IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FARHAD AZIMA, **ALG TRANSPORTATION, INC.,** **MAIN 3260 LLC,** **FFV W39 LLC, and** **FFV DEVELOPMENT LLC,** **Plaintiffs,** **v.** **DECHERT LLP,** **DAVID NEIL GERRARD,** **DAVID GRAHAM HUGHES,** **NICHOLAS DEL ROSSO,** **VITAL MANAGEMENT SERVICES, INC.,** **AMIT FORLIT,** **INSIGHT ANALYSIS AND RESEARCH LLC,** **SDC-GADOT LLC,** **AMIR HANDJANI,** **ANDREW FRANK, and** **KARV COMMUNICATIONS,** **Defendants.**	**Civil Action No:** **COMPLAINT** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

Page

INTRODUCTION 1

PARTIES AND NON-PARTY CO-CONSPIRATORS 4

Plaintiffs 4

RICO Defendants 5

Non-Party Co-Conspirators and Members of the Enterprise 9

JURISDICTION AND VENUE 12

FACTUAL ALLEGATIONS 17

I. THE INITIAL CRIME: UNLAWFUL DETENTION AND INTERROGATION OF AL SADEQ 17

A. Dechert and Gerrard Unlawfully Detain and Interrogate Al Sadeq 17

B. Azima and Others Attempt to Expose the Enterprise's Human Rights Violations 18

II. THE ATTACK ON AZIMA: HACKING, THEFT, AND FRAUDULENT LITIGATION 19

A. The Enterprise Hacks Azima, His Associates, and Other Perceived Enemies of RAK 19

B. The Enterprise Creates Its 2016 Action Plan to Harm Azima and Others 23

C. The Enterprise Induces Azima to Enter into a Fraudulent Settlement Agreement 24

D. The Enterprise Launders Azima's Stolen Data on the Internet 25

E. The Enterprise Brings Civil Litigation Against Azima 27

III. THE COVER-UP: OBSTRUCTION OF JUSTICE, A PROTRACTED SMEAR CAMPAIGN, AND A FABRICATED CRIMINAL INVESTIGATION 28

A. The Enterprise Seeks to Influence U.S. Law Enforcement in an Effort to Manufacture a Criminal Investigation of Azima and Others 29

B. The Enterprise Launches a Media Campaign to Harm Azima 30

C. Obstruction of Azima's D.C. District Court Proceeding 31

1. The Enterprise Makes False Statements in the D.C. District Court Proceeding and Develops False Testimony to Conceal Its Role in the Hacking of Azima 32

2. The Enterprise Destroys Evidence and Makes False Statements Regarding Evidence Preservation 40

3. The Enterprise Defrauds the D.C. District Court by Submitting Stolen Documents Laundered Through Lebanon 42

D. The Enterprise Obstructs Multiple Proceeding in the U.S. Under 28 U.S.C. § 1782 Related to Azima's UK Case 44

1. Handjani Obstructs Azima's Section 1782 Proceeding in New York 45

2. Forlit Obstructs Azima's Section 1782 Proceeding in Florida 46

E. Del Rosso Obstructs Azima's North Carolina Proceeding 48

1. The Enterprise Fabricates Evidence in the U.S. and Threatens Its Own Hackers 49

2. Enterprise Member Del Rosso Makes False Statements to the North Carolina District Court 52

F. The Enterprise Conducts Further Hacking to Determine the Sources of Funding for Azima's and Al Sadeq's Litigation 53

1. The Enterprise Seeks to Determine Who Was Funding Litigation Brought by Azima and Al Sadeq 53

2. The Enterprise Hacks Al Sadeq's Lawyers 54

3. The Enterprise Bribes Potential Witnesses in U.S. Proceedings 55

4. Del Rosso Obstructs Al Sadeq's Section 1782 Proceeding in North Carolina 57

IV. THE ENTERPRISE'S CRIMES AND COVER-UP HAVE CAUSED SIGNIFICANT DAMAGE TO AZIMA AND HIS BUSINESSES 57

V. DECHERT IS LIABLE FOR THE ACTIONS OF THE ENTERPRISE 59

A. Dechert Was at Least Recklessly Indifferent to Overwhelming Evidence of the Enterprise's Crimes 60

B. Dechert Played a Central Role in the Cover-Up of the Enterprise's Crimes 62

CLAIMS FOR RELIEF 66

FIRST CLAIM FOR RELIEF 66

The RICO Enterprise 66

Pattern of Racketeering Activity 67

1. Obstruction of Justice in Violation of 18 U.S.C. § 1503 68

2. Witness Tampering in Violation of 18 U.S.C. § 1512 69

3. Money Laundering in Violation of 18 U.S.C. § 1956(a)(2)(A) 69

4. Mail Fraud and Wire Fraud in Violation of 18 U.S.C. §§ 1341 and 1343 70

5. Bank Fraud in Violation of 18 U.S.C. § 1344 72

Summary of the Pattern of Racketeering Activity Alleged as to Each RICO Defendant 74

Injury to Plaintiffs' Business and Property 78

SECOND CLAIM FOR RELIEF 80

PRAYER FOR RELIEF 82

COMPLAINT

Plaintiffs Farhad Azima ("Azima"), ALG Transportation, Inc. ("ALG"), Main 3260 LLC ("Main 3260"), FFV W39 LLC ("FFV W39"), and FFV Development LLC ("FFV Development") (collectively, "Plaintiffs") allege as follows:

INTRODUCTION

1. For almost a decade, a sophisticated and organized group of individuals and entities (the "Enterprise") led by Neil Gerrard ("Gerrard") engaged in a global campaign against perceived enemies of Ras Al Khaimah ("RAK"),[1] a client of Dechert LLP ("Dechert"). RAK itself has recently accepted legal responsibility for some of the misconduct and formally sought to distance itself from Dechert and Gerrard, claiming in a recent court submission that it also has been victimized by the misconduct of Dechert and Gerrard described in this Complaint.

2. Dechert was hired by RAK to investigate the activities of Khater Massaad – the former head of RAKIA – and his associates. Dechert's work grew into a sprawling international investigation, led by Gerrard but involving other Dechert lawyers and various outside service providers, that spawned numerous related lawsuits in multiple countries.

3. One of the Massaad associates who became a target of the investigation was Karam Al Sadeq, who served as legal adviser, Group Legal Director, and, ultimately, Deputy Chief Executive Officer of RAKIA between 2008 and 2012. In 2014, Al Sadeq was renditioned from the United Arab Emirates ("UAE") and then detained indefinitely in a prison in RAK. In a lawsuit he filed in the High Court of Justice of England and Wales, Queen's Bench Division, captioned *Karam Salah Al Din Awni Al Sadeq v. Dechert, LLP, Neil Gerrard, David Hughes, and*

[1] For simplicity, the term RAK is used throughout this complaint to refer to the emirate, the Ruler of RAK, the sovereign wealth fund Ras Al Khaimah Investment Authority ("RAKIA"), and other RAK-based entities.

Caroline Black, Claim No. QB-2020-000322, Al Sadeq alleges that Gerrard and other members of the Enterprise violated international and United Arab Emirates law, as well as his human rights, during his detention.

4. Between 2007 and 2016, Farhad Azima was involved in various actual and proposed commercial joint ventures with RAK. Azima became a target of Dechert's investigation on behalf of RAK when he sought to expose RAK's history of human rights abuses generally and, in particular, the human rights abuses against Al Sadeq and Gerrard's role in Al Sadeq's mistreatment.

5. To silence Azima and others involved in seeking to generate press coverage, the Enterprise hacked the confidential computer data of Azima and others, and used that illegally obtained information to induce an agreement from Azima arising out of unrelated prior business contacts between Azima and RAK, with a premeditated plan to commence a lawsuit against Azima alleging violation of that agreement. *See Ras Al Khaimah Inv. Auth. v. Farhad Azima*, [2020] EWHC 1327, Case No. HC-2016-002798. The documented goal of this litigation was to silence Azima by financially and reputationally crippling him.[2]

6. Azima refused to buckle, however, and instead filed suit in the U.S. District Court for the District of Columbia against RAKIA for stealing his data, *Azima v. RAK Investment Authority*, No. 1:16-cv-01948. To counter the threat that started with Azima's 2016 U.S. hacking lawsuit and increased in urgency with the Al Sadeq's 2020 UK lawsuit, the Enterprise began a

[2] The UK case seeks damages for the 2016 hacking of Azima. This Complaint seeks damages for conduct that post-dates the 2016 hacking. In effect, the UK case focuses on crimes that occurred in or about 2016, while this Complaint focuses on efforts to cover-up those crimes. In addition, the parties in the two cases are not identical, and this Complaint includes defendants Handjani, Frank, KARV, Insight, SDC-Gadot, and Forlit, who are US persons and entities, and along with Defendant Hughes are not defendants in the UK case. UK law does not have a comparable statute to RICO.

more than six-year effort to cover up its role in the hacking of Azima and mistreatment of Al Sadeq.

7. The Enterprise's actions consisted of a continuing pattern of racketeering activity in the U.S. and elsewhere and involved the commission of numerous crimes under U.S. federal law, including money laundering, obstruction of justice, witness tampering, mail and wire fraud, further computer hacking, and the theft of highly confidential information, documents, and materials. The predicate acts committed by the Enterprise in the course of its cover-up campaign have caused Plaintiffs substantial harm in the U.S. to their business and property.

8. Dechert played a central role in the Enterprise's affairs and criminal activity. To carry out its scheme, Gerrard and the Enterprise relied upon Dechert's infrastructure, partners, employees, financial resources, and reputation. Dechert received millions of dollars in fees as a direct result of the Enterprise's continuing campaign of criminal conduct. Dechert and its leadership were at least willfully blind or recklessly indifferent to Gerrard's misconduct. The firm ignored "red flags" regarding Gerrard beginning when it first hired him as a partner in 2010 and turned a blind eye to increasingly clear evidence that emerged over the following decade showing that Gerrard was involved in serious ethical violations, human rights abuses, and criminal activity, including hacking.

9. In response to the Enterprise's criminal campaign, much of which occurred in the U.S., involved U.S. persons and companies, and was perpetrated through the U.S. financial system, Azima now brings this action under the Racketeering Influenced and Corrupt Organizations ("RICO") Act, 18 U.S.C. §§ 1961, *et seq*. The Enterprise's efforts to conceal its criminal conduct included the commission of numerous predicate acts under RICO, including: obstruction of justice, witness tampering, wire fraud, mail fraud, bank fraud, and money laundering. Allegations made

in this Complaint have been substantiated by sworn statements provided by members of the Enterprise and/or corroborated by documentary evidence.[3] As alleged in further detail below, Azima (a U.S. citizen) and his co-Plaintiffs (U.S.-based entities) have suffered significant and direct harm in the U.S. from these predicate criminal acts. That harm, which included damage to Azima's businesses, legal expenses, a UK judgment, and loss of litigation interests, were foreseeable and were intended by the Enterprise. Indeed, the Enterprise described these goals in writing. Plaintiffs are therefore entitled to recover treble damages from the RICO Defendants (as defined further below) and to other relief for the harm they have suffered at the hands of the Enterprise as a result of its long-running scheme.

PARTIES AND NON-PARTY CO-CONSPIRATORS

Plaintiffs

10. Plaintiff Farhad Azima is a U.S. citizen and businessman who has resided and worked in Kansas City, Missouri, since immigrating to the U.S. A successful entrepreneur, Azima founded and built numerous successful companies over the course of almost 50 years, including serving as chairman and CEO of multiple airlines. His companies have provided vital transportation services to the U.S. Department of Defense and the UK Ministry of Defence. Among other awards, he is a recipient of the Ellis Island Medal of Honor, which is bestowed on individuals who have made valuable contributions to the American way of life and immigrants who have preserved the distinct values and heritage of their ancestors. Azima was appointed by the President of the United States to the U.S. Economic Development Commission, and he

[3] Azima has obtained sworn affidavits from multiple members of the Enterprise, bank records, invoices, and copies of reports prepared by the Enterprise that included hacked data from Azima and his associates, as well as significant circumstantial evidence. All of this evidence was uncovered less than four years before the filing of this Complaint, and in most cases the evidence was obtained in the past year.

currently serves on the Board of Trustees of the United States Army Command and General Staff College Foundation and the American University of Afghanistan.

11. Plaintiff ALG Transportation, Inc. is a Missouri corporation with its principal place of business in Kansas City, Missouri. ALG is wholly owned by Azima.

12. Plaintiff Main 3260 LLC is a Missouri company with its principal place of business in Kansas City, Missouri. Main 3260 is a wholly-owned subsidiary of FFV Development LLC. As alleged in further detail below, it suffered significant harm as a result of the Enterprise's predicate acts.

13. Plaintiff FFV W39 LLC is a Missouri company with its principal place of business in Kansas City, Missouri. FFV W39 is a wholly owned subsidiary of FFV Development LLC. As alleged in further detail below, it suffered significant harm as a result of the Enterprise's predicate acts.

14. Plaintiff FFV Development LLC is a Missouri company with its principal place of business in Kansas City, Missouri. Azima owns 50% of FFV Development. As alleged in further detail below, it suffered significant harm as a result of the Enterprise's predicate acts.

RICO Defendants

15. Defendant Dechert LLP ("Dechert") is a Pennsylvania limited liability partnership registered in New York and also incorporated in the UK. Dechert is a global law firm with 22 offices around the world, including 10 in the U.S. As the firm has acknowledged in connection with a federal court proceeding, Dechert operates as a single firm and its offices are effectively a single entity. Dechert itself is a central figure in the RICO scheme. As alleged in further detail below, the Enterprise relied heavily on Dechert's personnel, infrastructure, offices, finances, and reputation to execute its scheme. Senior firm leadership was at least recklessly indifferent to the misconduct. Gerrard and others carried on the affairs of the Enterprise out of Dechert's New York

office, and the firm benefited substantially from the Enterprise's criminal activity, receiving millions of dollars in fees between 2014 and 2020.

16. Defendant Gerrard is one of the leaders of the Enterprise. Between 2011 and 2020, he was a partner, Global Co-Head of the White-Collar and Securities Litigation Practice, and member of Dechert's Policy Committee. In those roles, and using the substantial resources provided to him and the Enterprise by Dechert, Gerrard directed and oversaw the Enterprise's scheme to defraud and harm the Plaintiffs and the years-long cover up of the Enterprise's crimes.

17. Defendant David Graham Hughes ("Hughes") is a lawyer and former Dechert partner who served as a high-level deputy of Gerrard in the Enterprise. Between September 2014 and June 2017, Hughes was a partner at Dechert, where he worked closely with Gerrard in organizing and structuring the Enterprise, coordinating and carrying out its affairs, and directing and executing its illegal acts. After suddenly leaving Dechert in 2017 and bringing the UK proceeding with him, Hughes joined Stewarts Law LLP as a partner, where he continued to work with Gerrard to manage and execute the affairs of the Enterprise, including its criminal cover-up campaign.

18. Defendant Nicholas Del Rosso ("Del Rosso") lives and resides in Charlotte, North Carolina, and is the owner of Defendant Vital Management Services, Inc. ("Vital"), a company organized and based in North Carolina. Del Rosso and Vital were hired by the Enterprise, acting through Gerrard and Dechert, to conduct illegal computer hacking operations on its behalf in the U.S. and elsewhere. Del Rosso repeatedly met with other members of the Enterprise in New York to plan and coordinate its affairs. Del Rosso also worked with other members of the Enterprise to obtain and disseminate hacked and stolen materials to harm Azima and others; to obstruct multiple proceedings in U.S. courts related to the Enterprise's misconduct; and to manipulate U.S. law

enforcement into investigating Azima in an effort to silence Azima and distract from and conceal the Enterprise's own criminal conduct.

19. Defendant Vital is a company organized under the laws of North Carolina and located at 1340 Environ Way, Chapel Hill, North Carolina, 27517. Vital purports to provide legitimate private investigative services but was, in fact, used by Del Rosso to participate in the Enterprise's criminal conduct, including the receipt and transfer of funds into and from the U.S. to pay for and promote the Enterprise's illegal hacking operations and obstruction-of-justice campaign.

20. Defendant Amit Forlit ("Forlit") is a resident of Israel and the owner of U.S. companies Insight Analysis and Research LLC ("Insight") and SDC-Gadot LLC ("SDC-Gadot"). Acting at the direction of Gerrard and other members of the Enterprise, Forlit orchestrated the hacking and theft of private emails, and then assisted the Enterprise in covering up such conduct through the obstruction of U.S. judicial proceedings. To carry out these crimes and conceal their past criminal actions on behalf of the Enterprise, Forlit utilized Insight and SDC-Gadot to receive and transfer funds into and from the U.S. to pay for and promote the Enterprise's hacking operations and obstruction-of-justice campaign.

21. Defendant Insight is a limited liability company organized under the laws of Florida with its principal place of business at 13727 SW 152 Street, Unit 715, Miami, Florida. Insight is one of two U.S. entities created, owned, and controlled by Forlit that the Enterprise used to receive millions of U.S. dollars in U.S. bank accounts sent from outside the U.S., which was then used by the Enterprise to pay for and promote its hacking operations and obstruction-of-justice campaign, including through further transfers to bank accounts outside of the U.S. In addition, Forlit used

Insight to engage in further transfers in the U.S. to launder funds intended to pay for the Enterprise's unlawful activity.

22. Defendant SDC-Gadot is a limited liability company organized under the laws of Florida with its principal place of business at 210 West 89th Street, Apt 1K, New York, New York, 10024. SDC-Gadot is one of two U.S. entities created, owned, and controlled by Forlit that the Enterprise used to receive millions of U.S. dollars in U.S. bank accounts sent from outside the U.S., which was then used by the Enterprise to pay for and promote its hacking operations and obstruction-of-justice campaign, including through further transfers to bank accounts outside of the U.S. In addition, Forlit used SDC-Gadot to engage in further transfers in the U.S. to launder funds intended to pay for the Enterprise's unlawful activity.

23. Defendant Amir Handjani ("Handjani") is a U.S. citizen who lives in New York, New York, and currently serves as a "Senior Advisor" with Defendant KARV Communications Inc. ("KARV"). Handjani repeatedly met with other members of the Enterprise in New York and elsewhere to plan and coordinate its attacks on Azima and cover-up of the Enterprise's criminal actions. Handjani served for many years as a "front man" for the Enterprise, tasked with responsibility for befriending Azima and deceiving him as to the Enterprise's role in the hacking and theft of his documents, materials, and other information. Handjani also received reports prepared by Enterprise hackers, regularly attended high-level Enterprise meetings at Dechert's New York offices, and guaranteed offers of payment to witnesses in exchange for testimony concealing the roles of Enterprise members.

24. Defendant Andrew Frank ("Frank") is a U.S. citizen who lives in New York, New York, and is the founder and current President of Defendant KARV Communications. Frank repeatedly met with other members of the Enterprise in New York to plan and coordinate its affairs,

received materials unlawfully obtained from Azima and others by the Enterprise through hacking, and then disseminated those materials to the press for the purpose of attacking the credibility of Azima and others associated with Azima.

25. Defendant KARV is a purported communications and lobbying firm located at 370 Lexington Avenue, Suite 2001, New York, NY 10017. According to Foreign Agents Registration Act ("FARA") filings, KARV has served as a registered foreign agent of RAK since 2013. KARV was a key architect of the Enterprise's broader strategy for attacking and harming Azima. In addition, KARV received materials unlawfully obtained from Azima and others by the Enterprise through hacking and then disseminated those materials to the press for the purpose of attacking the credibility of Azima and others associated with Azima.

Non-Party Co-Conspirators and Members of the Enterprise

26. The Enterprise also included additional individuals and business entities (together with the Defendants, the "RICO Conspirators") who are not named as parties here. These members played important roles in the affairs of the Enterprise, including participating in the obstruction of justice and wire fraud scheme to harm and bankrupt Azima. Non-party RICO Conspirators include the following individuals and entities:

a. RAKIA is a sovereign wealth fund of the Emirate RAK, one of the United Arab Emirates. RAK and its Ruler control RAKIA. RAK hired Dechert, Gerrard, Hughes, James Edward Dennison Buchanan ("Buchanan") and Stuart Robert Page ("Page"), to conduct investigations involving Azima and others. In 2016, the Enterprise used Azima's stolen data to induce him to enter into a fraudulent settlement agreement with RAKIA (the "2016 Settlement Agreement") designed to ensnare him costly litigation.

b. Sheikh Saud Bin Saqr Al-Qasimi (the "Ruler") is the head of state of the Emirate of Ras Al Khaimah, which owns and controls RAKIA.

c. Buchanan is a resident of the UK and Canada (and at one point neighbor of Gerrard) who served as a key lieutenant of Gerrard in the operation of the Enterprise. Between 2014 and 2019, Buchanan worked closely with Gerrard in organizing and structuring the Enterprise, coordinating its affairs, and executing its illegal acts. Buchanan also used at least one shell company to pay for illegal activity on behalf of the Enterprise. Buchanan has transacted business and engaged in tortious and illegal conduct on behalf of the Enterprise in the U.S. and New York that gives rise in part to Plaintiffs' claims.

d. Page is a resident of the UK who helped organize the Enterprise's unlawful hacking operations. Acting on behalf of the Enterprise, Page hired others to assist in the Enterprise's hacking and wired funds from overseas into the U.S. to pay for and promote the Enterprise's hacking operations. Page also took part in the Enterprise's efforts to cover up its criminal activity by obstructing U.S. judicial proceedings, conspiring with other members of the Enterprise to provide false testimony regarding the source of the hacked and stolen materials. A UK court found that Page had given false testimony on this topic.

e. Eitan Arusy ("Arusy") is a resident of the U.S. who participated in regular meetings with Gerrard, Buchanan, Page, and Forlit regarding reports prepared by Page and Forlit that assembled and relayed information about Azima and others obtained through the Enterprise's unlawful hacking operations. Acting on behalf of the Enterprise, Forlit paid Arusy through Arusy's U.S.-based entity, Global Impact Services, LLC ("Global Impact Services"). In addition, although the reasons remain unclear, Arusy, through Global Impact Services, paid Forlit more than $700,000 on behalf of the Enterprise from September 2020 through September 2021.

f. Patrick Tristram Finucane Grayson ("Grayson") is a resident of the UK who procured, processed, and laundered stolen materials for the Enterprise. Together with the RICO Defendants, Grayson also obstructed U.S. proceedings on behalf of the Enterprise to cover up the Enterprise's criminal activity through witness tampering, concealment of evidence, and other obstructive conduct.

g. Paul Robinson ("Robinson") is a resident of the UK. He was paid by the Enterprise to hack certain victims on behalf of the Enterprise and to steal their data, documents, and information. Robinson also conspired with other members of the Enterprise to conceal the Enterprise's unlawful conduct through the destruction of documents. Robinson reported to Del Rosso and was at times supervised by Grayson.

h. Cyber Root Risk Advisory Private Limited ("Cyber Root") is a firm based in India that regularly engages in illegal hacking. On behalf of the Enterprise, Del Rosso and Vital paid Cyber Root over one million U.S. dollars using the U.S. financial system for hacking Azima, stealing his confidential data, documents, and personal information, and orchestrating their release on the internet.

i. Aditya Jain ("Jain") is a resident of India and the owner of Indian cyber company Cyber Defense and Analytics ("Cyber Defense"). Acting at the direction of Del Rosso, Jain and Cyber Defense hacked and stole private emails, documents, records, and other information from Azima and his associates. On behalf of the Enterprise, Del Rosso and Vital paid Jain, through Cyber Defense, significant sums of money in U.S. dollars sent from the U.S. for this hacking.

j. Majdi El Halabi ("Halabi") is a resident of Israel and a purported journalist. Halabi conspired with other members of the Enterprise, including Gerrard, Forlit, Page, and

Buchanan, to obstruct U.S. judicial proceedings and cover up the Enterprise's unlawful activities by, among other things, providing false testimony regarding the source of the hacked and stolen materials. A UK court found that Halabi had given false testimony on this topic and that his story on discovering the hacked documents with a simple Google search was "not true."

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. §§ 1331 and 1332, and under 18 U.S.C. § 1964(c). Plaintiffs' first claim for relief arises under 18 U.S.C. §§ 1961-1968, as alleged in further detail in this Complaint.

28. Venue is proper in this District under 28 U.S.C. § 1391(b)(2), as a substantial number of the events giving rise to this action occurred in this District, and also under 18 U.S.C. § 1965(a) because Defendants Dechert, KARV, Frank, and Handjani conduct their affairs in New York.

29. Personal jurisdiction exists over Dechert under 18 U.S.C. § 1965(a) because Dechert conducts its affairs in New York. Dechert has an office at Three Bryant Park, 1095 Avenue of the Americas, New York, New York. Dechert's website states: "Established in 1980, Dechert's New York office is our largest and most globally focused office in the United States." Dechert LLP, *New York Office*, https://www.dechert.com/locations/offices/new-york.html (last visited Oct. 13, 2022). Many of Dechert's decision-making stakeholders are also based in New York and because Dechert conducts extensive business activities in the state, and by and through the activities of its partners who are based out of and participate from New York. In addition, Dechert is a Pennsylvania-organized LLP. The exercise of jurisdiction over Dechert is proper in this District pursuant to 18 U.S.C. § 1965(b), and the ends of justice require application of the nationwide service provisions of 18 U.S.C. § 1965(b) because there is no district in which all of

the RICO Defendants could otherwise be tried together. Dechert has also transacted business and engaged in conduct in the United States and New York that gives rise to Azima's claims. Among other things, Enterprise meetings were regularly held at Dechert's offices in New York, and were attended by Dechert leaders, partners, and others. Dechert partners made or caused to be made false and misleading statements from New York, and participated in cover-up meetings from New York. As described in this Complaint, Dechert has served as a central figure in the conspiracy against Azima.

30. Exercise of jurisdiction over Defendants Andrew Frank and KARV Communications is reasonable and proper in this District pursuant to 18 U.S.C. § 1965(a) because Frank is a resident of New York and KARV is a New York entity, and both conduct extensive business within the state, including activities which give rise in part to Plaintiffs' claims. Frank is the Founder and President of KARV Communications, which is located and does business in New York. KARV's decision-making stakeholders are based in New York. Through his activities in New York, Frank participated in the Enterprise by defrauding Azima and causing the filing of false statements in U.S. and UK courts in service of the Enterprise's goal of inflicting reputation harm and massive litigation costs on Azima.

31. Exercise of jurisdiction over Defendant Handjani is reasonable and proper in this District pursuant to 18 U.S.C. § 1965(a) because Handjani is a citizen of New York and conducts extensive business activities within the State, including activities which give rise in part to Plaintiffs' claims. Handjani is employed by New York-based KARV Communications. Handjani met with Gerrard and other Dechert partners in New York regarding Enterprise business. Through his activities in New York, Handjani has assisted the Enterprise in defrauding Azima, causing the

filing of false statements in U.S. and UK courts in service of the Enterprise's goal of inflicting reputation harm and massive litigation costs on Azima, and tampering with witnesses.

32. Defendant Del Rosso is resident in North Carolina, and Vital is incorporated and has its principal place of business in North Carolina. The exercise of jurisdiction over each of these Defendants is proper in this District pursuant to 18 U.S.C. § 1965(b), and the ends of justice require application of the nationwide service provisions of 18 U.S.C. § 1965(b) because there is no district in which all of the RICO Defendants could otherwise be tried together. Defendants Del Rosso and Vital also transacted business and engaged in conduct in the United States and New York which give rise in part to Plaintiffs' claims. Del Rosso, at times through his company Vital,[4] participated in meetings in New York with the RICO Conspirators in which they discussed and planned the use of the hacked data and deploying false statements in U.S. and UK courts and to U.S. law enforcement agencies in service of the Enterprise's goal of inflicting reputation harm and litigation costs on Azima. In addition, Del Rosso and Vital used the U.S. financial system to send multiple wires overseas for the purpose of promoting unlawful criminal activity and, on information and belief, these wires passed through New York on their way overseas.

33. Defendant Insight is a Florida company owned and controlled by Forlit. The exercise of jurisdiction over this defendant is proper in this District pursuant to 18 U.S.C. § 1965(b), and the ends of justice require application of the nationwide service provisions of 18 U.S.C. § 1965(b) because there is no district in which all of the RICO Defendants could otherwise be tried together. Insight also transacted business and engaged in conduct in the United States and New York that give rise in part to Azima's claims. Through Insight, Forlit used the U.S. financial

[4] Vital is the alter ego of Del Rosso.

system to send multiple wires overseas for the purpose of promoting unlawful criminal activity and, on information and belief, these wires passed through New York. There is a substantial nexus between Insight's purposeful availment of the New York forum and Azima's claims. The ends of justice require application of the nationwide service provisions of 18 U.S.C. § 1965(b) because there is no district in which all of the RICO Defendants could otherwise be tried together.

34. Exercise of jurisdiction over Defendant SDC-Gadot is proper pursuant to 18 U.S.C. § 1965(a) because SDC-Gadot lists its principal place of business as New York. In addition, Defendant SDC-Gadot is a Florida company owned and controlled by Forlit. The exercise of jurisdiction over this defendant is proper in this District pursuant to 18 U.S.C. § 1965(b), and the ends of justice require application of the nationwide service provisions of 18 U.S.C. § 1965(b) because there is no district in which all of the RICO Defendants could otherwise be tried together. SDC-Gadot also transacted business and engaged in conduct in the United States and New York that give rise in part to Azima's claims. Through SDC-Gadot, Forlit used the U.S. financial system to send multiple wires overseas for the purpose of promoting unlawful criminal activity and, on information and belief, these wires passed through New York.

35. Exercise of jurisdiction over Defendant Gerrard is proper pursuant to 18 U.S.C. § 1965(b). Gerrard transacted business and engaged in conduct in the United States and New York which gives rise in part to Plaintiffs' claims. Through his regular business activities in New York while a partner at Dechert, Gerrard directed all aspects of the Enterprise's scheme to defraud and harm Azima, and to oversee the cover up of the Enterprise's illegal and actionable activities. Among other things, Gerrard (i) repeatedly met with Handjani, Frank, Del Rosso, and other Dechert lawyers in New York to cause the filing of false statements in U.S. and UK courts and to U.S. law enforcement agencies in service of the Enterprise's goal of inflicting reputation harm and

litigation costs on Azima; and (ii) met with Buchanan, Page, and others in New York and in Houston to encourage law enforcement reliance on false statements in the pursuit of meritless criminal investigations against Azima. Gerrard also caused payments to be made to Del Rosso in the United States for hacking and other illegal conduct. For the same reasons, Gerrard has engaged in intentional, wrongful, illegal, and/or acts the effects of which Gerrard knew and intended would be felt in the United States and New York. And, as set forth more fully herein, at Gerrard's direction, the RICO Conspirators have engaged in intentional, wrongful, illegal, and/or acts in the United States and New York. The activities of Gerrard's co-conspirators and agents benefited Gerrard, and his co-conspirators and agents were working at the direction, under the control, at the request, and/or on behalf of Gerrard in committing those acts.

36. Exercise of jurisdiction over Defendant Hughes is proper pursuant to 18 U.S.C. § 1965(b). Hughes has transacted business and engaged in conduct in the United States and New York which gives rise in part to Plaintiffs' claims. As detailed further below, Defendant Hughes engaged in conduct in the United States and directed toward the United States related to the scheme and directed at the United States proceedings. For the same reasons, Hughes has engaged in intentional, wrongful, illegal, and/or acts the effects of which Hughes knew and intended would be felt in the United States and New York. Also, as set forth more fully herein, Hughes' co-conspirators and agents have engaged in intentional, wrongful, illegal, and/or acts in the United States and New York. Hughes was aware of the effects in the United States and New York of those acts. The activities of Hughes' co-conspirators and agents were to the benefit of Hughes and the Enterprise, and his co-conspirators and agents were working at the direction, under the control, at the request, and/or on behalf of Hughes in committing those acts.

37. Exercise of jurisdiction over Defendant Forlit is proper pursuant to 18 U.S.C. § 1965(b) because Forlit transacted business and engaged in conduct in the United States and New York that give rise in part to Azima's claims. Among other things, Forlit participated in meetings in New York with the RICO Conspirators in which they discussed and planned the use of the hacked data and deploying false statements in U.S. and UK courts and to U.S. law enforcement agencies in service of the Enterprise's goal of inflicting reputation harm and litigation costs on Azima. Forlit, through his U.S.-based companies Insight and SDC-Gadot, used the U.S. financial system to send and receive multiple wires overseas and within the U.S. for the purpose of promoting unlawful criminal activity, including wires that passed through New York. Also, as set forth more fully herein, Forlit's co-conspirators have engaged in intentional, wrongful, illegal, and/or acts in the United States and New York. Forlit was aware of the effects in the United States and New York of those acts.

FACTUAL ALLEGATIONS

I. THE INITIAL CRIME: UNLAWFUL DETENTION AND INTERROGATION OF AL SADEQ

A. Dechert and Gerrard Unlawfully Detain and Interrogate Al Sadeq

38. In 2014, Gerrard and Dechert were hired to represent RAK to investigate allegations that its former CEO, Khater Massaad, had defrauded RAK. The matter presented an extremely important – and potentially lucrative – opportunity for Gerrard and the firm to generate substantial fees.

39. Gerrard quickly sought to expand Dechert's work for their new client. Under Gerrard's direction, Dechert embarked on a wide-scale global "investigation," which targeted several perceived enemies of its new client. One such target was Al Sadeq.

40. In 2020, Al Sadeq filed suit against Dechert, Gerrard, Hughes, and Dechert partner Caroline Black in the UK, detailing and seeking redress for his detention and abuse. According to Al Sadeq, after being illegally extradited to RAK, he was detained in inhumane conditions and subjected to coerced interrogations by Gerrard, Hughes, and others. Al Sadeq alleges that he was blindfolded with his hands tied behind his back while being interrogated by Gerrard, and that during the interrogations, Gerrard pressured Al Sadeq to pay Dechert's legal fees owed to the firm by RAK. He further alleges that Black also conducted an illegal search of Al Sadeq's home and threatened his wife and children. Al Sadeq, however, repeatedly refused to comply with his captors.

B. Azima and Others Attempt to Expose the Enterprise's Human Rights Violations

41. In the fall of 2014, Azima learned of the unlawful detention and interrogations of Al Sadeq, and Dechert's involvement in the abuse and mistreatment of Al Sadeq and others believed to be enemies of RAK.

42. Azima, Massaad, and others sought to end the mistreatment of Al Sadeq and secure his release by investigating and publicizing the conduct of Gerrard and others. Media outlets and humanitarian organizations were provided details of the abuse and began to investigate.

43. These efforts put Azima and others directly in the Enterprise's crosshairs once high-level members of the Enterprise learned of their efforts. Members of the Enterprise warned Al Sadeq's wife not to speak with journalist Simon Goodley from The Guardian regarding the matter. Simultaneously, the Enterprise put into motion a detailed and documented plan to hack and steal Azima's confidential information and data, then release the data to tarnish his personal and professional reputation and induce him into costly and damaging litigation.

II. THE ATTACK ON AZIMA: HACKING, THEFT, AND FRAUDULENT LITIGATION

44. In an attempt to prevent Azima and others from exposing their human rights abuses, Gerrard and the Enterprise developed a plan to retaliate against and intimidate him. The plan initially involved hiring hackers to unlawfully access and steal Azima's confidential and highly sensitive documents, data, and other information, publishing the hacked data to discredit Azima, and then using that hacked data to embroil Azima in litigation. Although Azima originally sought redress for this misconduct in U.S. courts, the litigation was eventually transferred to the UK by virtue of a forum selection clause in a settlement agreement that the Enterprise had deployed as a trap to force Azima to defend the litigation overseas. As a result, litigation over the hacking remains pending in UK court.

A. The Enterprise Hacks Azima, His Associates, and Other Perceived Enemies of RAK

45. A key component of the Enterprise's strategy against Azima involved a coordinated and concealed effort to hack him and steal his confidential and highly sensitive information. In April 2015, Gerrard, Buchanan, Handjani, Frank, and others had discussions via email and over the phone regarding how to "target" Azima, through a "coordinate[d] . . . attack" that would involve bringing civil or criminal lawsuits against Azima. While at least one member of the Enterprise recognized there was no basis for such litigation, the Enterprise did in fact seek to bring civil and criminal charges against Azima based upon hacked material.

46. Starting in 2015, Azima and his associates began to receive what were later determined to be "phishing" emails designed to gain unlawful access to their email accounts and computers. According to an analysis conducted by Reuters, hackers targeted more than a dozen email accounts owned or operated by Azima and his associates with a coordinated phishing campaign conducted between April 2015 and August 2016.

47. This hacking campaign was directed and paid for by the Enterprise, which employed multiple hackers. Del Rosso and his company, Vital, were retained and instructed by Dechert, and were paid by Dechert until at least 2019. Upon information and belief, Del Rosso received these funds through bank accounts in the U.S.

48. Del Rosso, in turn, hired Jain and his company, Cyber Defense, to hack Azima and other targets identified by Del Rosso. Del Rosso also hired CyberRoot to hack Azima, and Del Rosso, through Vital, paid CyberRoot more than $1 million. Buchanan's company Gravitas International also paid CyberRoot nearly $450,000 at the direction of Del Rosso.

49. The Enterprise also hired Forlit to hack and to prepare reports about the victims using the hacked data. Forlit, in turn, paid other individuals and entities who assisted in the hacking and analysis.

50. Through its illegal hacking operations, the Enterprise unlawfully obtained real-time access to Azima's computers and email accounts without his knowledge. For example, one of Azima's email accounts was accessed without his knowledge in October 2015. The two IP addresses that accessed Azima's accounts were traced back to computers located in Florida and New York, respectively.

51. Between March 2015 and May 2020, members of the Enterprise prepared regular reports ("Hacking Reports") detailing the substance of the information they had unlawfully obtained. Some of those reports included hacked data from Azima and outlined strategies for using the hacked data to attack him. Page worked closely with Gerrard and Buchanan to oversee the Enterprise's hacking operation and preparation of these Hacking Reports, which the Enterprise referred to as "Project Beech" and "Project Beach."

52. The Hacking Reports contained information that, on its face, was plainly confidential and clearly belonged to Azima, including excerpts of Azima's emails, his financial records, including documents reflecting account numbers and balances for multiple bank accounts belonging to or associated with him, and screen shots of his passports. Additionally, some Hacking Reports, including those dated January 2016 and February 2016, contained excerpts of privileged correspondence between Azima and his attorney. Buchanan received the Hacking Reports from Page immediately after they were written, and Gerrard sometimes read the reports in the presence of Buchanan. Gerrard has acknowledged that he read approximately twenty-four reports.

53. The Enterprise employed covert means to distribute these Hacking Reports to other members of the Enterprise. For example, Page and Forlit created a single email account to which they both had access. Forlit would prepare a draft email that attached a hacking report and leave that draft in the draft folder. Page would then access the draft folder of that email account, download the report, and then delete the draft message and the attached report. Members of the Enterprise also regularly used covert messaging applications, such as Confide, Threema, Silent Circle, Signal, and Telegram to communicate, and set the applications to automatically delete messages shortly after reading in order to avoid a record of their communications. After March 2020, the Enterprise transmitted Hacking Reports through these messaging applications. The Hacking Reports were also couriered to Gerrard at Dechert's London office and at Gerrard's home in the UK.

54. The Enterprise used the Hacking Reports to plan future attacks on Azima and others. Gerrard assembled a team, including Buchanan, Arusy, Page, and Forlit, to meet regularly and discuss strategy and tactics. During these meetings, Gerrard, Buchanan, and Arusy provided feedback to Page and Forlit regarding the contents of the reports and next steps in the investigation

of Azima. Forlit met with Gerrard at least a dozen times between 2015 and 2020, including at Dechert's offices in New York. Gerrard, Handjani, Buchanan, Frank, Del Rosso, and others also met regularly during this time period, including at Dechert's offices in New York, to plan strategy for the attacks against Azima.

55. The Enterprise spent millions of dollars on its hacking campaign. From March 2015 through May 2020, Page was paid approximately $300,000 per month for his role in the Enterprise, and he sometimes was paid additional amounts for extra work or expenditures. In order to conceal the illegal nature of the work, Page issued falsified invoices that appeared to be for legitimate services. For example, falsified invoices dated between November 2019 and June 2020 claim to be for a "feasibility study to identify market potential to provide management services in the African subcontinent" even though Page did not conduct any such feasibility study. The invoices were falsified to avoid producing the invoices in litigation.

56. Page, in turn, paid Forlit approximately $250,000 each month between October 2017 and May 2020. Page made these payments in U.S. dollars sent from outside the U.S. to U.S.-based bank accounts at JP Morgan Chase, Citibank, and Bank of America belonging to Forlit's Florida-based companies, Insight and SDC-Gadot. *See* Exhibit A (summary of money laundering transactions).

57. Forlit used the funds Page transferred to him on behalf of the Enterprise to make payments to other hackers who were, upon information and belief, employed by the Enterprise. For example, in March 2018, Forlit's company, SDC-Gadot, sent $55,000 to Aviram Hawk Consultant. In April 2018, Forlit's other company, Insight, sent an additional $32,000 to Aviram Hawk Consultant. Aviram Hawk Consultant is a company owned by or associated with Aviram Azari. In 2022, Azari pleaded guilty in federal court in New York to an indictment charging him

with conspiracy to commit computer hacking, conspiracy to commit wire fraud, wire fraud, and aggravated identity theft based on allegations that he successfully gained access to private email accounts through the use of phishing emails.[5]

58. Forlit also caused Insight and SDC-Gadot to send payments to Dinka Analysis Services, a company owned by Rafi Pridan, for Pridan's role in introducing Forlit to Page. Pridan has twice been charged in Israel in connection with illegal wiretapping. Other "analysts" paid by Forlit, through Insight and SDC-Gadot, included BMI Analysis Limited, Insight GSIA, Global Impact Services, and Fusion GPS.

B. The Enterprise Creates Its 2016 Action Plan to Harm Azima and Others

59. The Enterprise's scheme to attack Azima and cause him to incur significant financial damages was reflected in writing. The plan, which was drafted at least in part by Frank and KARV (for whom Handjani serves as a senior advisor) with direction from Gerrard and others, described a multi-prong approach by the Enterprise to attack and damage Azima, including civil litigation, criminal investigations, and planting stories with media. One of the objectives of the Enterprise's scheme to defraud was to cause economic damages to Azima and his businesses.

60. In December 2015, Frank, Gerrard, and others, including upon information and belief Handjani, met in New York to discuss this plan. In early January 2016, Frank provided an informal outline of the plan, which was prepared based on documents obtained through the Enterprise's hacking and intelligence-gathering operation described above. The outline, titled "View from the Window," summarized a strategy for attacking and harming those who had sought to expose the Enterprise's criminal conduct, with a particular focus on Azima. In the document,

[5] *See* Indictment ¶ 3f, *United States v. Azari*, No. 19-cr-610 (S.D.N.Y. Sept. 30, 2019), ECF No. 7.

Frank solicited additional information from Gerrard that Frank could use to develop the outline to attack Azima and others further.

61. On or about January 26, 2016, the Enterprise prepared a "comprehensive action plan" (the "Action Plan") stating that the Enterprise's scheme was about to enter "a new and decisive phase in that a wide-scale legal action is about to commence in multiple jurisdictions" against Azima and others. The Action Plan was created shortly after Frank's email to Gerrard describing the "View from the Window" and includes overlapping content, indicating that Frank and KARV were also responsible for drafting the Action Plan in conjunction with Gerrard. This was later confirmed by Gerrard, who testified in a UK court that Gerrard hired Frank to create "a global strategic plan." The ten-page Action Plan identified steps the Enterprise would take to damage Azima's "reputation and even [ex]pose him [to] criminal exposure," including "an online campaign against U.S. individuals." An important step outlined in the Action Plan was "the publishing of selected materials" and the use of "blogs in order to harm his reputation." The object of the scheme was to defraud Azima of money and property by harming his businesses and bankrupting him.

C. The Enterprise Induces Azima to Enter into a Fraudulent Settlement Agreement

62. Consistent with the Action Plan, after the Enterprise obtained Azima's stolen data in or around August 2015, the Enterprise sought to develop a basis to "target" Azima with civil and criminal litigation. Using a stale commercial dispute between Azima and RAK, the Enterprise, acting through Dechert, induced Azima to enter into a written settlement agreement ("the 2016 Settlement Agreement") with RAK, which imposed on Azima (1) a duty of "good faith" towards RAK and (2) an English jurisdiction and choice of law clause, even though neither party was located in England. The English jurisdiction benefited the Enterprise since the lawsuit against

Azima was filed and managed by Dechert, Gerrard, Hughes, and others. Azima was reluctant to sign the 2016 Settlement Agreement, but eventually did so at the urging of Handjani and Buchanan, who were acting on behalf of the Enterprise.

63. The 2016 Settlement Agreement was a trap. While it provided Azima a $2.6 million payment, it imposed on him obligations that the Enterprise already intended to exploit in future litigation. At the time Dechert was purportedly negotiating in good faith with Azima, it had access to his confidential documents and emails, including communications between Azima and his attorney discussing the proposed 2016 Settlement Agreement. Upon information and belief, after inducing Azima to assume a duty of "good faith" towards RAK, Dechert intended to sue Azima on behalf of their client, arguing that he violated his duty of good faith based on the documents and communications the Enterprise had already unlawfully obtained through its hacking activities.

64. Indeed, in a letter to the Ruler of RAK, Buchanan described the good-faith clause as "the key clause in this agreement" given the Enterprise's "wider objectives." Upon information and belief, those "wider objectives" included harming Azima to neutralize him and cause him injury for attempting to bring the human rights abuses of Dechert and RAK to light. Dechert also included the forum-selection provision to enable it to sue Azima on behalf of RAK in England, a highly inconvenient and expensive forum given his residence in Kansas City, Missouri.

D. The Enterprise Launders Azima's Stolen Data on the Internet

65. On or about July 16, 2016, after the 2016 Settlement Agreement had been signed, Azima met with Buchanan, Gerrard, and another Dechert lawyer. During this meeting, Gerrard threatened to make Azima "collateral damage" in the Enterprise's attacks against Massaad.

66. To make use of the confidential documents and information of Azima it had obtained through its hacking operations, the Enterprise needed a plausible and innocent

explanation for how it came into possession of the materials. Accordingly, it devised a complicated plan to launder the materials by publishing them on the internet.

67. Within weeks of the July 2016 meeting in which Gerrard threatened Azima, anonymous blog sites appeared on the internet which included content disparaging Azima. These blog sites also contained links through which some of Azima's stolen data could be downloaded from the internet. On or around August 4, 2016, approximately 27.75 GB of Azima's materials appeared on the internet sites. Additional data appeared on or around August 30, 2016 and September 8, 2016. In total, the blogs included links to more than 30 GB of data unlawfully obtained from ten email accounts belonging to Azima and one of his associates. The stolen data comprised approximately 161,702 emails, 13,736 photographs or other images, and 840 voice recordings. It also included Azima's calendar appointments, call history, SMS messages, Viber messages, WhatsApp messages, videos, voicemails, contacts, and notes. Additionally, the data included important business records, privileged and confidential communications, financial documents, information, and trade secrets for Azima's businesses, including ALG.

68. Members of the Enterprise then created a false exculpatory data trail intended to show they had innocently found the data on the internet in August 2016. On August 16, 2016, for example, Buchanan wrote to Frank and Handjani and falsely stated that he was informed by Page "last night that there is an internet site that is carrying a huge amount of material relating to FA." Similarly, Gerrard sent an email via Dechert's servers deceptively asking Del Rosso to search for the website that he knew that the Enterprise itself was responsible for creating, and which held data he had been repeatedly reviewing through regular Hacking Reports. In addition, Gerrard had emailed Del Rosso a week before (on August 9) about links containing the hacked data, proving that the emails on August 15 and 16 were a ruse.

E. The Enterprise Brings Civil Litigation Against Azima

69. Once the data was made available on the internet, the Enterprise executed the next step of the plan, in which the Enterprise would deploy the hacked materials against Azima, as outlined in the Enterprise's January 2016 Action Plan. On September 23, 2016, Hughes sent a letter via U.S. mail and wire to Azima's U.S. counsel claiming that Azima had breached the 2016 Settlement Agreement. Hughes's letter threatened to sue Azima on behalf of RAK unless Azima paid $4.2 million within seven days. Days later, as contemplated by the Action Plan, the Enterprise brought suit against Azima in the English High Court on behalf of RAKIA for breach of the 2016 Settlement Agreement (the "UK Proceeding").[6]

70. To support its claim of breach, Dechert's letter attached excerpts from Azima's hacked documents and data, which had been printed from Dechert's servers by a Dechert secretary. Although the Enterprise was responsible for stealing the information from Azima and placing it on the internet, Hughes's letter claimed that Dechert had innocently found the documents on "publicly available" websites.

71. Those claims, which were false, were intended to defraud Azima and extort him into paying millions of dollars to RAK. The Enterprise itself had placed Azima's documents and data on the internet after hacking his accounts and stealing it from him. Initially, the links to all 30 GB of Azima's stolen material were inaccessible to all but Dechert and the RICO Conspirators. After Azima's counsel noted this fact, the Enterprise published WeTransfer links on the blog sites

[6] The UK Proceeding remains ongoing. In 2020, RAKIA secured a favorable trial decision in the UK against Azima, but it was recently vacated and remanded for a new trial regarding whether RAKIA, Dechert, Gerrard, and Buchanan were responsible for the hacking of Azima. RAKIA has since withdrawn its defense and offered to settle Azima's claim, acknowledging that its officers "may have been the victims of dishonest and unscrupulous former third-party advisors" – i.e. Gerrard and Dechert – "who have taken steps to advance their own interests for their own gains."

three different times – as recently as June 2019 – containing Azima's hacked data. These new links made Azima's previously unavailable data available to anyone, not just Dechert and the RICO Conspirators. Upon information and belief, the updated links were created by the Enterprise in order to conceal the fact that the Enterprise was responsible for the hacking.

72. The same day that Dechert filed suit in the UK against Azima for the alleged breach of contract, Azima sued RAKIA in the U.S. for hacking him and stealing his data. This suit was based in part upon the fact that Dechert's letter enclosed Azima's stolen data.

III. THE COVER-UP: OBSTRUCTION OF JUSTICE, A PROTRACTED SMEAR CAMPAIGN, AND A FABRICATED CRIMINAL INVESTIGATION

73. As alleged above, the Enterprise and its members committed serious crimes against Al Sadeq and Azima. Much of this initial criminal activity by the Enterprise, including the detention and abuse of Al Sadeq and its early efforts to attack Azima, is the subject of ongoing litigation in the UK.

74. But the Enterprise's criminal conduct did not stop there. As detailed below, the Enterprise continues to this day to engage in an extensive and prolonged effort to cover up its crimes. Over at least the past four years, the Enterprise has continued its attacks on Azima and others, as initially outlined in its Action Plan, in an effort to silence him and to harm and bankrupt Azima and his businesses. Among other things, once the Enterprise placed Azima's stolen data on the internet, the Enterprise used the data to lobby law enforcement to investigate Azima and sought to induce media outlets to write false and damaging stories about Azima in an attempt to harm him and his businesses.

75. Then, as Azima came closer to uncovering the truth about the hacking through litigation in the U.S. and UK, the Enterprise repeatedly sought to obstruct justice – including in

multiple proceedings brought in U.S. courts – to avoid detection and to obtain a multi-million-dollar judgment against Azima.

A. The Enterprise Seeks to Influence U.S. Law Enforcement in an Effort to Manufacture a Criminal Investigation of Azima and Others

76. As alleged above, the Enterprise's Action Plan to ruin Azima financially included using the data it hacked and stole from him to manipulate U.S. law enforcement agencies into launching a criminal investigation of him. From 2016 through at least 2019, the Enterprise, through Dechert and others, provided U.S. federal law enforcement agencies with a selection of documents stolen from Azima through hacking and an extensive dossier prepared by Dechert lawyers. Upon information and belief, the RICO Conspirators did not disclose to U.S. law enforcement that they had obtained Azima's data illegally.

77. As part of this scheme, the Enterprise sought to arrange multiple meetings with U.S. law enforcement authorities. For example, in February 2019, Page and others met in New York to plan for an upcoming meeting that was scheduled with agents from the Federal Bureau of Investigation ("FBI"). That meeting was ultimately canceled and rescheduled for March 2019.

78. In March 2019, Page, Gerrard, Buchanan, and attorney Chris Swecker, a former FBI agent who worked closely with Del Rosso and claimed to have significant personal contacts with the FBI, met with FBI agent Paul Zukas at a hotel in Houston, Texas. During the meeting, Zukas interviewed Page about Azima.

79. The Enterprise initially succeeded in instigating an FBI investigation of Azima that closely tracked the allegations raised by RAK in its demand letter and subsequent UK litigation against Azima. Azima, who fully cooperated, was forced to incur significant legal and professional fees responding to document requests and subpoenas. The investigation was subsequently terminated.

B. The Enterprise Launches a Media Campaign to Harm Azima

80. The Action Plan also called for the Enterprise to "contact several world leading reporters and investigative journalists and supply them with materials and evidence" about Azima "in order to be published." To implement this aspect of the plan, the Enterprise planted false and disparaging stories in the press alleging that Azima had defrauded RAK and violated international sanctions laws. The Enterprise also used false information and stolen data to influence other stories in the media regarding Azima and others.[7] Upon information and belief, the Enterprise did not reveal that they had stolen the information that they provided to reporters, nor did it reveal to the media that some of their information was produced through coerced interrogations of Al Sadeq in violation of international law.

81. For example, AP journalists John Gambrell, Jack Gillum, and Jeff Horwitz published a June 2017 article citing hacked documents that denigrated Azima. In May 2018, Zach Dorfman with Politico cited Azima's hacked emails in another article that negatively portrayed Azima. Some journalists such as Gambrell, Horwitz, and Dorfman not only cited Azima's hacked documents in their negative coverage, but were also were "anonymously" sent new hacked

---

[7] *See, e.g.*, Ellen Milligan, *UAE Wealth Fund Wins Fraud Suit Against Aviation Executive*, Bloomberg Law (May 22, 2020, 12:53 PM) https://www.bloomberglaw.com/product/blaw/document/QAQS4HDWX2QH?criteria_id=6332b7a3203c0c78ad56c7836f39245a&searchGuid=d44a63d0-2de5-464e-a23f-6fdbd9ad49a7; Krishnan Nair, *Dechert Partner in Mining Company Dispute is Now Accused of Conspiring Against Tycoon*, LAW.COM (Aug. 20, 2019, 4:18 AM), https://www.law.com/international-edition/2019/08/20/dechert-partner-in-enrc-dispute-is-now-accused-of-conspiring-against-tycoon/; Zach Dorfman, *The Mysterious Tale of a Powerful American Businessman, Three Sanctioned Iranians and an Imprisonment in Tehran*, POLITICO (May 27, 2018), https://www.politico.com/magazine/story/2018/05/27/the-mysterious-tale-of-a-powerful-american-businessman-an-emirati-sheikhdom-three-sanctioned-iranians-and-an-imprisonment-in-tehran-218405/; Paul Peachey, *Aircraft magnate accused of 'secret plot' to smear RAK ruler*, THE NATIONAL NEWS (July 19, 2018); https://www.thenationalnews.com/world/europe/aircraft-magnate-accused-of-secret-plot-to-smear-rak-ruler-1.751760; Jon Gambrell, Jack Gillum, and Jeff Horwitz, *'Worth killing over': How a plane mogul dodged US scrutiny*, AP NEWS (June 21, 2017); https://apnews.com/article/iran-mo-state-wire-ks-state-wire-middle-east-international-news-4a4b6e9dfc0949e698ee0ada284414ed.

documents by Gerrard in April 2019 to generate more negative press. *See* ¶¶ 120-126. As alleged in further detail below, the Enterprise's successful efforts to plant false and disparaging stories such as these about Azima in the press caused extensive damage to his reputation and business interests.

82. In addition, in June 2019, the Enterprise published Azima's stolen data on WeTransfer links on the internet, which triggered additional negative media coverage directly harming Azima and his businesses.

C. Obstruction of Azima's D.C. District Court Proceeding

83. As alleged above, in September 2016, Azima filed his own suit against RAKIA in the United States District Court for the District of Columbia, seeking compensation for the hacking of his accounts and theft of his emails, documents, and other information (the "D.C. District Court Proceeding"). The D.C. District Court Proceeding remained pending until 2020, when the D.C. court transferred it to the UK based on the forum selection clause contained in the 2016 Settlement Agreement that the Enterprise had fraudulently induced Azima to sign.

84. The D.C. District Court Proceeding threatened to expose the Enterprise's misconduct, and members of the Enterprise repeatedly sought to avoid detection through obstruction of justice. In March 2018, the D.C. Court denied RAKIA's motion to dismiss, filed by Dechert, paving the way for discovery to commence regarding the Enterprise's hacking. At that point, the UK Proceeding did not yet include any claims relating to hacking, which meant that the D.C. District Court Proceeding was the only legal proceeding then ongoing that posed a threat to expose the Enterprise's hacking operations.

85. Throughout the pendency of the D.C. District Court Proceeding, from 2016 up to and including 2020, the Enterprise repeatedly fabricated and destroyed evidence in order to obstruct the case by concealing their involvement in the hacking of Azima's accounts and the theft

of his data and information. The first evidence of this obstruction did not begin to come to light until approximately April 2019. Since then, additional evidence of the Enterprise's obstruction has continued to emerge, including as recently as April 2022.

86. Additionally, between February 2020 and June 2022, Azima obtained confessions from certain members of the Enterprise, including individuals who hacked on behalf of the Enterprise. In June 2022, Azima also obtained copies of a number of the Hacking Reports, discussed above, which for the first time revealed that many of the statements that the Enterprise made to the court and in affidavits and filings in connection with the D.C. District Court Proceeding were false, misleading, and/or deceptive. Upon information and belief, because the D.C. District Court Proceeding remained pending until July 2020, all steps by the RICO Conspirators until then to cover up their involvement in the hacking were taken, at least in part, to obstruct those proceedings.

1. The Enterprise Makes False Statements in the D.C. District Court Proceeding and Develops False Testimony to Conceal Its Role in the Hacking of Azima

87. RAK's defense to the D.C. District Court Proceeding relied on two factual assertions: (1) the venue provision of the 2016 Settlement Agreement was valid and enforceable and had been obtained through a good-faith negotiation, and (2) the Enterprise had no involvement with the hacking of Azima, and Dechert had found the stolen documents through publicly available internet sources. Both of these foundational pillars were false, and the Enterprise members involved in the D.C. District Court Proceeding knew they were false. Gerrard and Hughes induced other Dechert partners to make statements Gerrard and Hughes knew were false, and that the other Dechert partners knew, or should have known, were false, each of which contributed to the Enterprise realizing its goals in relation to the D.C. litigation.

88. The first lie was successful. In 2019, the U.S. Court of Appeals for the D.C. Circuit held that the case must be transferred to the UK based on the venue provision of the 2016 Settlement Agreement. The D.C. District Court subsequently did so in 2020.

89. The second lie was also successful, at least initially. Due to the Enterprise's obstruction of the D.C. District Court Proceeding, it was able to conceal for many years its hacking of Azima and its role in laundering his documents and other data through the internet. It was able to embroil Azima in costly litigation, as it had described in its Action Plan, and ultimately was able to obtain a judgment against him based on the stolen data and false testimony.

90. Both false narratives were developed and perfected through a series of meetings involving the RICO Conspirators and were repeated in both the D.C. District Court Proceeding and the UK proceeding. Ultimately, the purposes of the false statements were to damage Azima, his associates, and his businesses by obtaining a multi-million judgment against him and to prevent him from recovering in the D.C. District Court Proceeding (and exposing the Enterprise's misconduct) by concealing that misconduct.

91. The Enterprise took numerous obstructive acts to corruptly interfere with the D.C. District Court Proceeding by inducing Dechert partners to make representations the Enterprise knew were false. For example, on October 6, 2016, Dechert's then-general counsel, Arthur Newbold, sent an email to Azima's U.S. counsel, copying Gerrard and Hughes, stating: "Your email suggests that our partner, David Hughes, has done something wrong, and I don't see from what you have said that he has done anything wrong." In a subsequent email to Azima's U.S. counsel, Newbold, speaking on behalf of Dechert and again copying Gerrard and Hughes, stated: "I have been assured that neither Dechert nor our client knows whether your client's computer was

hacked or by whom. I have also been told that Dechert is unaware of any communications between your client and his counsel."

92. Newbold's assurances, presumably obtained from Gerrard, were false and misleading. Gerrard, who was copied on Newbold's emails, knew that the Enterprise had hacked Azima's computer and stolen his confidential information. Gerrard was also aware that the Enterprise had unlawfully obtained privileged communications between Azima and his counsel, which they relied on as part of their scheme to defraud Azima.

93. On October 20, 2016, Dechert Partner Linda Goldstein emailed Azima's U.S. counsel and "reaffirmed the representations previously made" by Hughes and Dechert's General Counsel. Goldstein repeated the false claim that the hacked documents in Dechert's possession were found by the firm through publicly available internet sources. The email from Goldstein falsely stated that: "our client engaged experts to monitor press articles and other information . . . . The monitoring initially disclosed websites of documents from the Panama Papers detailing Mr. Azima's financial arrangements . . . . Standard Google searches also identified numerous websites (such as the ones identified in Mr. Hughes's letter of September 29) from which other documents relating to your client could be and were obtained." As with Newbold's statements, Gerrard knew that the documents had been stolen via hacking by the Enterprise at the time Goldstein made these claims.

94. In a motion to dismiss electronically filed on December 12, 2016 in the D.C. District Court Proceeding and signed by Goldstein, Dechert repeated the false claim that "Azima's documents were publicly available on the internet, which is where RAKIA obtained them."

95. On April 18, 2017, Goldstein stated during a hearing in the D.C. District Court Proceeding that "We, of course, deny that RAK Investment Authority or my law firm [Dechert] had anything whatsoever to do with hacking these documents."

96. On June 13, 2017, in Dechert's second motion to dismiss in the D.C. District Court Proceeding, electronically filed and signed by Goldstein, Dechert again falsely and misleadingly stated that "a consultant engaged by RAKIA identified a trove of Azima's documents that were available for download on the internet." In the motion, Dechert insisted the 2016 Settlement Agreement was obtained through a good-faith negotiation, and not fraud. Specifically, Dechert argued that RAK "would not have paid Azima $2.6 million in March 2016 in reliance on a warranty of good faith" if they had been able to hack Azima's emails prior to the settlement. This statement was false and misleading because the Enterprise had hacked Azima prior to March 2016, was reviewing his communications (including privileged communications about the 2016 Settlement Agreement) in real-time at the time the agreement was executed, and already intended to sue Azima to recoup more than the $2.6 million that he was initially paid out under the 2016 Settlement Agreement.

97. On June 13, 2017, Dechert electronically filed a sworn affidavit from Buchanan in support of RAK's motion to dismiss. In his affidavit, Buchanan falsely claimed that "The allegations in Mr. Azima's Complaint and First Amended Complaint are completely untrue." Buchanan also falsely claimed that "If RAKIA had been able to read and monitor Mr. Azima's communications beginning back in October 2015, as Azima claims in the First Amended Complaint, we . . . would have never paid Mr. Azima $2.6 million in connection with the March 2016 settlement agreement."

98. In July 2018, Azima sought to stay the UK proceeding until the D.C. District Court Proceeding could determine whether RAK hacked Azima. In opposition to that application, both Hughes and Goldstein filed witness statements. Hughes falsely stated that a "public relations company" innocently found Azima's stolen data on the internet, and Goldstein adopted Hughes's account regarding the acquisition of Azima's data.

99. On August 3, 2018, Dechert, Goldstein, Gerrard and Hughes falsely stated in an email to Azima's counsel, sent in connection with the D.C. District Court Proceeding, that no Dechert attorney, employee or agent (including Gerrard), had "been complicit in, or had knowledge of any of" the hacking of Azima.

100. On August 8, 2018, Dechert filed a brief before the U.S. Court of Appeals for the D.C. Circuit falsely and misleadingly asserting that Azima's stolen data was "obtained via publicly available internet sources." In addition, Dechert falsely and misleadingly stated: "It is highly implausible that RAKIA had ten continuous months of unfettered access to Azima's personal computers, as Azima contends." Finally, Dechert falsely and misleadingly stated: "Again, there are no facts showing that anyone – much less RAKIA – accessed Azima's communications in real time, or sent any emails appearing to come from him."

101. From late 2018, while the D.C. District Court Proceeding was pending, the Enterprise went to great efforts to ensure that its members had their stories straight. Beginning in October of that year, Gerrard convened a series of meetings of RICO Conspirators in Cyprus, London, and Switzerland designed to provide key members of the Enterprise with the opportunity to rehearse and perfect false testimony regarding the hacking of Azima and the theft of his confidential information. Throughout this period, the D.C. District Court Proceeding was pending, meaning that all of the Enterprise's efforts to develop false and misleading testimony – including

those relevant to the UK Proceeding – were also intended, in large part, to obstruct the D.C. District Court Proceeding.

102. On or about October 25, 2018, Gerrard, Hughes, Buchanan, Page, Forlit, and Halabi met in Cyprus, where they agreed that Halabi would falsely attest that he had discovered Azima's hacked data on the internet. At the time, the D.C. District Court Proceeding was being actively litigated. Dechert had appealed the district court's order denying RAKIA's motion to dismiss, and Azima had filed a motion to begin discovery, which was pending. Thus, Halabi's false testimony was necessarily intended, at least in part, to obstruct the D.C. District Court Proceeding.

103. On November 6, 2018, Hughes signed another sworn statement in the UK proceeding falsely stating that Page had obtained the links to Azima's stolen data from an unnamed individual who was not an agent of RAK. As alleged above, given the status of the D.C. District Court Proceeding, this false statement was necessarily intended, at least in part, to obstruct those proceedings.

104. On or about November 21, 2018, Gerrard, Hughes, Page, Forlit, and Halabi met again in Cyprus to further develop Halabi's false narrative that he had discovered Azima's hacked data on the internet. Dechert has admitted that Goldstein attended this meeting virtually from New York.

105. On December 11, 2018, Hughes repeated the false narrative in another sworn statement in the UK proceeding, stating that "Mr Page was informed of the existence of the publicly available links to the first cache of data by a freelance journalist and lawyer called Majdi Halabi." As alleged above, given the status of the D.C. District Court Proceeding, and the repeated similar false statements to the federal courts in D.C., this false statement was necessarily intended, at least in part, to obstruct those U.S. proceedings.

106. On May 1, 2019, Halabi met in London with Gerrard, Forlit, and Page to further rehearse his false testimony. Halabi did so again the next day with Gerrard, Buchanan, and Forlit. On May 3, 2019, Halabi met with Gerrard, Hughes, and Forlit at Dechert's office in London to prepare his false witness statement. Halabi then met with other attorneys from Hughes's new law firm, Stewarts Law, and Dechert, including New York partner Goldstein, to help him prepare his witness statement for the UK Proceeding.[8] As alleged above, given the status of the D.C. District Court Proceeding, this false statement was necessarily intended, at least in part, to obstruct those proceedings.

107. On June 24, 2019, Gerrard signed a witness statement that was emailed to Azima's UK counsel recounting the false story that he and RAK did not learn of the existence of Azima's hacked data until August 2016. Gerrard also falsely stated: "I should make it clear at the outset that I was never instructed . . . to hack Farhad Azima's emails or computer. I certainly did not undertake any such hack on my own initiative, nor did I give instructions to any person to hack Farhad Azima's documents. I do not know who hacked Farhad Azima's computers or other devices or when or how the hacking took place." As alleged above, given the status of the D.C. District Court Proceeding, this false statement was necessarily intended, at least in part, to obstruct those proceedings.

108. On October 17, 2019, Dechert Chairman Andrew Levander, sent a letter to the Washington Free Beacon on behalf of RAK and Handjani. The letter denied that RAK had hacked Azima's computers and threatened to sue the newspaper for reporting that allegation.

[8] Hughes left Dechert in June 2017 for Stewarts Law. Dechert continued to represent RAK in the D.C. District Court Proceeding, but after Hughes's departure, Stewarts Law represented RAKIA in the UK Proceeding.

109. In December 2019, Gerrard, Forlit, Page, and Halabi met at the Moosegg hotel outside of Bern, Switzerland, just one month before Gerrard, Buchanan, Page, and Halabi were scheduled to testify in the UK Proceeding. The RICO Conspirators went to great lengths to conceal their activities, including by taking indirect transportation methods and reserving the entire hotel for the RICO Conspirators in order to maintain secrecy. While dining with a private chef and enjoying an extensive selection of fine wines, Gerrard, Page, Forlit, and Halabi engaged in a mock trial, with Gerrard acting as judge and cross-examining counsel in an effort to perfect the narrative and ensure that the testimony at the upcoming UK trial remained consistent.

110. Page, Halabi, Gerrard, and Buchanan subsequently offered their well-refined perjury to the UK court in January 2020. Page and Halabi have since acknowledged through sworn testimony that the story fabricated in Cyprus and rehearsed in Switzerland was false. In a sworn witness statement signed in 2022, and in other discussions, Halabi admitted that the false story was created by Gerrard, Hughes, Buchanan, Forlit, and Page. Halabi also admitted that he was first asked to provide this false story in 2017, when the D.C. District Court Proceeding was the only forum in which Azima's hacking claims were being litigated. RAK has recently sought to distance itself from the meeting in Switzerland, claiming that the meeting was organized by Gerrard without client authorization.

111. The above-described meetings, correspondence, and testimony were part of a broader scheme to conceal the Enterprise's illegal acts and were intended, at least in substantial part, to obstruct the D.C. District Court Proceeding, which was pending throughout the duration of the obstructive conduct. Goldstein, who was then handling the D.C District Court Proceeding, was present at the meetings in November 2018 and May 2019.

112. The RICO Conspirators' false statements, all transmitted over U.S. wires, prevented Azima, the D.C. district court, and the U.S. Court of Appeals for the D.C. Circuit from learning material information central to the pending D.C. District Court Proceeding. They prevented Azima from demonstrating that the 2016 Settlement Agreement (including its UK forum clause) was a fraud, caused the court to transfer his case to the UK based on the Agreement's forum selection clause, and prevented Azim from obtaining a favorable judgment in the D.C. District Court Proceeding against RAKIA. Moreover, as a direct result of the obstruction detailed above, Azima did not learn about the extent of the RICO Conspirators' false statements until years later, starting in 2020, when individuals involved in the hacking began confessing their involvement.

2. The Enterprise Destroys Evidence and Makes False Statements Regarding Evidence Preservation

113. The Enterprise also obstructed the D.C. District Court Proceeding by destroying evidence and documents, and by making false statements to Azima and his counsel regarding their efforts to preserve and retain relevant materials.

114. Throughout the almost four years the D.C. District Court Proceeding was pending, Azima's counsel made at least five requests to Dechert and to the court intended to ensure the preservation of relevant evidence. Dechert, Gerrard, and Hughes, through correspondence from Goldstein and Newbold, made affirmative, but false, assurances that relevant evidence was being preserved, despite knowing that evidence had already been destroyed and/or was in the process of being destroyed.

115. For example, just one week after Azima filed the D.C. District Court Proceeding in September 2016, Buchanan brought his iPhone to an Apple store, where much of his webmail, including mail stored remotely in the "cloud," was allegedly deleted. On October 22, 2016,

Buchanan informed Dechert's Goldstein that his emails and other data had been deleted but that the emails and data could be restored if steps were taken immediately. Goldstein instructed Buchanan to restore *only* emails from August to September 2016, ensuring that earlier emails, which upon information and belief they knew would necessarily include emails related to the hacking of Azima and the Enterprise's preparation of Hacking Reports, would be permanently deleted, destroyed, and unrecoverable. The Enterprise concealed this document destruction until April 2019 through false statements that were relied upon by Azima.

116. Buchanan's laptop also disappeared under mysterious circumstances. Buchanan claimed in a sworn statement that his laptop was stolen in January 2017, just a few months after Azima's D.C. District Court Proceeding was filed. At the time, Dechert had not taken any steps to preserve his laptop or its data. Upon information and belief, Buchanan destroyed the laptop to prevent evidence stored on it from being produced in the D.C. District Court Proceeding. The Enterprise concealed this document destruction until April 2019 through false statements that were relied upon by Azima.

117. In July 2021, Dechert revealed that it had furnished Gerrard with at least fifteen different mobile devices between 2014 and 2020 – a period when Gerrard and others were actively involved in the Enterprise's unlawful activities. Dechert admitted that data and evidence from eight of those devices could not be retrieved and had not been preserved because the devices were "temporarily mislaid," "stolen," "reissued to another member of the firm," "returned to [the] Dechert IT team," or "lost." The Enterprise concealed this document destruction until July 2021 through false statements that were relied upon by Azima. Indeed, throughout his tenure with Dechert, Gerrard consistently and repeatedly replaced his devices – at least twenty-two times since he joined the law firm.

118. Though Dechert was aware as early as 2016 that Buchanan and/or Gerrard had destroyed and/or failed to preserve relevant evidence, it repeatedly provided Azima and his counsel with false and misleading information regarding document retention and preservation in connection with the D.C. District Court Proceeding. Dechert did not disclose that data from Buchanan's laptop or Gerrard's cell phones had been lost or destroyed at any point in the D.C. District Court Proceeding. In fact, Dechert, through Goldstein, and with the knowledge and approval of Gerrard, Hughes, and others, falsely assured Azima's U.S. legal team that all relevant documents had been preserved even though Gerrard, Hughes, and others knew that relevant evidence had already been destroyed.

119. Upon information and belief, Gerrard and Hughes caused Goldstein to make these false statements in order to obstruct discovery in the D.C. District Court Proceeding. Had the truth about the document destruction been known, Azima would have immediately sought judicial intervention.

3. The Enterprise Defrauds the D.C. District Court by Submitting Stolen Documents Laundered Through Lebanon

120. The Enterprise also obstructed the D.C. District Court Proceeding in 2019 through a clumsy effort to inject select emails stolen from Azima into the case by anonymously sending copies of the stolen emails to the district court judge, Dechert, and Azima's U.S. lawyers, as well as members of the media.

121. In or around March 2019, members of the Enterprise identified a hacked email chain from August 12, 2016 that they wanted to file with the court in the D.C. District Court Proceeding. However, the email post-dated the initial publication of Azima's hacked documents on the internet about a week earlier. Accordingly, there was no plausible explanation for how

Dechert had the document in its possession given its claim that it "innocently discovered" Azima's hacked and stolen materials on the internet on or about August 8, 2016.

122. Confronted with this conundrum, Gerrard, Del Rosso, and Grayson hatched a complicated scheme to use a subcontractor in France to travel to Lebanon to anonymously mail printed copies of the August 12, 2016 emails to Dechert's New York office, the D.C. district court, Azima's counsel, and others. This scheme was intended to provide Dechert's U.S. lawyers with a false basis for claiming that it had innocently come into possession of the email chain and allow the firm to use the documents against Azima in the case.

123. The Enterprise thus arranged for printouts of the email chain to be mailed from Lebanon to the presiding district court judge, Azima's counsel, Goldstein, Gerrard, and others. However, the co-conspirator neglected to include a recipient list in each package. When Gerrard received his package without the master recipient list, he grew concerned that it would undermine his ability to pose as an innocent recipient of the stolen document. Accordingly, he instructed Del Rosso and Grayson to repeat the mailing with the recipient list included, which they did. According to the recipient list, the hacked and stolen email was mailed directly to the district court judge presiding over the case by the RICO Conspirators.

124. On April 18, 2019, Goldstein informed Azima's counsel that Dechert had received a copy of Azima's hacked August 2016 emails and intended to use the document in the D.C. District Court Proceeding.

125. As alleged above, the Enterprise went to great lengths to obstruct the D.C. District Court Proceeding between 2016 and 2020, including lying to Azima's counsel and the district court on multiple topics; destroying evidence and then lying to Azima's counsel and the district court about document preservation; concocting false testimony designed to mask the Enterprise's

complicity in the merits of the suit, the hacking of Azima and the theft of his data; hiding the fact that the 2016 Settlement Agreement was procured through fraud; and submitting stolen documents to the D.C. district court under false pretenses.

126. Through its obstructive conduct, Dechert and RAK successfully avoided U.S. discovery that threatened to unravel the Enterprise's conspiracy and reveal its role in the hacking of Azima. The case was transferred to the UK based on the forum selection clause in the fraudulent 2016 Settlement Agreement, and the matter has been pending ever since.

D. The Enterprise Obstructs Multiple Proceeding in the U.S. Under 28 U.S.C. § 1782 Related to Azima's UK Case

127. Even after the Enterprise succeeded in avoiding discovery in the D.C. District Court Proceeding, the threat remained that discovery in the U.S. would reveal the Enterprise's criminal conduct. After Azima's claims in the D.C. District Court Proceeding were transferred to the UK, he re-asserted them as counterclaims in the pending UK Proceeding brought by RAKIA against Azima for breach of contract. In addition, in 2020, Al Sadeq filed suit against Dechert, Gerrard, Hughes, and Caroline Black in the UK asserting claims based on his mistreatment at the hands of the Enterprise. Azima and Al Sadeq subsequently filed proceedings in New York, North Carolina, and Florida under 28 U.S.C. § 1782 ("Section 1782") in which they sought the aid of U.S. federal courts to obtain evidence for use in their respective UK cases.

128. The Enterprise thus faced a similar problem – specifically, that discovery obtained in these Section 1782 proceedings would lead to exposure of the Enterprise's past crimes, including its abuse of Al Sadeq and its hacking, intimidation, and harassment of Azima. Accordingly, the Enterprise developed and implemented a corrupt plan to obstruct and disrupt these Section 1782 proceedings as well.

1. Handjani Obstructs Azima's Section 1782 Proceeding in New York

129. On June 29, 2021, Azima filed a Section 1782 application in the U.S. District Court for the Southern District of New York (the "New York § 1782 Proceeding") seeking discovery from Handjani relevant to Azima's pending retrial of his claims in the UK Proceeding. In his opposition to Azima's application, which was filed with the court, Handjani stated that he had "attested in his witness statement [in the UK Proceeding] that he had no knowledge of or involvement in any hacking of Azima and did not become aware of Azima's hacking until August 16, 2016." In the same filing, Handjani also stated that he had affirmed at trial "under oath and with a penalty of perjury, I had no knowledge of Azima's material being hacked, who hacked it, or of it appearing online." In addition, Handjani asserted that he served solely as a "channel of communication" between Azima and RAK and "was only intermittently involved in the parties' settlement discussions."

130. These statements were false and misleading, and they have been directly contradicted by confessions from three of Handjani's co-conspirators and the Hacking Reports discussed above. In December 2021, Azima learned that Handjani had attended regular meetings every four to six weeks with Gerrard, Frank, and Buchanan to discuss and implement the plan to attack and harm Azima. Upon information and belief, these meetings included discussions regarding hacking victims, including Azima.

131. In addition, upon information and belief, Handjani was also involved in the preparation of the Action Plan and reviewed at least some of the Hacking Reports. And, as alleged in more detail below, Handjani was directly involved in instructing Page to work with hackers, including Forlit, to investigate who was funding the litigation brought by Azima and Al Sadeq.

132. Taken together, these facts demonstrate significant involvement by Handjani in the Enterprise's hacking operations, including its hacking of Azima. They make clear that Handjani's

statements in the New York § 1782 Proceeding were materially false, misleading, and corruptly made with an intent to obstruct that matter and to thereby prevent discovery of facts that would have exposed the Enterprise's criminal activity.

2. Forlit Obstructs Azima's Section 1782 Proceeding in Florida

133. On March 8, 2022, Azima filed another application under Section 1782 in the U.S. District Court for the Southern District of Florida (the "Florida § 1782 Proceeding") seeking discovery from Forlit, Insight, and SDC-Gadot relevant to Azima's claims in the UK Proceeding. Forlit subsequently opposed the application. In support of his opposition, Forlit filed two affidavits with the court that contained materially false and misleading statements that were intended to obstruct the proceeding. Upon information and belief, Forlit made these false statements to the court in order to avoid U.S. discovery that threatened to reveal the Enterprise's prior criminal conduct.

134. On March 16, 2022, Forlit filed an affidavit with the court falsely asserting that he and SDC-Gadot had "not conducted business in the state of Florida" and that SDC-Gadot "has not conducted any business in years." Forlit's affidavit was submitted in order to conceal his company's role in laundering payments for the Enterprise's hacking of Azima.

135. However, bank records for SDC-Gadot, which were obtained from Citibank through another Section 1782 proceeding, prove that Forlit's affidavit was false. Those bank records show that SDC-Gadot received millions of dollars in revenue between 2017 and 2021 from transactions with other Florida companies. In addition, in 2017, Forlit represented to Citibank that he expected approximately $5 million in revenue over a 12-month period for "services." Two of the three customers he listed as "major customers" were Page Group, which is owned by Page, and Global Impact, which is owned by Arusy. Forlit also represented that he expected to receive approximately $250,000 per month from the United Arab Emirates, the United Kingdom, and/or

Hong Kong for "services," and that he intended to wire approximately $100,000 per month to Israel for "IT analysis services." The company address listed for SDC-Gadot on the documents provided to Citibank was in Florida.

136. SDC-Gadot's bank records, together with the account-opening documents that Forlit submitted to Citibank, thus make clear that his statements in this first affidavit regarding SDC-Gadot's business operations were false, misleading, and made with an intent to obstruct the matter and to thereby prevent discovery of facts that would have exposed the Enterprise's criminal activity.

137. On June 1, 2022, Forlit filed a second affidavit that falsely stated that: (1) he "was not a hacker" and hacking was "not something that I ever performed" and (2) he "show[ed] Stuart Page the existence of online links that were available to anyone with internet access." Like his first affidavit, Forlit's second affidavit was submitted in an attempt to conceal his company's role in hacking and in laundering hacking payments for the Enterprise.

138. Forlit was deposed in July 2022 and repeated his false statements that he was not a hacker and did not hack Azima (though he admitted to many other key facts, including that he prepared regular reports and was paid $250,000 per month by Page).

139. As alleged above, however, Forlit was in fact directly involved in the preparation of monthly Hacking Reports on Azima and his associates. *See supra* ¶¶ 45-61. These reports contained information and excerpts that clearly came from Azima's hacked documents. They demonstrate that Forlit had obtained access to much of Azima's hacked and stolen documents and information as early as August 2015, approximately one year before that information appeared on the internet.

140. In this second affidavit, Forlit also repeated the false statement that he had never performed any work in the state of Florida. However, as alleged above, his company, SDC-Gadot, which he solely owned and controlled, in fact engaged in millions of dollars in transactions with Florida companies. These transactions included receipt of millions of dollars of payments from Page, which were intended to fund the Enterprise's hacking operations.

141. Forlit also submitted filings with the court in the Florida § 1782 Proceeding that included materially false statements intended to thwart document discovery. Shortly after filing the two false affidavits discussed above, Forlit made a filing with the court in which he stated that SDC-Gadot and Insight had no responsive documents to produce in discovery, which sought information relating to Azima's claims that he had been hacked by the Enterprise. This statement was false.

142. As alleged above, voluminous bank records for both entities subsequently obtained by Azima make clear that both entities engaged in millions of dollars in transfers between at least 2017 and 2021. Page has confirmed that many of the transfers reflected in these records were payments to Forlit and his companies for hacking and the preparation of the Hacking Reports and other obstructive conduct, including, for example, providing "security" for the perjury school at the Moosegg Hotel.

143. Thus, Forlit's affidavits submitted in the Florida § 1782 Proceeding, his subsequent filings, and his statements made in his deposition, were materially false, misleading, and corruptly made with an intent to obstruct that matter and to cover up his involvement in the hacking and other illegal activities of the Enterprise.

E. Del Rosso Obstructs Azima's North Carolina Proceeding

144. In a further effort to prevent exposure of its criminal conduct, the Enterprise also obstructed U.S. litigation brought by Azima against Del Rosso for his role in the hacking and

dissemination of Azima's data and trade secrets. In October 2020, Azima sued Del Rosso in the U.S. District Court for the Middle District of North Carolina (the "North Carolina Proceeding"). As it did with the D.C. District Court Proceeding, the Enterprise took extensive steps to obstruct Azima's lawsuit, including interfering with witnesses, manufacturing evidence, and making false statements to the court.

1. The Enterprise Fabricates Evidence in the U.S. and Threatens Its Own Hackers

145. To prevent disclosure of its illegal activity in the North Carolina Proceeding, the Enterprise threatened and tampered with one of their own RICO Conspirators, hacker Aditya Jain, whom they feared was cooperating with Azima, Al Sadeq, and others and would be an important witness in the North Carolina Proceeding.

146. As alleged above, Del Rosso hired Jain on behalf of the Enterprise to hack Azima and his associates. In 2020, Jain confessed to his involvement with the Enterprise and its illegal conduct and detailed his role in the Enterprise. The RICO Conspirators learned of Jain's confession and, fearing that he would emerge as an important witness in Azima's lawsuit, took steps to minimize the damage.

147. On August 29, 2020, Del Rosso contacted Jain, accusing him of working with Azima's lawyers "to [p]oint finger[s]" at the RICO Conspirators and instructing Jain to stop. Jain viewed this contact as a threat.

148. On September 11, 2020, just one month before Azima filed his complaint in the North Carolina Proceeding, at a time when litigation was contemplated, Del Rosso messaged Jain again and accused him of assisting with Azima's case, saying that they both could be "dragged into" the litigation. Del Rosso expressed a fear of being sued, stating that Azima's legal team "seem[s] to have information" about the hacking. In response, Jain suggested that he conduct

additional hacking to determine who was responsible for the leak, feigning his alignment with Del Rosso. Jain asked Del Rosso who to hack, and Del Rosso responded, "I don't have any names but imagine somewhere Stuart Page is in this." The next day, Jain sent Del Rosso a text saying he had details about Azima, and Del Rosso immediately called Jain to discuss. Jain and Del Rosso subsequently discussed the destruction of documents to cover their tracks.

149. In September or October of 2020, Del Rosso deleted his Threema account "~Sierra," which contained communications with his co-conspirators and others that were relevant to the U.S. proceedings. By November 2020, Del Rosso created a new Threema account "~SA BC 86" to communicate with Jain. That account has also since been deleted, in violation of a litigation hold notice sent by Azima in connection with the North Carolina Proceeding.

150. On October 15, 2020, Azima sued Del Rosso in the Middle District of North Carolina, seeking damages and other relief from Del Rosso based on his role in the hacking. One week later, Azima filed a motion seeking permission to issue third party subpoenas for Del Rosso's bank records.

151. The Enterprise then enlisted Jain's help in creating fake documents to cover its tracks. On November 6, 2020, shortly after Azima sought Del Rosso's bank records, Del Rosso messaged Jain expressing concern that Jain's company, Cyber Defense, appeared in Del Rosso's bank statements. Jain and Del Rosso agreed to create a fake contract with Cyber Defense and fake reports to cover up the fact that Del Rosso paid Jain for hacking.

152. On November 9, 2020, Jain sent a draft of the fake contract to Del Rosso for review. On November 18, 2020, Jain sent Del Rosso a fully signed PDF of the fake contract, which falsely stated that Jain's company, Cyber Defense, would provide legitimate IT-related services for Del

Rosso's company, Vital. Though the fake contract was conceived and created in November 2020, the final draft was backdated to May 7, 2019, prior to the filing of the North Carolina Proceeding.

153. On November 26, 2020, Del Rosso also tried to entice Jain to travel to Dubai, where he would be vulnerable to kidnapping or attack by the Enterprise. Jain was concerned for his safety and declined to meet. In December 2020, Del Rosso again asked Jain to meet in Dubai to "clear the air" and to "get to the bottom" of whether Jain was cooperating with Azima's counsel. Jain declined to meet in Dubai for fear that the meeting was a pretext to detain and subject him to coercive interrogation in the same manner as Al Sadeq. On or around January 2021, Del Rosso, CyberRoot employees, and others gathered in Dubai to discuss Jain's cooperation with Azima's counsel and to coordinate their intimidation campaign.

154. The Enterprise also appears to have attempted to hack Jain, presumably to obtain information it could use to prevent him from providing truthful testimony in the North Carolina Proceeding. In July 2021, Jain received phishing emails seeking his personal login information. That same month, a former CyberRoot employee was contacted by someone at CyberRoot, who asked about Jain and suggested that CyberRoot had successfully compromised Jain's Skype account.

155. In August 2021, while the North Carolina Proceeding was pending, the Enterprise further tampered with Jain and pressured him not to cooperate with Azima. Jain received a call from a hacker who worked with CyberRoot. The hacker warned Jain not to reveal the hacker's role in the Enterprise. Jain felt threatened and thought it to be a coordinated effort by the Enterprise to intimidate him and stop him from cooperating with Azima and providing truthful testimony and information in connection with the North Carolina Proceeding.

2. Enterprise Member Del Rosso Makes False Statements to the North Carolina District Court

156. In addition to intimidating a key witness, creating false documents, and destroying records, the Enterprise also sought to obstruct the North Carolina Proceeding by making false statements to the court.

157. After filing the complaint in the North Carolina Proceeding, Azima sought permission to serve subpoenas on third parties to obtain bank records and other documents that could corroborate the allegations in his complaint, including the payments made by Del Rosso and Vital for the Enterprise's hacking activities. On November 12, 2020, in a filing opposing Azima's motion for leave to serve third-party subpoenas and signed by Del Rosso's lawyer, Brandon Neuman, Del Rosso and Vital "categorically den[ied]" Azima's allegations that they had overseen and directed the hacking of Azima and then lied about it in court. These statements were false. The court subsequently denied Azima's motion on December 14, 2020. Bank records showed that Vital paid CyberRoot, the Indian hacking firm, more than $1 million during the same period the Enterprise was hacking Azima and stealing his documents and information.

158. Upon information and belief, these false statements were intended to prevent the North Carolina federal court from authorizing third-party discovery into Del Rosso's and Vital's bank records.

159. On October 12, 2022, Del Rosso filed an answer in the North Carolina proceedings in which he again falsely denied involvement in the hacking. Del Rosso also admitted that he worked for Dechert and Gerrard, was paid more than $1 million by Dechert, and paid more than $1 million to CyberRoot.

160. The obstruction of justice and witness tampering committed by Del Rosso in connection with the North Carolina Proceeding harmed Azima's interest in the litigation and caused unnecessary legal fees and associated costs in connection with the litigation.

F. The Enterprise Conducts Further Hacking to Determine the Sources of Funding for Azima's and Al Sadeq's Litigation

161. As described in the 2016 Action Plan, a principal aim of the Enterprise was to attack the enemies of RAK in part through burying them with costly litigation. Enterprise victims resisted these attacks and brought claims of their own. Accordingly, to further its plan to attack Azima and others, the Enterprise sent, among other wires, fraudulent spear-phishing emails in a campaign of further hacking, to determine who was funding litigation involving Azima, Al Sadeq, and others. The wires were sent as part of the Enterprise's scheme to deprive Azima of his interest in the litigation.

1. The Enterprise Seeks to Determine Who Was Funding Litigation Brought by Azima and Al Sadeq

162. As alleged above, after Azima's D.C. District Court Proceeding was dismissed in favor of a UK forum, he brought counterclaims in the already pending UK Proceeding based on the unlawful hacking and theft of his documents and information. In addition, on January 28, 2020, Al Sadeq sued Dechert, Gerrard, and others in the UK for the mistreatment described above (the "Al Sadeq Proceeding").

163. In early February 2020, during the pendency of the UK Proceeding and just days after the Al Sadeq Proceeding was filed, Handjani, Page, and Gerrard met at the Royal Automobile Club in London. During the meeting, Handjani, Gerrard, and Page discussed their concern that Azima and Al Sadeq appeared to be well funded, frustrating the Enterprise's plan to inflict financial harm on them through litigation. Gerrard and Handjani thus instructed Page to determine

who was funding Azima's and Al Sadeq's litigation. Based on that instruction, Page then contacted Forlit to effect the instruction.

164. Upon information and belief, Gerrard and Handjani knew and intended that Page would engage hackers, such as Forlit and those engaged by him, to carry out their instructions because Page had been providing them for years with regular Hacking Reports that contained information obviously obtained through hacking. Indeed, on July 19, 2022, Dechert and Gerrard conceded that "Mr. Gerrard was aware in or around February 2020 that Mr. Forlit carried out work for Mr. Page and that, as a result, Mr. Page had 'access' to Mr. Forlit's services."

2. The Enterprise Hacks Al Sadeq's Lawyers

165. At approximately the same time that Gerrard and Handjani directed Page to obtain information about the funding of litigation brought by Azima and Al Sadeq, Del Rosso also directed hackers to obtain such information from Al Sadeq's UK lawyers. Upon information and belief, Gerrard instructed Del Rosso to gather this information about Al Sadeq's litigation funding, just as he had done with Page.

166. Del Rosso engaged Patrick Grayson to uncover information concerning the funding source for Al Sadeq's litigation. Grayson suggested hacking Maltin PR, a litigation support and PR firm known to be used by Al Sadeq. Afterwards, Grayson met with Paul Robinson in London on January 30, 2020, to pass on Del Rosso's instructions to investigate the source of Al Sadeq's litigation funding. Grayson and Robinson have since admitted to their role in the hacking of Al Sadeq's lawyers to determine the source of his litigation funding, including that Del Rosso directed the hacking using clandestine messaging applications paid them via transfers sent from U.S.-based bank accounts.

167. Shortly thereafter, Al Sadeq's UK lawyers, Stokoe Partnership Solicitors ("Stokoe"), received numerous phishing emails and text messages.

168. In April 2020, suspicious of the phishing campaign against it, Stokoe set up a sting operation in which the Enterprise hacked and obtained internal Stokoe documents with embedded tracking features.

169. In April or May of 2020, in response to earlier instructions from Gerrard and Handjani, Forlit produced a Hacking Report concerning the source of the litigation funding for Azima and Al Sadeq. Upon information and belief, the report contained information obtained through hacking. According to Page, Handjani was sensitive to who was permitted to view the report. Page sent the hacking report to Handjani using the Signal encrypted messaging application. Additionally, Page provided a hard copy of the report to Gerrard at a gas station near Gatwick Airport in London, where Gerrard requested that they meet because he believed he would not be easily surveilled or spotted there.

3. The Enterprise Bribes Potential Witnesses in U.S. Proceedings

170. On or about June 25, 2020, Grayson met with Robinson at the Goring Hotel in London, where Grayson took Robinson into a black minivan and confiscated Robinson's phone. Grayson told Robinson that "we have a problem" and that someone connected to Robinson had been passing information to "the other side." Grayson then asked Robinson to destroy and "sanitize" any materials that could be traced back to Grayson and Del Rosso. Immediately after the meeting, Robinson returned to his office and enlisted his sister and brother-in-law to help identify, destroy, and doctor documents connecting Robinson to Grayson or Del Rosso.

171. On July 1, 2020, Stokoe issued proceedings in the UK seeking information from Robinson and others about their role in the hacking of the firm (the "Stokoe Proceeding"). In addition, Stokoe subsequently filed a Section 1782 application in the U.S. District Court for the Middle District of North Carolina (the "North Carolina 1782 Proceeding") seeking discovery from Del Rosso concerning the hacking.

172. Upon information and belief, Del Rosso was alarmed by the Stokoe Proceeding and concerned that his role in the Enterprise's hacking would be exposed. Accordingly, he attempted to conceal his connections to Robinson and the hacking by, among other things, fabricating and destroying documents and bribing Robinson. Upon information and belief, Del Rosso's conduct was directed at obstructing both the Stokoe Proceeding in the UK and potential litigation in the US.

173. On July 1, 2020, Del Rosso instructed Robinson not to mention Del Rosso in relation to the Stokoe Proceeding. In return for Robinson's silence, Del Rosso offered to pay him. Del Rosso instructed Robinson to contact his U.S. lawyer, Neuman, who would facilitate the payment. After the phone call with Del Rosso, Robinson destroyed invoices that he had sent to Del Rosso associated with his hacking-related work. On July 2, 2020, Del Rosso paid Robinson $25,000.

174. On or around July 4, 2020, Del Rosso and Neuman called Grayson several times to discuss Stokoe's case against Robinson. Del Rosso and Neuman then drafted a witness statement for Grayson to file in the Stokoe Proceeding. The draft contained false and misleading statements in order to disguise Del Rosso's role in directing Grayson to hack Stokoe. According to Del Rosso, he wanted the Stokoe hacking litigation to "stay over there" in the UK. Del Rosso thereafter contacted Grayson and offered to increase his monthly retainer from $10,000 to $20,000 and offered him a "bonus payment" of £500,000, presumably in exchange for his silence concerning Del Rosso's role in the hacking of Stokoe. Handjani also discussed the "bonus" payment with Grayson, and reassured Grayson that Del Rosso's offer would be honored and could be relied upon. Handjani told Grayson that his legal fees would be fully paid by the "client," which Grayson understood to mean Dechert.

4. Del Rosso Obstructs Al Sadeq's Section 1782 Proceeding in North Carolina

175. On February 5, 2021, Al Sadeq and Stokoe filed a Section 1782 application in the United States District Court for the Middle District of North Carolina seeking discovery from Del Rosso and Vital concerning the attempted hack of Stokoe.

176. On November 30, 2021, Del Rosso falsely denied any involvement in the hacking of Azima in a filing with U.S. District Court for the Middle District of North Carolina, stating that he "had no involvement in the alleged hacking" of Azima.

177. Del Rosso also falsely denied any involvement in the hacking of Stokoe. However, as alleged above, Del Rosso oversaw the hacking of Stokoe and paid Robinson to obtain Stokoe's hacked information. Upon information and belief, Del Rosso made these false and misleading statements in the North Carolina 1782 Proceeding to conceal his and the Enterprise's criminal conduct.

178. On October 18, 2021, the court granted Al Sadeq's Section 1782 application and on March 18, 2022, denied Del Rosso's motion to quash Al Sadeq's subpoenas issued following the court's order granting Al Sadeq's application. This litigation remains pending today.

IV. THE ENTERPRISE'S CRIMES AND COVER-UP HAVE CAUSED SIGNIFICANT DAMAGE TO AZIMA AND HIS BUSINESSES

179. As foreshadowed by the Action Plan, the attacks alleged above successfully damaged Azima and the other Plaintiffs, not only by causing extensive damage to Azima's reputation but also by destroying his business ventures and forcing him to incur substantial debts associated with legal fees and related expenses. The damage the Enterprise has caused to Azima's reputation, business, and property is continuous, ongoing, and significant. Banks have closed Azima's accounts and denied him loans citing the negative publicity brought on by the Enterprise's litigation against Azima in the UK based on the hacked documents.

180. For example, Mr. Azima held a 50% stake in FFV Development (which wholly owns 3260 Main and FFV W39) and planned to develop land owned by each of the LLCs into multi-unit apartment complexes in Kansas City, Missouri. This planned development was subject to lender financing, which had been agreed in principle and approved by lenders at the local level. Main 3260 LLC, in particular, was expecting to receive a loan of approximately $13.5 million. However, as a result of the actions taken by the Enterprise against Azima detailed above, the financing was rejected in January 2019. The lender refused to provide financing due to the negative publicity instigated by the Enterprise that the bank found when conducting its due diligence. Azima attempted to secure alternative financing for both projects but was unsuccessful. As a result, Azima and his companies suffered approximately $15 millions of dollars in lost profits that they otherwise would have obtained from these two projects.

181. The Enterprise also harmed Azima through costly litigation designed to "force [Azima] to invest both energy and funds defending himself, and slowly to fade away from" RAK's disputes with Al Sadeq and Massaad, as outlined in one of the early Hacking Reports. Azima incurred millions of dollars in attorneys' fees and costs defending himself in the litigation in the UK, exposing the Enterprise's pervasive fraud in the litigation in the U.S. and UK, and interacting with law enforcement. As alleged above, one of the objects of the Enterprise's scheme to defraud Azima was to cause him to expend significant legal fees and expenses.

182. The Enterprise's pattern of racketeering activity described herein caused the above harm to Azima, just as the Enterprise foresaw in its Action Plan. The Enterprise's numerous and repeated false statements have been relied upon by U.S. courts, U.S. law enforcement agencies, financial institutions, the media, and by UK courts. But for these false statements and the Enterprise's other obstructive conduct – including witness tampering, document destruction, and

fabrication and manipulation of evidence – Azima could have demonstrated that the 2016 Settlement Agreement (and its UK forum selection clause) was a fraud; avoided a transfer of his case to the UK based on the Agreement's forum selection clause, where he has been forced to participate in costly and burdensome litigation; and obtained a favorable judgment in the D.C. District Court Proceeding against RAK and the North Carolina Proceeding against Del Rosso. But for these false statements and the Enterprise's other obstructive conduct, Azima could have exposed the Enterprise's misconduct and avoided a judgment against him in the UK.

183. These losses were not only foreseeable to the Enterprise but were also the intended result of the Enterprise's actions. The Action Plan outlined a plan to cause damage to Azima through civil and criminal litigation and reputational damage. Attorneys' fees and expenses, improper judgments, the impairment of Azima's business interests, and his loss of access to financial services were all foreseeable, proximate, intended consequences of the harm the RICO Defendants scheme caused Azima. The RICO Defendants have even recently signaled their intent to continue the damage: with their own client (RAKIA) withdrawing from the UK proceedings, Dechert and Gerrard have attempted to take their client's place to maintain the judgment against Azima and continue driving up Azima's legal costs.

V. DECHERT IS LIABLE FOR THE ACTIONS OF THE ENTERPRISE

184. As explained above, not only did at least two Dechert partners participate as members of the Enterprise, but the firm was also itself a central figure in the Enterprise, including its conspiracy, crimes, and subsequent coverup. In addition to providing the resources and infrastructure for the criminal conduct of Dechert partners Gerrard and Hughes, Dechert also played an active and critical role in supporting, facilitating, and concealing the Enterprise's misconduct.

185. Dechert for years either had knowledge of, consciously disregarded, or was at least recklessly indifferent to accusations and, later, overwhelming evidence that two of its equity partners – Gerrard and Hughes – were masterminding and participating in a global criminal enterprise. As alleged above, Dechert committed numerous predicate acts in violation of U.S. federal law in the ordinary course of Dechert's representation of RAKIA. Motivated initially by legal fees and ultimately by a desire to cover up the Gerrard's and Hughes's misconduct, Dechert ignored red flags for years and continued to defend and protect Gerrard, Hughes, and the Enterprise from public exposure and attempts by victims to hold them accountable for their campaign of rampant criminal conduct. Indeed, according to recent press reports, Dechert was "[g]ripped by Gerrard's moneymaking powers" and became a "shrine to Neil," who was regularly applauded for his high billings and was given a seat on the firm's Policy Committee. The firm reportedly went so far as to provide him with "do not enter" rooms that were dedicated to Gerrard's team and his work.

A. Dechert Was at Least Recklessly Indifferent to Overwhelming Evidence of the Enterprise's Crimes

186. Dechert, including partners in leadership positions, were aware of Gerrard's reputation before hiring him. In October 2010, then-Dechert partner Graham Defries informed Dechert management, including its chairman, that Gerrard engaged in "scaremongering in order to increase [Gerrard's then-firm] DLA's fees." This assessment was based upon Defries' firsthand observations. Dechert nevertheless hired Gerrard as a Global Co-Head of the firm's White Collar and Securities Litigation practice and agreed to pay him £2 million in annual compensation (or approximately $3 million USD) on the condition that he produce £12 million in annual fees.

187. In April 2013, however, one of Dechert's largest clients fired Gerrard and Dechert after discovering that they had engaged in what a UK court later characterized as "shocking"

betrayals of the client during the course of the representation.[9] The client's firing of Gerrard and Dechert left Gerrard without a major source of revenue (as he had depended on it for almost the entirety of his billings) thus placing enormous pressure on Gerrard to find another deep-pocketed client he could exploit to justify the outsized compensation package he had received from Dechert. Notwithstanding this obvious red flag regarding Gerrard's conduct, Dechert continued to support Gerrard for approximately nine more years.

188. By April 2014, Dechert received a sworn witness statement stating that Gerrard had said he was "in rape mode" when billing the Dechert client referenced above. By February 2018, Dechert also learned through another witness statement that Gerrard had said he was prepared to "screw these fuckers" (the same large Dechert client) for £25 million in fees. Notwithstanding these startling statements about Gerrard and his billing practices, Dechert continued to support Gerrard for approximately six more years.

189. By 2015, Dechert was aware of accusations that Gerrard engaged in human rights abuses as part of his work. Al Sadeq had accused Gerrard, Hughes, and another Dechert partner of interrogating him under degrading, filthy, and illegal conditions in secret prisons in RAK. When Gerrard learned of Azima's coming campaign against Gerrard's human rights abuses, Gerrard briefed Dechert's leadership on the potential threat posed by Azima's media campaign, which directly implicated Gerrard in human rights abuses. Nevertheless, Dechert continued to support Gerrard for approximately seven more years.

---

[9] A UK court found that Gerrard had leaked the client's privileged and confidential information to the media, engaged in numerous unauthorized and undisclosed meetings with UK government officials, and participated in other misconduct. The same UK court found that Gerrard and Dechert had been "dishonest" with respect to their former client, had engaged in a wide range of serious and unethical conduct that "would be almost unimaginable in the case of a straightforward competent solicitor," and had "lied continuously" when testifying in a suit brought by the former client against them and others.

190. Since 2016, Dechert and partners within the firm's leadership knew, were willfully blind, or otherwise recklessly indifferent to repeated allegations and evidence that Gerrard masterminded the hacking of Azima and suborned perjury before U.S. and UK courts. At each opportunity to rein in potential wrongdoing by Gerrard, Dechert instead actively defended him, and failed to expel him from the partnership.

191. In March 2017, Azima's counsel told Dechert that Dechert remained the only party able to obtain Azima's hacked materials. Although this information should have caused Dechert to investigate why Dechert partners Gerrard and Hughes were the only ones who had access to supposedly publicly available documents – which by then had been downloaded to Dechert servers – Dechert continued to stonewall against allegations of misconduct by Gerrard and continued to permit Gerrard to manage related litigation.

B. Dechert Played a Central Role in the Cover-Up of the Enterprise's Crimes

192. Dechert, through its partners, also played a central role in the coverup of the Enterprise's misconduct. In 2018 and 2019, Gerrard organized a series of meetings in Cyprus, London, and Switzerland to create, develop, and rehearse false testimony about Azima's stolen data. Dechert partner Goldstein (who was handling the U.S.-based D.C. District Court Proceeding at the time) participated in at least two of the meetings.

193. Dechert was also willfully blind or recklessly indifference during separate civil litigation involving Gerrard and defended Gerrard's misconduct even as incriminating details emerged. In an unrelated case in the UK, Gerrard was accused of (and now has been found liable for) mailing an anonymous manilla envelope with sensitive, privileged client information to the UK Serious Fraud Office in order to harm Dechert's own client. One of the envelopes had a hair stuck to it, and Gerrard's client sought to DNA test the hair to see if it belonged to Gerrard or his assistant. Dechert opposed the testing of the hair, and the UK court found that there was a strong

inference that the reason Dechert declined was because the DNA testing might have shown that the hair on the envelope was Gerrard's. Thus, when given a clear opportunity to discover Gerrard's misconduct, Dechert chose to obstruct and prevent the discovery, either because they already knew of the misconduct or because they didn't want to learn the extent of it.

194. In mid-2019, RAK removed Gerrard from its cases, but Dechert continued with the representation and continued to push the false story that its client had innocently found Azima's stolen documents on the internet. Even after Gerrard was removed, the firm remained on the case, with other Dechert partners, including Dechert Chairman Andrew Levander, taking a larger role in the representation. Though Gerrard was removed from the representation, he continued to participate in the Enterprise's affairs and cover-up campaign, including for example organizing the Swiss meetings described above to perfect perjurious witness testimony.

195. In January 2020, during Azima's UK trial, Gerrard falsely denied any involvement or knowledge of the hacking of Azima or improper treatment of Al Sadeq. Yet in June 2020, Gerrard recanted some of his false testimony concerning the treatment of Al Sadeq. Dechert demonstrated reckless indifference to the fact that Gerrard provided false testimony and continued to permit Gerrard to testify.

196. Dechert also provided Gerrard with "burner phones" and allowed him to repeatedly scrub the data from them. Remarkably, Dechert provided Gerrard with at least 15 different mobile devices between 2014 and 2020, during the height of the Enterprise's conspiracy to harm Azima. Dechert did not preserve the data on many of these "burner" phones, even after the phones were returned to the firm.

197. Even in those instances where Dechert did retain Gerrard's data, it was not produced as required in litigation. In July 2021, Dechert's International General Counsel James

Croock conceded that the firm committed a "significant omission" by failing to disclose numerous text messages from 2011 through 2013 on Gerrard's mobile devices that showed Gerrard's previous testimony was false.

198. According to press reports, even as the allegations around Gerrard mounted, Croock (the firm's now-retired former general counsel) "helped establish a 'party line'" that "Dechert and Gerrard were right." Upon information and belief, firm management sent emails to its partners indicating that Dechert had a strong case.

199. Despite more than a decade of red flags and clear indications that Gerrard was engaging in unethical and illegal behavior, it was not until May 2022 that Dechert half-heartedly condemned Gerrard's conduct. Even then, Dechert belatedly attempted to distance itself from Gerrard only following court findings that Gerrard lied under oath. Dechert issued a statement that they "recognise fully the seriousness of the judge's findings in relation to Mr Gerrard's conduct. We are considering the judgment to see what we should learn from it."

200. But Dechert did not learn. Rather, on June 14, 2022, just days after being asked to reconsider the truthfulness of some of statements in the D.C. District Court Proceeding made in reliance on Gerrard, Dechert General Counsel Benjamin Rosenberg replied that the firm had reviewed the record of the D.C. District Court Proceeding and could not find any statement that warranted correction, and repeated yet again Dechert's false statement that Azima's hacked documents were found through publicly available sources.

201. The judicial finding of Gerrard's criminal conduct ultimately led RAK to publicly disavow him. On June 15, 2022, in a letter to Azima's counsel, RAK stated that it had been defrauded by "Mr Gerrard and his gang" and was also a victim of "criminal wrongdoing" by Gerrard. On June 23, 2022, RAK took the remarkable step of withdrawing from the UK

proceeding, claiming it had been misled and lied to by Gerrard and Dechert. In doing so, RAK conceded liability for the hack, saying it "is content for judgment to be entered against it, for damages to be assessed and it will take all necessary steps to ensure that such a judgment is satisfied." RAK cited the recent judgment against Gerrard and Dechert that found Gerrard "to be a dishonest witness who engaged in serious wrongdoing and ethical violations towards a client." In a letter regarding its request to withdraw, RAK described Gerrard and other Enterprise co-conspirators as "dishonest and unscrupulous third-party advisers who have taken steps to advance their own interests for their own gains."

202. On August 9, 2022, in an effort to blame Gerrard for the firm's deliberate breaches of fiduciary duty, Dechert finally conceded through a spokesperson that the firm had "acted in reliance on the assurances given to us by Mr. Gerrard." Dechert continues to repeat the Enterprise's false story to fraudulently mislead Azima, courts, law enforcement, and the public about how they had come into possession of Azima's hacked documents.

203. For all of these reasons, Dechert is liable for the acts of its partners Gerrard and Hughes, as well as the predicate acts of RICO Conspirators committed at their behest.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

(Violations of RICO, 18 U.S.C. § 1962(c))
(Against All RICO Defendants)

204. Plaintiffs reallege and incorporate herein by reference each and every foregoing paragraph of this Complaint as if set forth in full.

205. At all relevant times Plaintiffs Azima, ALG, and Main 3260, FFV W39, and FFV Development each was and is a person within the meaning of 18 U.S.C. §§ 1961(3) and 1962(c).

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

The RICO Enterprise

207. The RICO Defendants and their co-conspirators are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs of this Complaint; namely through a multi-year, multi-faceted campaign of computer hacking, illegal surveillance, witness tampering and intimidation, obstruction of justice, perjury, money laundering, bank fraud, and wire fraud. The Enterprise's goal was to manufacture and prosecute claims against perceived enemies of RAK, including Plaintiffs, and to commit further crimes in the U.S. and overseas to cover up their unlawful conduct and obstruct Plaintiffs' efforts to seek a legal remedy. Over the years, the RICO Defendants and their co-conspirators have adapted their scheme to changing circumstances, expanding the scope and nature of their activities to harm Plaintiffs and conceal their illegal conduct. The affairs of the Enterprise were intended to, and have in fact resulted in, great financial gain for the RICO Defendants through millions in fees for their criminal services and great harm to the business and property of Plaintiffs in the US.

208. These RICO Defendants and their co-conspirators have organized their operation into a cohesive group with specific and assigned responsibilities and command structure, operating in the U.S. and other countries, with funding and direction coming to and going from the US. The Enterprise has operated continuously since 2014, when Gerrard and Dechert were first retained by RAK for this work.

209. Gerrard was a leader of the Enterprise, and he relied upon and utilized the vast resources of Dechert in executing the plan of the Enterprise. Dechert, through Gerrard, oversaw and directed the use of hacking coordinators, Del Rosso and Page, each of whom engaged hackers to participate in the affairs of the Enterprise as described above. The Enterprise continues to this day, with RICO Defendants and co-conspirators continuing their efforts to cover-up the Enterprise's illegal conduct by, among other things, making false statements in judicial proceedings and tampering with witnesses and evidence.

210. The RICO Defendants and their co-conspirators constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). Each of the RICO Defendants participated in the operation or management of the Enterprise.

211. At all relevant times, the Enterprise was engaged in, and its activities affected interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

Pattern of Racketeering Activity

212. The RICO Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the Enterprise's affairs through a "pattern of racketeering activity" within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c), including the following acts of racketeering activity:

1. Obstruction of Justice in Violation of 18 U.S.C. § 1503

213. Over the past six years, numerous cases have arisen in the U.S. that threaten to expose the misconduct and crimes of the Enterprise. In a concerted effort to thwart Azima's attempts to uncover the truth and avoid discovery that would reveal their illegal conduct, the RICO Defendants have engaged in a lengthy pattern of obstruction and lies through document destruction, fabrication of evidence, mail fraud, and witness tampering and intimidation, as alleged in detail above.

214. The obstructive conduct also included false declarations stating that: (1) they did not hack Azima and did not know who had hacked Azima; (2) they did not have Azima's hacked documents in March 2016, when they induced Azima to sign the fraudulent 2016 Settlement Agreement; (3) they only obtained Azima's hacked data from publicly available links on the internet and they had no role in creating those links; and (4) the innocent discovery of Azima's hacked documents on publicly available internet sites prompted them to bring litigation against Azima.

215. The RICO Defendants have made these statements with full knowledge that the statements were false and misleading, as evidenced by the documents showing that the Enterprise was in possession of Azima's hacked documents as early as August 2015.

216. By making these deliberate and strategic false representations in various pending federal judicial proceedings, including the D.C. District Court Proceeding and Section 1782 proceedings, from September 2016 through as recently as September 2022, with full awareness of their consequence and with the specific intent to corruptly endeavor to influence, obstruct, and impede the due administration of justice, the RICO Defendants have repeatedly engaged in obstruction of justice in violation of 18 U.S.C. § 1503.

2. Witness Tampering in Violation of 18 U.S.C. § 1512

217. In order to conceal their criminal conduct and harm to Azima, the Enterprise engaged in multiple instances of witness tampering as recently as July 2020 in violation of 18 U.S.C. § 1512.

218. In August and September 2020, Azima was preparing to file a complaint against Del Rosso and Vital in the North Carolina Proceeding. In addition, Azima had filed the New York § 1782 Proceeding against Handjani, Al Sadeq had filed Section 1782 proceedings against Del Rosso, and Stokoe had filed proceedings against Robinson. Each of those proceedings risked exposing that Del Rosso had hired co-conspirators CyberRoot and Jain to hack Azima and others.

219. Fearing that Jain would expose the truth about the hacking and Del Rosso's involvement and the Enterprise's illegal conduct, Del Rosso knowingly engaged in intimidation, threats, and corrupt persuasion toward Jain with the specific intent to influence, delay and prevent Jain's testimony or to cause Jain to withhold relevant evidence during the North Carolina Proceeding. Del Rosso also knowingly fabricated evidence to impair discovery during U.S. proceedings. Additionally, as alleged above, Del Rosso and Handjani bribed Grayson and Robinson for their silence during the Stokoe Proceeding and instructed Robinson to destroy relevant evidence of the Stokoe hack.

220. The foregoing conduct constitutes witness tampering in violation of 18 U.S.C. § 1512.

3. Money Laundering in Violation of 18 U.S.C. § 1956(a)(2)(A)

221. The RICO Defendants have engaged in repeated acts of money laundering in furtherance of and to promote the unlawful objectives and activities of the Enterprise. Members of the Enterprise knowingly caused the transportation, transmission, and/or transfer of funds to or from the United States to themselves and other RICO Conspirators to promote unlawful activity,

including but not limited to violations of 18 U.S.C. §§ 1341, 1343, 1344, 1503, and 1512, as alleged in this Complaint.

222. Exhibit A details known money laundering transactions in furtherance of the scheme to defraud. As described above, these transactions were made in U.S. dollars by or to RICO Conspirators via wire either in to or out of the U.S. Each of these transfers was made for the purpose of carrying on and promoting illegal activity in violation of 18 U.S.C. § 1956, as alleged above. The 413 money laundering transactions listed in the chart total more than $29 million.

4. Mail Fraud and Wire Fraud in Violation of 18 U.S.C. §§ 1341 and 1343

223. As alleged herein, as part of the cover-up, the RICO Defendants engaged in a wide-ranging scheme or artifice to defraud Azima and harm him financially by embroiling him in expensive litigation, obtaining a judgment against him, and destroying his businesses and ability to generate income. Many of the wires in furtherance of this scheme were sent in the past four years.

224. As part of the scheme to defraud Azima, the Enterprise manufactured false evidence and used that evidence against Azima, claiming it was true when it was not. The scheme included the use of wires to deceive Azima, the U.S. courts, UK courts, and the public to believe that the RICO Conspirators had found Azima's stolen data on publicly available links on the internet, when in fact the RICO Conspirators hacked Azima and posted his data on the internet to hide the fact that they had stolen it. The scheme also included attempts to deceive Azima, the U.S. courts, UK courts, and the public to believe that the 2016 Settlement Agreement was negotiated in good faith when in fact it was procured by fraud. The objective of the scheme was to deprive Azima of money and property as described herein, including by coercing Azima to pay RAK significant sums of money that would benefit the RICO Defendants, by forcing him to incur substantial fees

and costs associated with litigation, by causing substantial damage to his businesses, and by preventing him from succeeding in litigation against RAK, as alleged herein.

225. As part of the scheme to defraud Azima, the Enterprise sent wires designed to harm Azima's businesses, including posting Azima's stolen data on WeTransfer links on the internet in 2019, sending stolen data to media outlets to create negative publicity to harm Azima, and sending wires containing false statements about Azima and his stolen data to deceive the courts and the public. The object of the scheme was to cause financial harm to Azima and his businesses to "force him to invest both energy and funds defending himself, and slowly to fade away" from RAK's ongoing litigation, as described in one of the Hacking Reports.

226. As part of the scheme to defraud Azima, the Enterprise engaged in a hacking campaign through at least 2020, including attempts to determine whether Azima's litigation was being funded. The object of the scheme was to deprive Azima of money and property related to his ongoing litigation.

227. Azima incorporates by reference Exhibit B, which sets forth particular uses of wire and mail communications in the U.S. in furtherance of the scheme to defraud, describing which RICO Conspirator caused the communication to be mailed or wired, when the communication was made, and how it furthered the fraudulent scheme. The 173 wire and mail communications described in Exhibit B were made in furtherance of the scheme to defraud Azima.

228. Azima also incorporates by reference Exhibit A, which sets forth money laundering transactions in furtherance of the scheme to defraud. Each of these wire transfers was made in furtherance of the scheme to defraud and constitutes another instance of wire fraud.

229. This scheme to defraud was intended to, and in fact did, cause cognizable injury to Azima (a U.S. citizen) and his co-Plaintiffs (U.S. entities) by depriving them of money and

property in the U.S. and causing detrimental injuries to their U.S. business interests. These injuries included depriving Azima of identifiable and quantifiable business opportunities and causing Azima's banks to close accounts, cancel credit cards and lines of credit, and cancel business financing and/or refuse to provide Azima with such financing. The injuries caused by the scheme to defraud also included defeating Azima's meritorious claims for the Enterprise's hacking and related injuries, as well forcing Azima to spend fees to pursue these claims that would have been unnecessary but for RICO Defendants' acts of fraud. The injuries to Azima were directly and proximately caused by the Defendants' fraudulent schemes in violation of the mail and wire fraud statute, have occurred within the past four years, and continue to this day.

230. The RICO Defendants' false and misleading statements have been relied on by Azima, U.S. courts, U.S. government agencies, the UK court, and Azima's customers, business partners, potential customers and business partners, lenders and banks. As a foreseeable and intended result of the RICO Defendants' false and misleading statements, the fraudulent scheme has caused Azima and his co-Plaintiffs substantial damages and lost business opportunities.

5. Bank Fraud in Violation of 18 U.S.C. § 1344

231. The Enterprise unlawfully executed and attempted to execute a scheme to obtain money, funds, and credits from a financial institution under false and fraudulent pretenses and via false and misleading representations in violation of 18 U.S.C. § 1344.

232. From October 2017 through as recently as October 2021, Forlit, Insight, and SDC-Gadot opened bank accounts with financial institutions in the U.S. through false statements and representations, intentionally designed to defraud banks into providing their services in support of the Enterprise's illicit money laundering. For example, in its account opening documents, Citibank asked Forlit to state the "Purpose or Reason for Wire" of wires SDC-Gadot intended to send and receive internationally using its account. Forlit falsely and/or misleadingly answered that SDC-

Gadot's U.S.-based Citibank account would send wires of approximately $100,000 each up to ten times per month to bank accounts in Israel for "IT ANALYSIS SERVICES." Forlit also misleadingly stated that SDC-Gadot's U.S.-based Citibank account would receive regular monthly wires of approximately $250,000 up to ten times per month from the UAE, UK, and Hong Kong for vague "SERVICES." In fact, the purposes of all wires sent and received internationally by SDC-Gadot's Citibank account were to channel money from Page and RAK to Forlit's Israeli company "Gadot Information Services," which investigated and hacked Enterprise targets, including Azima. Indeed, under oath, Forlit later admitted that his U.S. entities SDC-Gadot and Insight had "no business activity other than to serve as a conduit to transfer money" to pay Forlit's Israel-based company, which hacked Azima and other Enterprise targets.

233. In SDC-Gadot's account opening submissions to Citibank, Forlit also misleadingly stated that co-conspirator Eitan Arusy's company Global Impact Services was among Gadot's "major customers." In fact, under oath, Forlit later admitted that Arusy was actually a co-conspirator within the Enterprise who served on the team that hacked Azima and others. Forlit admitted that he and Arusy met with Gerrard, Buchanan, and Page – all high-level members of the Enterprise – to discuss the hacking of Azima at least five to ten times. Far from serving as one of Gadot's "major customers," Arusy and his company were co-conspirators in the same scheme splitting the proceeds of their criminal conduct using Citibank's wires.

234. To deceive U.S. banks into facilitating their transfer of proceeds from the Enterprise's scheme, Forlit and Page fabricated false and misleading invoices to convince banks to approve transactions. Forlit has admitted that when banks raised concerns about funds transfers, he and Page "would make some [written] arrangements that would pacify the banks." Despite having no retainer agreement between Forlit and Page for hacking services, they fabricated retainer

agreements for "special IT network protection consulting" to convince banks to approve wire transfers paying Forlit for hacking Enterprise targets like Azima. Forlit also admitted that invoices for the hacking of Azima and others would reference this "agreement" to "make the bank pay more easily" if the bank asked to see the invoice supporting the wire transfer.

235. Until as recently as October 2021, Forlit and Page succeeded in deceiving U.S.-based Citibank, Bank of America, and J.P. Morgan into approving wire transfers of the hacking proceeds. By Forlit's own admission, the banks approved transfers of at least $5 million from Page to Forlit through U.S. bank accounts for "Project Beech" targeting Azima and others for hacking.

236. Del Rosso and Vital also engaged in similar acts of bank fraud against U.S. financial institutions. As with Forlit's account opening submissions to Citibank, upon information and belief, Del Rosso and Vital concealed from his U.S.-based bank, PNC Bank, that one of their accounts would be used to pay over $1 million USD to hackers associated with CyberRoot and Aditya Jain's company Cyber Defence and Analytics. In a sworn witness statement in the UK proceedings, Jain admitted to receiving over $50,000 from Del Rosso to hack Azima and other Enterprise targets. Jain also testified that CyberRoot employees shared with Jain that CyberRoot was paid over $1 million to hack Azima.

Summary of the Pattern of Racketeering Activity Alleged as to Each RICO Defendant

237. Each of the RICO Defendants has participated in and conducted the affairs of the Enterprise by engaging in multiple predicate acts, as alleged above and summarized immediately below. The conduct of each of the RICO Defendants constitutes a pattern of racketeering activity, within the meaning of 18 U.S.C. § 1961(5).

238. Defendant Gerrard has committed numerous predicate acts, including mail and wire fraud, obstruction of justice, witness tampering, and money laundering. Gerrard engaged in

obstruction of justice and wire fraud by causing false statements to be made in U.S. and UK courts and to U.S. law enforcement agencies in service of the Enterprise's scheme to defraud Azima. Gerrard caused to be filed in U.S. courts and sent via wire to Azima's counsel documents that falsely represented that RAK innocently discovered Azima's hacked materials on the internet after negotiating the 2016 Settlement Agreement in good faith. Gerrard also directed the scheme to defraud the U.S. courts by mailing stolen documents to the D.C. district court. Gerrard engaged in witness tampering by secretly coaching witnesses to commit perjury directed at least in part toward the U.S. litigation. Gerrard engaged in money laundering by knowingly causing funds to be transported, transmitted, or transferred to and from the US with the intent that such payments would fund the Enterprise's criminal activity. Specific instances of wire fraud and mail fraud are listed in Exhibit B, and specific instances of money laundering are listed in Exhibit A.

239. Defendant Dechert, through the actions of its partners, has committed numerous predicate acts, including mail and wire fraud, obstruction of justice, witness tampering, and money laundering. Dechert engaged in obstruction of justice and wire fraud by causing false statements to be made in U.S. and UK courts and to U.S. law enforcement agencies in furtherance of the scheme to defraud Azima. Dechert filed in U.S. courts and sent via wire to Azima's counsel documents that falsely represented that RAK innocently discovered Azima's hacked materials on the internet after negotiating the 2016 Settlement Agreement in good faith. Specific instances of wire fraud and mail fraud are listed in Exhibit B, and specific instances of money laundering are listed in Exhibit A.

240. Defendant Hughes has committed numerous predicate acts, including mail and wire fraud, obstruction of justice, witness tampering, and money laundering. Hughes engaged in obstruction of justice and wire fraud by causing false statements to be made in U.S. and UK courts

and to U.S. law enforcement agencies in service of the Enterprise's scheme to defraud Azima. Hughes caused to be filed in U.S. courts and sent via wire to Azima's counsel documents that falsely represented that RAK innocently discovered Azima's hacked materials on the internet after negotiating the 2016 Settlement Agreement in good faith. Hughes also directed the scheme to defraud the U.S. courts by mailing stolen documents to the D.C. district court. Hughes engaged in witness tampering by secretly coaching witnesses in the UK proceeding to commit perjury directed at least in part toward the U.S. litigation. Specific instances of wire fraud are listed in Exhibit B.

241. Defendants Del Rosso and Vital have committed numerous predicate acts, including mail and wire fraud, obstruction of justice, witness tampering, bank fraud, and money laundering. Del Rosso engaged in obstruction of justice and wire fraud by manufacturing evidence and causing false statements to be made to U.S. and UK courts, to Azima's counsel, and to U.S. law enforcement agencies, many of which were made over the wires in furtherance of the Enterprise's scheme to harm and defraud Azima. Del Rosso has also engaged in witness tampering and extortion through threats to Jain, Robinson and Grayson. Del Rosso and Vital have committed wire fraud and engaged in money laundering by knowingly causing funds to be transported, transmitted, or transferred from the United States to hackers CyberRoot and Aditya Jain in India with the intent that such payments would fund the RICO Defendants' criminal activity. Specific instances of wire fraud and mail fraud are listed in Exhibit B, and specific instances of money laundering are listed in Exhibit A.

242. Defendants Forlit, Insight, and SDC-Gadot have committed numerous predicate acts, including mail and wire fraud, obstruction of justice, witness tampering, bank fraud, and money laundering. Forlit engaged in obstruction of justice and wire fraud by manufacturing

evidence and causing false statements to be made to U.S. and UK courts, to Azima's counsel, and to U.S. law enforcement agencies, many of which were made over the wires in furtherance of the Enterprise's scheme to defraud Azima. Forlit engaged in witness tampering by manufacturing a false witness statement for Halabi, which was directed at least in part toward the U.S. litigation. Insight and SDC-Gadot are alter egos of Forlit and are liable for Forlit's conduct. Forlit, Insight, and SDC-Gadot have committed wire fraud and engaged in money laundering by knowingly causing funds to be transported, transmitted, or transferred from the United States to hackers in Israel with the intent that such payments would fund the Enterprise's criminal activity. Specific instances of wire fraud and mail fraud are listed in Exhibit B, and specific instances of money laundering are listed in Exhibit A.

243. Defendant Handjani has committed numerous predicate acts, including mail and wire fraud, obstruction of justice, and witness tampering. Handjani has engaged in obstruction of justice and wire fraud by participating in multiple meetings regarding the attacks on Azima, causing false statements to be made in U.S. and UK courts in service of the Enterprise's scheme to harm and defraud Azima. Handjani has also engaged in witness tampering by guaranteeing payment of Patrick Grayson's legal fees in exchange for false testimony concealing Del Rosso's and Vital's roles in the Enterprise's hacking operations.

244. Defendants Frank and KARV Communications have committed numerous predicate acts, including mail and wire fraud, obstruction of justice, and witness tampering. Frank and KARV have engaged in obstruction of justice by causing false statements to be made in U.S. and UK courts in in furtherance of the scheme to defraud Azima by drafting the action plan by which the Enterprise would use false statements in litigation to inflict attorneys' fees, costs, and reputational harm to Azima. Frank and KARV engaged in extortion of Azima by developing and

executing the scheme to manufacture false evidence to be used against Azima and relied upon that false evidence in U.S. and UK legal proceedings and with the press. Frank and KARV have also committed wire fraud and engaged in money laundering by knowingly causing funds to be transported, transmitted, or transferred to the United States from the UAE through RAK with the intent that such payments would fund the Enterprise's criminal activity. Specific instances of wire fraud and mail fraud are listed in Exhibit B, and specific instances of money laundering are listed in Exhibit A.

Injury to Plaintiffs' Business and Property

245. Azima was injured in his business and property by reason of the RICO Defendants' violation of 18 U.S.C. § 1962(c). The injuries to Azima caused by reason of the violations of 18 U.S.C. § 1962(c) include but are not limited to, the impairment of Plaintiff's business interests in executed contracts including but not limited to those described above; damages to Azima's reputation and good will; and attorneys' fees, costs to defend himself, and payments made in connection with improper litigation, as well as costs to investigate and disprove false testimony, as alleged herein.

246. Plaintiff ALG Transportation Inc. was injured in its business and property by reason of the Defendants' violation of 18 U.S.C. § 1962(c). The injuries to ALG Transportation, Inc. caused by reason of the violations of 18 U.S.C. § 1962(c) include but are not limited to damages to ALG Transportation's reputation and goodwill; damages stemming from the unlawful hacking and release of ALG Transportation's business records, financial documents, and trade secrets; and the attorneys' fees and costs to defend against subpoenas, which were issued to ALG Transportation as a result of the Enterprise's campaign to instigate FBI pressure.

247. Plaintiff Main 3260 was injured in its business and property by reason of the Defendants' violation of 18 U.S.C. § 1962(c). The injuries to Main 3260 LLC caused by reason

of the violations of 18 U.S.C. § 1962(c) include but are not limited to damages stemming from the loss of financing that had been preliminarily approved for the housing projects, lost profits related to the projects, and damages to the company's reputation and goodwill.

248. Plaintiff FFV W39 injured in its business and property by reason of the Defendants' violation of 18 U.S.C. § 1962(c). The injuries to FFV W39 LLC caused by reason of the violations of 18 U.S.C. § 1962(c) include but are not limited to damages stemming from the loss of financing that had been preliminarily approved for the housing projects, lost profits related to the projects, and damages to the company's reputation and goodwill.

249. Plaintiff FFV Development was injured in its business and property by reason of the Defendants' violation of 18 U.S.C. § 1962(c). The injuries to FFV Development LLC caused by reason of the violations of 18 U.S.C. § 1962(c) include but are not limited to damages stemming from the loss of financing that had been preliminarily approved for the housing projects, lost profits related to the projects, and damages to the company's reputation and goodwill.

250. Further, these injuries to Plaintiffs Azima, ALG Transportation, Inc., Main 3260, FFV W39, and FFV Development were a direct, proximate, and reasonably foreseeable result of the violation of 18 U.S.C. § 1962. Plaintiffs are the ultimate victims of the RICO Defendants' unlawful Enterprise. Plaintiffs have been and will continue to be injured in their business and property in an amount to be determined at trial, with total damages in excess of $100 million.

251. Pursuant to 18 U.S.C. § 1964(c), Plaintiffs are entitled to recover treble damages plus costs and attorneys' fees from the RICO Defendants.

WHEREFORE, Plaintiffs Azima, ALG, Main 3260, FFV W39, and FFV Development pray for judgment as set forth below.

SECOND CLAIM FOR RELIEF

(Conspiracy to Violate RICO, Violation of 18 U.S.C. § 1962(d))
(Against All RICO Defendants)

252. Plaintiffs reallege and incorporate herein by reference each and every foregoing paragraph of this Complaint as if set forth in full.

253. The RICO Defendants have unlawfully, knowingly and willfully combined, conspired, confederated and agreed together and with others to violate 18 U.S.C. § 1962(c) as described above, in violation of 18 U.S.C. § 1962(d).

254. Upon information and belief, the RICO Defendants knew that they were engaged in a conspiracy to commit the predicate acts, and they knew that the predicate acts were part of such racketeering activity, and the participation and agreement of each of them was necessary to allow the commission of this pattern of racketeering activity. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c) and, (d).

255. Upon information and belief, the RICO Defendants agreed to conduct or participate, directly or indirectly, in the conduct, management, or operation of the Enterprise's affairs through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

256. Each RICO Defendant knew about and agreed to facilitate the Enterprise's scheme to inflict massive legal fees upon and spoil business interests of Plaintiffs. It was part of the conspiracy that the RICO Defendants and their co-conspirators would commit a pattern of racketeering activity in the conduct of the affairs of the Enterprise, including the acts of racketeering set forth herein.

257. As a direct and proximate result of the RICO Defendants' conspiracy, the acts of racketeering activity of the Enterprise, the overt acts taken in furtherance of that conspiracy, and violations of 18 U.S.C. § 1962(d), Azima has been injured in his business and property, including

but not limited to the impairment of Azima's interest in executed contracts including the apartment projects described above, damages to Azima's reputation and good will, a judgment against Azima procured by fraud, and attorneys' fees and costs to defend himself in fraudulently manufactured and improperly motivated litigation in the UK and to investigate and disprove false testimony and declarations provided by the RICO Defendants in judicial proceedings in the U.S. and UK.

258. As a direct and proximate result of the RICO Defendants' conspiracy, the acts of racketeering activity of the Enterprise, the overt acts taken in furtherance of that conspiracy and violations of 18 U.S.C. § 1962(d), Plaintiff ALG Transportation, Inc. has been injured in its business and property, including but not limited to damages to ALG Transportation's reputation and goodwill; damages stemming from the unlawful hacking and release of ALG Transportation's business records, financial documents, and trade secrets; and the attorneys' fees and costs to defend against subpoenas, which were issued to ALG Transportation as a result of the Enterprise's campaign to instigate FBI pressure.

259. As a direct and proximate result of the RICO Defendants' conspiracy, the acts of racketeering activity of the Enterprise, the overt acts taken in furtherance of that conspiracy and violations of 18 U.S.C. § 1962(d), Plaintiff Main 3260 has been injured in its business and property, including but not limited to damages to Main 3260's reputation and goodwill, which proximately caused the collapse of financing for housing development projects.

260. As a direct and proximate result of the RICO Defendants' conspiracy, the acts of racketeering activity of the Enterprise, the overt acts taken in furtherance of that conspiracy and violations of 18 U.S.C. § 1962(d), Plaintiff FFV W39 has been injured in its business and property, including but not limited to damages to FFV W39's reputation and goodwill, which proximately caused the collapse of financing for housing development projects.

261. As a direct and proximate result of the RICO Defendants' conspiracy, the acts of racketeering activity of the Enterprise, the overt acts taken in furtherance of that conspiracy and violations of 18 U.S.C. § 1962(d), Plaintiff FFV Development has been injured in its business and property, including but not limited to damages to FFV Development's reputation and goodwill, which proximately caused the collapse of financing for housing development projects.

262. Pursuant to 18 U.S.C. § 1964(c), Plaintiffs are entitled to recover treble damages plus costs and attorneys' fees from the RICO Defendants.

WHEREFORE, Plaintiffs pray for judgment as set forth below.

PRAYER FOR RELIEF

1. For general damages according to proof at trial, trebled according to statute, 18 U.S.C. § 1964(c).

2. For pre-judgment interest according to statute;

3. For Plaintiffs' reasonable attorneys' fees and costs according to statute, 18 U.S.C.§ 1964(c); and

4. For such other legal and equitable relief as the Court may deem appropriate.

October 13, 2022

Respectfully submitted,

/s/ Calvin Lee

Calvin Lee (#5621677)
Kirby D. Behre (*pro hac vice* motion forthcoming)
Timothy P. O'Toole (*pro hac vice* motion forthcoming)
Ian A. Herbert (*pro hac vice* motion forthcoming)
Cody F. Marden (*pro hac vice* motion forthcoming)
Miller & Chevalier Chartered
900 Sixteenth St. NW
Black Lives Matter Plaza
Washington, DC 20006
Tel. (202) 626-5800
Fax. (202) 626-5801
Email: clee@milchev.com
Email: kbehre@milchev.com
Email: totoole@milchev.com
Email: iherbert@milchev.com
Email: cmarden@milchev.com

Counsel for Plaintiffs