action; Therefore, This Court Will Not Dismiss This Case Under The Doctrine Of *Forum Non Conveniens*

As explained in Part II.C., *supra*, the doctrine of *forum non conveniens* requires a court to assess different venue-related issues, including whether or not the proposed alternative forum is an adequate one. *See Agudas Chasidei Chabad*, 528 F.3d at 950; *Nemariam v. Fed. Democratic Republic of Eth.*, 315 F.3d 390, 394 (D.C. Cir. 2003); *El-Fadl v. Cent. Bank of Jordan*, 75 F.3d 668, 676 (D.C. Cir. 1996) *abrogated on other grounds by Samantar v. Yousuf*, 560 U.S. 305 (2010). In general, evaluating the adequacy of a proposed forum is a relatively straightforward endeavor. The district court must first confirm that the defendants “are subject to service of process [in the foreign forum] and [that] the forum permits ‘litigation of the subject matter of the dispute.’” *EIG Energy Fund XIV, LP v. Petroleo Brasileiro S.A.*, 246 F. Supp. 3d 52,

74 (D.D.C 2017) (quoting *Piper Aircraft Co.*, 454 U.S. at 254 n.22). Then, the court must find that no procedural barrier (such as a statute of limitations or sovereign immunity defense) would prevent the parties from litigating the given dispute. *See id.*

It is important to note that the onus is not on the district court to research the proposed alternative forum in order to make the necessary assessment of its adequacy; rather, “the defendant ‘must provide enough information to enable the District Court’ to evaluate the alternative forum.” *El-Fadl*, 75 F.3d at 677 (quoting *Piper Aircraft*, 454 U.S. at 258). “[T]he amount of information that the defendant must provide, in supporting affidavits or other evidence, depends on the facts of the individual case[.]” *id.* (citation omitted), and it appears that defendants routinely provide the declaration of a legal expert from the alternative jurisdiction, who testifies to the adequacy and availability of the foreign forum, to meet this burden, *see, e.g., id.* (noting submission of affidavit by Jordanian lawyer); *Philipp v. Fed. Republic of Ger.*, 248 F. Supp. 3d 59, 84 (D.D.C. 2017) (discussing the expert opinions regarding the German legal system); *Petroleo Brasileiro S.A.*, 246 F. Supp. 3d at 75 (analyzing declarations regarding the availability of relief in Brazil). Such evidence goes a long way toward helping the defendant to sustain its “‘heavy burden’ of demonstrating that [the alternative forum] is an adequate forum to resolve [plaintiff’s] claims.” *Peroleo Brasileiro S.A.*, 246 F. Supp. 3d at 75.

In the instant case, RAKIA has provided no such testimony and its arguments do not convince this Court that the English High Court would have jurisdiction over the claims Azima seeks to advance here. The first reason for RAKIA’s shortcoming in this regard is the fact that foreign sovereigns typically enjoy a form of state immunity in the

United Kingdom (much like in the United States) under Parliament's State Immunity Act of 1978, *see generally* State Immunity Act of 1978, 1978, c. 33 (U.K.), *reprinted in* 17 I.L.M. 1123 (1978), and similar to the FSIA, that act begins with a general presumption of immunity, then proceeds to carve out narrow exceptions where the courts of the United Kingdom can exercise jurisdiction over a case filed against a foreign sovereign. *Id.* § 1. None of the exceptions that appear in the State Immunity Act apply to the present dispute on their face. *See, e.g., id.* § 2 (consent); § 3 (commercial transactions and contracts performed in the United Kingdom); § 5 (personal injuries and property damage based on an act in the United Kingdom). RAKIA's *forum non conveniens* argument nevertheless suggests that the State Immunity Act's exception for the consent of the foreign sovereign might apply if Azima brings his hacking claims in a London court. (*See* Def.'s Mem. at 38 ("The High Court is potentially better-suited to hear this dispute because RAKIA has already agreed to that court's jurisdiction.")) But the consent to jurisdiction that RAKIA points to as precedent was provided in a lawsuit that RAKIA brought against Azima for fraud regarding the sale of the Sheraton Hotel in Tbilisi, Georgia (*see* Claim Form & Particulars of Claim, Ex. K. to Def.'s Mot., ECF No. 31-14, at 5–7), and RAKIA is careful to avoid making any representation that it would necessarily consent to the High Court's jurisdiction with respect to the claims that Azima makes in the instant case. This omission is significant, because the State Immunity Act makes clear that a foreign sovereign's waiver of immunity is limited, and does not "extend[] to . . . any counter-claim unless it arises out of the same legal relationship or facts as the claim." State Immunity Act of 1978, c. 33, § 2(6). So, perhaps RAKIA is signaling its willing to

execute a fresh waiver of immunity that would cover the claims that Azima brings here (*see* Def.'s Reply at 23), but then again, it is also entirely possible that RAKIA will withhold consent, leaving Azima with “no forum in which he can litigate this dispute” (Pl.'s Opp'n at 51).

Moreover, even if RAKIA did consent to waiving its state immunity for the purposes of this lawsuit and Azima refiled his claims in the United Kingdom, RAKIA has not demonstrated that the United Kingdom offers an adequate remedy for the injuries Azima has complained of in this case. To be sure, “a foreign forum is not inadequate merely because it has less favorable substantive law,” *El-Fadl*, 75 F.3d at 678, and RAKIA points to the United Kingdom's Data Protection Act of 1998, 1998, c. 29 (U.K.), and cases decided under that act, in an attempt to show that some remedy is available for computer breaches under English law (*see* Def.'s Mot. at 38, Def.'s Reply at 23). But the U.K. statute's text makes clear that it only regulates (1) “data controllers”—i.e., individuals who “determine[] the purposes for which and the manner in which any personal data are, or are to be processed[,]” Data Protection Act of 1998, 1998, c. 29, § 1(1) (U.K.)—and (2) such individuals must be either “established in the United Kingdom” or “use[] equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom,” *id.* § 5(1). RAKIA is an entity based in the United Arab Emirates, not the United Kingdom, and this Court has no evidence that RAKIA uses equipment for processing personal data in the U.K. Thus, the Data Protection Act appears inapposite to Azima's dispute with RAKIA, and this circumstance also renders the case RAKIA cites, *Gulati v. MGN Ltd* [2015] EWHC 1482 (Ch), irrelevant. (*See* Def.'s Mot. at 38.) Without any declarations

from U.K. law experts, or any other evidence showing that Azima could sue RAKIA in the United Kingdom for the hacking harm that Azima alleges in this case, RAKIA has not carried its heavy burden of demonstrating that the United Kingdom is a forum that would provide Azima with an adequate remedy. *See, e.g., Nemariam*, 315 F.3d at 394–95 (noting that the defendant was “unable to substantiate its claim that [the plaintiff] will receive a remedy” in the proposed alternative forum); *Yueh-Lan Wang v. New Mighty U.S. Trust*, 322 F.R.D. 11, 25–26 (D.D.C. 2017) (“Defendants have not carried their burden to prove that an alternative forum is actually, not just theoretically, available.”).

RAKIA maintains that, despite the foregoing analysis, this Court should dismiss the instant action on *forum non conveniens* grounds because the March 2016 Settlement Agreement between Azima and RAKIA demands that it be so. (*See* Def.’s Mot. at 35 (arguing that “the Settlement Agreement between RAKIA and Azima contains a valid forum-selection clause, which represents the parties’ agreement as to the most proper forum, and should be given controlling weight in all but the most exceptional cases” (internal quotation marks and citation omitted).) To hear RAKIA tell it, the parties here previously entered into a binding contract that specifically relegates “any dispute or claim arising out of, or in connection with [the Settlement Agreement] or its subject matter or formation (including, without limitation, any contractual or non-contractual disputes, claims or obligations)” (Settlement Agreement at 5–6), and as a result, the instant action must be brought in a U.K. court.

Of course, to the extent that RAKIA has failed to establish that the United Kingdom’s courts provide an adequate remedy, this argument is irrelevant. But even if

RAKIA had shown that the United Kingdom provides an forum for Azima's claims, it is clear to this Court that RAKIA has mischaracterized the parties' Settlement Agreement. By its terms, the forum-selection clause in the March 2016 Settlement Agreement expressly pertains to disputes or claims that arise out of or connect to *the Settlement Agreement's* "subject matter or formation" (*id.* at 5), and it is indisputable that the "subject matter" of the Settlement Agreement was the then-existing dispute between the parties regarding the HeavyLift joint venture agreement (*id.* at 3 ("Each Party . . . wishes to resolve all outstanding issues relating to the [HeavyLift] Joint Venture Agreement.")). RAKIA cannot credibly maintain that the Settlement Agreement addressed or encompassed any and all new claims that might arise in the future based on actions of the signatories—especially those that do not pertain to the formation, execution, or terms of the Settlement Agreement—such as the allegedly egregious and tortious hacking of Azima's computers and dissemination of his Azima's personal information by RAKIA, much less that the parties intended to mandate that any future claims that arose out of acts that were not known to the parties when the HeavyLift joint venture dispute was settled must be litigated in London.

RAKIA's suggestion that, because Azima's complaint links the alleged hacking that is the subject of the instant action to RAKIA's commercial activity (including the HeavyLift joint venture) for FSIA purposes then this Court must also view the hacking and the HeavyLift joint venture as connected under the language of the Settlement Agreement (*see* Def.'s Mot. at 37; Def.'s Reply at 20–21) only goes so far. That is, it is clear to this Court that the alleged hacking may well have been undertaken in connection with the HeavyLift joint venture as set forth in Azima's complaint (i.e., it

was an act that was partly motivated by the parties' disputes in regard to that venture), and yet Azima's *claims* alleging that the computer hacking violates the CFAA and D.C. common law do not themselves arise from or connect to the "subject matter or formation" of the Settlement Agreement, which is what the parties clearly contemplated when they agreed that claims "arising out of, or in connection with" the Settlement Agreement must be filed in London. (Settlement Agreement at 5–6.) Stated simply, it is the subject matter *of the Settlement Agreement* that governs the scope and extent of the parties' forum-selection clause, and RAKIA does not, and cannot, maintain that the hacking conduct of which Azima complains here was addressed in, or was a reasonably foreseeable result of, that agreement, such that the forum-selection clause governs.

Without the support of the settlement agreement, RAKIA's *forum non conveniens* motion depends solely on this Court finding that the balance of public and private interests weigh in favor of a London forum, and then dismissing this lawsuit conditioned upon the lawsuit being litigated in that jurisdiction. *See, e.g., MBI Grp., Inc. v. Credit Foncier Du Cameroun*, 558 F. Supp. 2d 21, 31–32 (D.D.C. 2008) (conditioning dismissal on defendants' submission to Cameroonian jurisdiction). And such an analysis is unnecessary here, because RAKIA has failed to demonstrate the availability of an adequate alternative forum, as explained above. *See El-Fadl*, 75 F.3d at 677 ("Only if there is an adequate alternative forum must the court then weigh the relative conveniences to the parties against the presumption of the plaintiff's forum selection."). But even if the Court was to proceed to the balancing stage, it would find that RAKIA has not demonstrated that the balance of public and private factors has "a strong tilt towards a particular forum[.]" *Petroleo Brasileiro S.A.*, 246 F. Supp. 3d at 74

(quotation marks and citation omitted), because RAKIA's primary argument in this regard relies upon the inapposite forum-selection clause that appears in the March 2016 Settlement Agreement.

IV. CONCLUSION

For the reasons explained above, this Court has subject matter jurisdiction over Azima's claims under the commercial activity exception of the FSIA, and RAKIA's *forum non conveniens* argument fails. Accordingly, and as set forth in the accompanying Order, RAKIA's motion to dismiss is **DENIED**.

DATE: March 30, 2018

Ketanji Brown Jackson
KETANJI BROWN JACKSON
United States District Judge