D.C. Court Rules that Cyberattack Victim Can Sue Foreign State's Agency or Instrumentality under the FSIA

A recent decision by a federal district court in Washington, D.C., opened a path for bringing transnational computer hacking claims against foreign states and their agencies and instrumentalities under the commercial activity exception of the Foreign Sovereign Immunities Act (FSIA).[1] The case is notable because it comes on the heels of a decision last year by the U.S. Court of Appeals for the D.C. Circuit, which held that cyberattacks originating from outside the United States do not fall within the scope of the FSIA's non-commercial, tortious conduct exception, which requires the alleged tort to have occurred "*entirely* in the United States."[2]

These decisions suggest that U.S. courts are still shaping the contours of the FSIA in dealing with claims against foreign sovereigns for their alleged participation in cyberattacks and cyberespionage having links to the United States.

I. Allegations of Computer Hacking arising from Commercial Dealings

The latest case arose from a business relationship between Farhad Azima, a U.S. businessman who resides in Missouri, and RAKIA, a commercial investment entity of the United Arab Emirates (UAE). For decades, Azima and RAKIA engaged in various business dealings, including foreign joint ventures and, more recently, an arrangement in which Azima was retained to mediate a dispute between RAKIA and its former CEO.

The complaint alleged that, throughout the mediation, computer hackers repeatedly broke into Azima's personal and business laptops and took files and other data, using two IP addresses in the United States. The hackers' location was unknown. The hackers also infected Azima's laptops with malware, which damaged the devices. Unaware of these attacks, Azima continued to use the computers to communicate about privileged and confidential matters with the former CEO's attorneys.[3] The mediation eventually broke down, and RAKIA threatened an "all-out war" against its former CEO and Azima.[4]

Shortly thereafter, multiple websites started to publish information about Azima, including text messages, photos, voicemails and other data from his iCloud account, as well as documents saved on his computers. RAKIA also threatened to sue Azima in a letter attaching documents with confidential details that he kept only on his laptops.

---

[1] *Azima v. Rak Inv. Auth.*, No. 16-cv-1948, 2018 U.S. Dist. LEXIS 53648, at *1 (Mar. 30, 2018).

[2] *Doe v. Fed. Democratic Republic of Ethiopia*, 851 F.3d 7, 8 (D.C. Cir. 2017) (emphasis in original).

[3] *Azima*, 2018 U.S. Dist. LEXIS 53648, at *7.

[4] *Id.* at *8.

Azima claimed that "RAKIA commissioned the repeated surreptitious hacking" and then published the "disparaging material that was illicitly gleaned" from his devices, all to gain an advantage in their commercial dealings and to punish him for his failed role in the mediation.[5] According to the complaint, RAKIA's conduct violated the Computer Fraud and Abuse Act (CFAA) and constituted common-law conversion and unfair competition.

II. Jurisdiction Is Proper under the Commercial Activity Exception

Because RAKIA qualified as an agency or instrumentality of a foreign state (the UAE), jurisdiction for the suit was premised on the FSIA specifically the tortious conduct and commercial activity exceptions to sovereign immunity. RAKIA moved the court to dismiss the claims on various grounds, including for lack of jurisdiction.

The U.S. District Court for the District of Columbia denied the motion and allowed the case to proceed. The court addressed the interaction between the tortious conduct and commercial activity exceptions. Although the D.C. Circuit had recently ruled that transnational hacking did not fall within the *tortious conduct* exception—which requires both the tort and the injury to occur inside the United States—the district court held that the *commercial activity* exception could apply, regardless of those geographic limitations, if the hacking was sufficiently connected to the parties' commercial dealings.

The commercial activity exception has three independent clauses, each of which supports jurisdiction in different situations. The court's analysis centered on the last two clauses: those provisions authorize jurisdiction in cases where the action is based upon "an injurious act that was performed either within the United States in connection with commercial activity outside the United States [the second clause], 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 [the third or 'direct effect' clause]."[6]

The court found that the business dealings between Azima and RAKIA were commercial in nature, and that they had occurred outside the United States. Thus, the key questions were (1) whether the cyberattacks occurred "in connection with" those commercial activities, (2) whether the hacks had a "direct effect" in the United States, and (3) whether the hacking itself took place inside or outside the United States.[7]

First, the court interpreted the phrase "in connection with a commercial activity" narrowly to mean that "the acts complained of must have some substantive connection

[5] *Id.* at *1.

[6] *Id.* at *18-19 (citing 28 U.S.C. § 1605(a)(2)).

[7] *Id.* at *19.

or a causal link to the commercial activity."[8] The court concluded that Azima had "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" in the demand letter.[9] The "in connection with a commercial activity" requirement was thus satisfied.

Second, because cyberattacks "sound in tort," the "direct effect" analysis focused on the place where the tortious act was completed—typically the location where the plaintiff suffers the injury—rather than on the place of performance as would be relevant in contract cases.[10] Thus, the direct effect inquiry depended only on "whether or not the plaintiff sustained his cognizable injury in the United States."[11] "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 supports an inference that at least one of [his] U.S.-based personal and business laptops was in the United States when the hacking occurred," Azima had sufficiently pleaded a "direct effect."[12]

Since the allegations satisfied the first two requirements, the court concluded that jurisdiction was proper under the "direct effect" clause and passed on deciding the third question: the location of the hacks. The court explained that it did not matter where the hacking had originated because, unlike the *tortious conduct* exception, the *commercial activity* exception did not require that the tort occur entirely within the United States; just that there be either an injurious act in the United States, or an act outside the United States that injured the plaintiff in the United States.[13] Although it is difficult to determine exactly where cyberattacks occur, as explained by the D.C. Circuit in the earlier case, it was "indisputable" that the hacking of Azima's laptops happened somewhere in or outside the United States.[14] Either way, jurisdiction would be proper under the second or third clause. And since the claims satisfied the "more stringent" test under the third clause, the court did not have to rule on the second clause.[15]

---

[8] *Id.* at *32 (quoting *Adler v. Fed. Republic of Nigeria*, 107 F.3d 720, 726 (9th Cir. 1997)) (citing *Fed. Ins. Co. v. Richard I. Rubin & Co.*, 12 F.3d 1270, 1289-91 (3d Cir. 1993)).

[9] *Id.* at *35 (alteration supplied).

[10] *Id.* at *37.

[11] *Id.* at *37-38 (citing *Atlantica Holdings v. Sovereign Wealth Fund Samruk-Kazyna JSC*, 813 F.3d 98, 109 (2d Cir. 2016)). Under the FSIA, the alleged effect also had to be "more than purely trivial." *Id.* at *38 (quoting *Princz v. Fed. Republic of Ger.*, 26 F.3d 1166, 1172 (D.C. Cir. 1994)). The court found that the destruction of data on the defendant's laptop was sufficiently significant. *Id.* at *44.

[12] *Id.* at *39

[13] *Id.* at *44-49.

[14] *Id.* at *49.

[15] *Id.*

The court also found that the cyberattacks were the harmful acts that formed the basis of the claims as required under the commercial activity exception. Under the CFAA, a defendant is liable if it "intentionally accesses a protected computer without authorization" and causes financial loss above a certain amount.[16] Likewise, for unfair competition, the "gravamen" of the claim is the interference with Azima's "business computers."[17] And for conversion, the tortious conduct occurs "where the force takes effect on the thing."[18] The court was therefore satisfied that the alleged hackings were the acts that caused the injuries in the United States under these theories of liability.

The court concluded with an observation on the potential consequences of its decision: "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. . . . [U]nless 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."[19]

* * * * *

About Curtis

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 17 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

[16] *Id.* at *41 (quoting 18 U.S.C. §§ 1030(a)(5), (c)(4)(A)(i)(I), (g)).

[17] *Id.* at *41, *42.

[18] *Id.* at *42.

[19] *Id.* at *49-50.

Please feel free to contact any of the persons listed below if you have any questions on this important development:

Joseph D. Pizzurro
Partner
jpizzurro@curtis.com
New York: +1 212 696 6196

Robert B. Garcia
Partner
robert.garcia@curtis.com
New York: +1 212 696 6052

Kevin A. Meehan
Associate
kmeehan@curtis.com
New York: +1 212 696 6197

Juan O. Perla
Associate
jperla@curtis.com
New York: +1 212 696 6084