UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELLIOTT BROIDY and BROIDY CAPITAL MANAGEMENT, LLC, Plaintiffs, —v.— GLOBAL RISK ADVISORS LLC, GRA QUANTUM LLC, GRA RESEARCH LLC, GLOBAL RISK ADVISORS EMEA LIMITED, GRA MAVEN LLC, QRYPT, INC., KEVIN CHALKER, DENIS MANDICH, ANTONIO GARCIA, and COURTNEY CHALKER Defendants.	Case No. 1:19-CV-11861 JURY TRIAL DEMANDED

SECOND AMENDED COMPLAINT

Plaintiffs Elliott Broidy ("Broidy") and Broidy Capital Management, LLC ("BCM") (collectively, "Plaintiffs"), pursuant to Fed. R. Civ. P. 8, file this Second Amended Complaint against Global Risk Advisors LLC ("GRA"), GRA Quantum LLC ("GRA Quantum"), GRA Research LLC ("GRA Research"), Global Risk Advisors EMEA Limited ("GRA EMEA"), GRA Maven LLC ("GRA Maven"), Qrypt, Inc. ("Qrypt"), Kevin Chalker ("Chalker"), Denis Mandich ("Mandich"), Antonio Garcia ("Garcia"), and Courtney Chalker (collectively, "Defendants") based on the following allegations:

1. Broidy is a prominent business and civic leader and a philanthropist who has actively served in leadership roles in the Republican Party and Jewish organizations. His advocacy against terrorism and extremism in protection of his country is well known, as is his criticism of

Qatar for sponsoring terrorists. Plaintiffs are victims of a hack-and-smear operation whose goal was to silence Broidy's criticism of Qatar's support for terrorism. Defendants sought to achieve this objective through the use of computer hacking and surveillance that occurred on numerous occasions in 2017, 2018, and at least the first half of 2019.

2. The hackers were extremely sophisticated and undertook measures to conceal their identities, including through their use of virtual private networks ("VPNs").

3. Nevertheless, through direct and circumstantial evidence, including information provided by third-party sources with direct and personal knowledge of relevant facts (e.g. part D below), and after a diligent inquiry, Plaintiffs have an informed belief that Defendants are responsible for the unauthorized access and theft of Plaintiff's legally protected electronic communications and other materials.

4. Indeed, Plaintiffs have interviewed numerous former GRA employees who have tied Chalker and GRA directly to the hacking, surveillance, and other covert projects for Qatar. The declaration of one of these former GRA employees, made under penalty of perjury, is attached here and is incorporated into the pleading.

5. Plaintiffs bring this action to recover damages owed to them under the federal statutes prohibiting computer hacking, theft of trade secrets, and racketeering, as well as related claims arising under California statutory and common law.

PARTIES

6. Broidy is a California citizen and the chief executive officer, chairman, and sole member of BCM.

7. BCM is a venture capital investment company organized under Delaware law and headquartered in California. Because Broidy is BCM's sole member, BCM is a citizen of California.

8. GRA is a cybersecurity company organized under Delaware law and headquartered in New York. Because Chalker is GRA's sole member, GRA is a citizen of New York.

9. Chalker is the owner and sole member of GRA, which he operates and controls. Chalker is a citizen, resident, and domiciliary of New York. Chalker also owns and/or controls several other affiliated entities, including but not limited to GRA Maven, GRA Quantum, GRA EMEA, GRA Research, Qrypt, Bernoulli Limited, and Toccum Limited. At all relevant times, all of these entities and their employees and agents operated under the direct control and domination of GRA and Chalker.

10. Mandich was the mastermind behind the GRA's secretive covert operations. At all relevant times, Mandich was acting within the scope of his employment and under Chalker's direct control.

11. At all relevant times, Garcia was GRA's Chief Security Officer and was acting within the scope of his employment and under Chalker's direct control.

12. Courtney Chalker is Chalker's brother and carried out the destruction of electronic devices and other materials containing evidence of the hacking on behalf of GRA and under Kevin Chalker's direct control.

JURISDICTION AND VENUE

13. The Court has diversity jurisdiction under 28 U.S.C. § 1332(a), because Plaintiffs are California citizens whereas Defendants are not. Additionally, the amount in controversy far exceeds $75,000.

14. The Court also has federal question jurisdiction under 28 U.S.C. § 1331, because this action arises under the laws of the United States.

15. The Court has supplemental jurisdiction under 28 U.S.C. § 1367(a), because Plaintiffs' state law claims are so related to the federal claims that they form part of the same case or controversy.

16. The Court has original jurisdiction under 18 U.S.C. § 1836(c).

17. The Court has personal jurisdiction over GRA because it is headquartered in New York, and thus resides in and is domiciled in this state.

18. The Court has personal jurisdiction over Chalker because he resides in and is domiciled in New York.

19. Because GRA and Chalker are New York residents, this Court has personal jurisdiction over the remaining Defendants under 18 U.S.C. § 1965.

20. Also, because the remaining Defendants were acting as agents of GRA and Chalker, the Court has personal jurisdiction under New York CPLR § 302(a)(1).

21. This Court is the proper venue under 28 U.S.C. § 1391(b)(2) and (3), because a substantial part of the events giving rise to Plaintiffs' claims occurred in this district, and at least one Defendant resides in this district.

22. This Court is the proper venue under 18 U.S.C. § 1965(a).

FACTUAL BACKGROUND

A. At the Time the Hack-and Smear Operation Began in 2017, Qatar Had a Motive to Silence Broidy Because of His Increased Criticism of Qatar's Support for Terrorism.

23. Elliott Broidy is a staunch supporter of Israel and a recognized leader in conservative Jewish political circles. He has a long history of investing personal time and resources in anti-terrorist causes.

24. Broidy served on the Department of Homeland Security's Advisory Council between 2006 and 2009. There, he contributed to the report of the Council's Future of Terrorism Task Force, which called for the elimination of terrorist safe havens throughout the world. Broidy has long provided major funding for the Joint Regional Intelligence Center ("JRIC"), which is a cooperative effort between U.S. federal, state, and local law enforcement agencies to collect, analyze, and disseminate terrorism-related threat intelligence. The JRIC continues to serve as the Regional Threat Assessment Center for the Central District of California. Although Broidy is a committed Republican, his contributions in the area of counter-terrorism and America's national security have been widespread and bipartisan, including his efforts via the America Matters Foundation, American Freedom Alliance, the George Washington University Center for Homeland Security, the Hudson Institute, the Manhattan Institute of New York, the Pacific Council on International Policy, and the Panetta Institute for Public Policy.

25. As part of those efforts, Broidy has been an outspoken critic and opponent of the State of Qatar because of the country's ties to terrorism. Broidy's efforts to shed light on Qatar's support for terrorism and its influencing of U.S. foreign policy to be less harsh toward Iran and terrorist groups like Hamas have included, among other things, financial support for think tanks and other non-profits, correspondence with elected and governmental officials, and op-eds in national publications. The Department of Justice has "impaneled a grand jury in Washington, DC.

[as part of an] ongoing probe into Qatar's influence efforts by unregistered operatives,"[1] and in recent months, DOJ has demanded that multiple Qatari-controlled entities must register under FARA, including Al Jazeera[2] and the Qatar-America Institute.[3] Neither Chalker nor any of his GRA entities has registered under FARA for representation of Qatar.

26. Qatar is widely recognized as a sanctuary for terrorist leaders and organizations, including but not limited to Al Qaeda (including Al-Shabab and Al Qaeda in Syria, also known as Al-Nursa Front or Jabhat Al-Nursa), Hamas, the Taliban, and the Muslim Brotherhood. Indeed, the U.S. Department of Treasury has sanctioned numerous individuals residing in Qatar for raising funds for Al Qaeda. Qatar also has permitted Hamas leaders to operate freely within Qatar and has provided substantial funding to the group, despite the threat of international political and economic sanctions for such support. Similarly, Qatar has allowed the Taliban to operate and maintain an office in Doha since at least 2014. Qatar has given safe haven to many leaders of the Muslim Brotherhood after their expulsion from Egypt by the Egyptian government. And Qatar has allied itself in close strategic partnership with regimes governing Iran and Russia.

27. Broidy has for years viewed Qatar as a major threat to U.S. Security. He has funded public initiatives, such as conferences, to educate Americans about Qatar's support for terrorism.

28. Broidy's efforts were particularly prominent in 2017. On May 23, 2017, the Foundation for Defense of Democracies ("FDD") hosted a conference entitled "Qatar and the Muslim Brotherhood's Global Affiliates: New U.S. Administration Considers New Policies."

[1] https://www.motherjones.com/politics/2021/04/businessman-charged-with-foreign-lobbying-crimes-paid-for-secret-trump-white-house-mission-to-qatar/
[2] https://www.axios.com/doj-enforce-al-jazeera-foreign-agent-ruling-a5a58129-5a12-4aee-8a2b-cbfbb7d8f900.html
[3] https://www.rubio.senate.gov/public/index.cfm/2020/8/rubio-and-zeldin-lead-members-of-congress-in-urging-al-jazeera-s-registration-under-fara

29. The speakers at the conference repeatedly argued that Qatar was a state-sponsor of terrorism and that the U.S. should undertake efforts to combat it. For example, Jake Sullivan (the current National Security Advisor) stated that, "we are not placing a high enough priority on the national security threats to the United States that is [sic] emanating from the financing of terror groups by Qatar and other countries. And we have to be doing more on that."

30. Broidy partly financed the FDD's conference.

31. Five months later, on October 23, 2017, the Hudson Institute hosted a similar conference entitled "Countering Violent Extremism: Qatar, Iran, and the Muslim Brotherhood."

32. Like the speakers at the FDD's conference earlier in the year, the speakers at the Hudson Institute's conference strongly condemned Qatar's sponsorship of terrorism and argued for policy changes.

33. Broidy partially financed the Hudson Institute's conference.

34. Broidy also supported President Trump's 2016 political campaign, and once Trump took office in January 2017, Broidy continued voicing his strong concerns about Qatar at the highest levels of the U.S. government.

35. Around the same time, President Trump, with whom Broidy had discussed Qatar, criticized the country as "a funder of terrorism at a very high level" and made comments in support of an embargo. President Trump also publicly denounced Qatar through a tweet and during a Republican National Committee meeting in 2017.

36. During that same month, Qatar's Middle Eastern neighbors were equally unnerved by Qatar's support for terrorist organizations. Saudi Arabia, the UAE, Egypt, Bahrain, and Yemen

announced that they were cutting off diplomatic relations with Qatar, and blocking all land, air, and sea travel to and from Qatar.[4]

37. One of Qatar's top D.C. lobbyists, Nicolas Muzin, had also identified Broidy to the Qatari Embassy as an impediment to Qatar's foreign policy interests in the United States. Muzin has signed FARA filings on behalf of his company, Stonington Strategies LLC, which is a registered foreign agent of Qatar. Plaintiffs sued Muzin separately in the U.S. District Court for the District of Columbia, captioned *Broidy Capital Management, et al. v. Nicholas D. Muzin, et al*, No. 1:19-cv-0150 (DLF). Muzin's motion to dismiss in that litigation was denied in part by the district court, and the case is currently on appeal in the D.C. Circuit Court of Appeals.

38. In light of all this, Qatar viewed Broidy as a serious threat to its international standing and, more specifically, to its relationship with the U.S., both of which Qatar feared could ultimately result in the tiny emirate losing some or all of its hosting privileges for the 2022 World Cup. Qatar therefore had a strong incentive to silence Broidy, so as to prevent further criticism and what it considered to be unfavorable changes to U.S. policy.

B. To Help Neutralize the Threat, Qatar Reached Out to Its Longtime Business Associate, Kevin Chalker.

39. As a result of the above, Qatar had motive to neutralize a powerful and high-profile U.S. businessman in Broidy. But it needed to do so in a clandestine and covert manner to maintain deniability and avoid any official connection to the misconduct.

40. Qatar, Chalker, and GRA had, at the time, an existing business relationship related to denigrating Qatar's critics in order to enhance the wealthy emirate's image and standing in the U.S. and elsewhere more generally. According to former GRA personnel, these denigration

[4] Anne Barnard & David D. Kirkpatrick, *5 Arab Nations Move to Isolate Qatar, Putting the U.S. in a Bind*, N.Y. Times (June 5, 2017), https://www.nytimes.com/2017/06/05/world/middleeast/qatar-saudi-arabia-egypt-bahrain-united-arab-emirates.html

campaigns were executed in large part by utilizing tradecraft and other clandestine skills that Chalker and various GRA employees acquired while working for the CIA or other arms of the U.S. government.

41. Indeed, Chalker, through GRA and its affiliated entities, had received tens of millions of dollars for such work.

42. As a result, GRA was perfectly suited to be engaged by Qatar in an effort to discredit and silence Broidy, thereby neutralizing the effect of his criticisms of Qatar.

i. GRA markets its cybersecurity skills as though it is a legitimate consulting firm, even though it only made money through its "special projects" for Qatar.

43. GRA's website says that the company provides "the highest caliber of security products and advisory services to governments and multinational corporations worldwide."

44. Chalker describes his company as "an international strategic consultancy specializing in cybersecurity, military and law enforcement training, and intelligence-based advisory services."

45. Despite marketing itself as a consultant and government contractor, GRA's only meaningful revenue came from so-called "special projects" for the State of Qatar, according to former GRA employees.

ii. GRA's personnel are hand-picked from the special ops and intelligence communities and are more than capable of covert hacking.

46. GRA is comprised of former intelligence, national security and military personnel trained in all levels of deception, disinformation, and cyber warfare.

47. Founded and led by Chalker, a former CIA officer, GRA specifically employs experienced hackers from the intelligence and military communities.

48. For example, former GRA employee John Sabin was identified by the *New York Times* two months before the start of the hack of Plaintiffs as "a former hacker for the National Security Agency,"[5] and was also described as "now a director of network security at GRA Quantum."

49. That same October 2017 article ended with the implication that Sabin himself had actually already managed to circumvent some of the most advanced commercially available encryption technology, including for Gmail: "When asked if he had already circumvented physical multifactor authentication devices like Google's keys, Sabin would offer only: 'No comment.'"

50. GRA and its associates are experts in the tactical collection of hard-to-access information.

51. Indeed, GRA holds two patents related to resonant cryptography—a system Chalker co-invented as a method for the secure transmission of data across any network. The patent applications are premised on Chalker's hacking expertise. Chalker's own filings showcase his deep understanding of system vulnerabilities to "brute force attack" (cracking a password or other security feature by automated, trial-and-error mechanisms) and argues in one application that it is a "profound understatement" to say that "the current security architecture is woefully inadequate."[6] That filing further explains that "[c]omplex systems break and are compromised in complex ways rarely understood or appreciated by their naïve makers. The essence of modern day hacking is based on this principle and only grows with technical complexity . . . ."[7]

52. Chalker's patent argues that no current system is safe from well-funded hackers:

---

[5] *See* Brian X. Chen & Nicole Perlroth, How Google's Physical Keys Will Protect Your Password, N.Y. Times (Oct. 25, 2018), https://www.nytimes.com/2017/10/25/technology/personaltech/google-keys-advanced-protection-program.html. In addition, GRA's Managing Director of its London office, Roy Wilson, is a former covert officer in the CIA's clandestine service, and its former Managing Director of its Washington, DC office, Will Rankin, is a former top CIA expert on illicit finance.

[6] US Patent No. 9,660,803, col. 2 ll. 63-67, col. 3 ll. 60-62 (issued May 23, 2017).

[7] *Id*. at col. 3 ll. 3-7.

> The battle to make devices/hardware/software perfectly secure has already been lost. The signature based tools of firewalls and antivirus software have failed because they cannot predict the future profile of infections. . . . **[I]f your company is a priority target entity at all costs, say by a determined and well-funded state actor, escalating resources will be deployed to break into the network normally reserved for the hardest targets**.[8]

53. And GRA makes no secret of its ability to use this expertise offensively to penetrate computer networks. GRA has advertised on its website its expertise with "penetration testing," which refers to hacking into a network to identify its security weaknesses. The underlying skills for penetration testing can be employed offensively or defensively. If an entity has hired an outside consultant to help identify its weaknesses, it is considered a "white hat" operation that is being used defensively to help that entity shore up its security system. But if the entity did not grant that consultant permission to conduct "penetration testing" on its network, and the consultant penetrates the network anyway, it is the same skillset being used in a wholly different, and illegal, type of operation, commonly referred to as a "grey hat" or "black hat" operation.

54. GRA's current website highlights case studies involving "penetration testing" and "pioneering military training."

55. In October 2015, GRA's website more explicitly marketed "Grey Hat + Penetration Testing" that described GRA's expertise in the exact sort of hacking techniques employed against Broidy and BCM:

> GRA's Grey Hat + Pen Testing (GHPT) service is a comprehensive suite designed to evaluate an organization's perimeter, public, and private network security. We utilize advanced techniques developed from years of expertise within the US government and private sector. These experiences include penetrating the networks of America's adversaries, such as, terrorists and narcotics organizations.[9]

[8] *Id*. at col. 4 ll. 6-22 (emphasis added).
[9] http://web.archive.org/web/20151002155106/http:/globalriskadvisors.com/; http://web.archive.org/web/20150830070535/http://www.globalriskadvisors.com/wp-content/uploads/Global-Risk-Advisors-Grey-Hat-Penetration-Testing.pdf

56. And in a 2015 video promoting GRA's Grey Hat service, GRA admits to having "advanced techniques to penetrate target networks," including private sector, private networks.[10] The video states that GRA employs both common attack methods to intrude into servers and, also, "uncommon and customized attacks," including custom "spear phishing" campaigns.

57. Mandich, a former CIA officer, worked for GRA and under Chalker's direct control at all relevant times. According to former GRA personnel, Mandich's job duties included designing the "special projects" at the direction of Chalker.

58. Garcia, a former U.S. Marine, worked as GRA's chief information officer and under Chalker's direct control at all relevant times. According to former GRA personnel, Garcia assisted Chalker by destroying evidence, including electronic devices, of the Broidy hacking after Broidy initiated litigation.

59. Likewise, Courtney Chalker, acting as an agent of GRA and under his brother Kevin Chalker's direct control, destroyed evidence of the Broidy hacking, according to former GRA personnel.

60. While GRA had hackers in a number of locations, many of the GRA hackers working on this campaign were located in GRA Research's offices in Northern Virginia. GRA broadly employed many former intelligence and Special Forces personnel with offensive hacking and surveillance skills developed while in government service, with a large team in Northern Virginia that was referred to as the "Reston Group" and affiliated with GRA Research. The Reston Group was centrally involved in many "special projects" hacking and surveillance operations, including the hack-and-smear operation targeting Plaintiffs.

[10] Global Risk Advisors, *GRA GreyHat Penetration Testing Service*, You Tube (Oct. 28, 2015), https://www.youtube.com/watch?v=BLAYD64JxXQ

61. The head of the Reston Group was a former CIA official with information security expertise. Other members in the Reston Group included a software engineer formerly with the military, a former member of the Army's special operations forces, and others with prior work experience in cyberwarfare and employing disinformation in furtherance of campaigns to denigrate targeted entities. The Reston Group included one particularly trusted operative, Defendant Anthony Garcia, who was GRA's Chief Security Officer.

iii. Chalker leveraged his history with Qatar and the skills of his employees into a lucrative business relationship.

62. Chalker's relationship with Qatar dated back to his time in the CIA, according to former GRA personnel.

63. Qatari official Ali al-Thawadi, known as "Shep," is the Chief of Staff to the Qatari Emir's brother, and has long been GRA's primary contact. Shep worked with GRA on the World Cup special projects. GRA frequently provided updates to Shep regarding surveillance activities, including of American citizens.

64. According to former GRA personnel, when Abdullah Al-Thawadi (a high-ranking Qatari official) was abducted for ransom in or around 2009, his sons turned to Chalker for assistance. Chalker frequently bragged to employees and non-employees that he successfully obtained Al-Thawadi's release, thereby earning the trust of Qatari officials.

65. According to former GRA personnel, Qatar subsequently engaged GRA to assist Qatar in its efforts to secure the bid for the World Cup 2022. This and similar work were referred to as "special projects." GRA's efforts were ultimately successful, as Qatar was awarded the World Cup bid and has managed to retain it since then, despite strong criticism that was eventually silenced.

66. For years, GRA worked to help Qatar win its blatantly corrupt bid for the 2022 World Cup and then to maintain it, even when the bid was on the verge of being revoked because of growing concern with Qatar's unsavory conduct, including the use of slave labor for construction.

67. For example, a widely-covered report by Amnesty International documented slave-like labor conditions in Qatar's construction sector where workers went without pay for months on end (or sometimes without pay at all), had their passports confiscated so they could not leave the country, and were forced to live in "squalid" accommodations.[11]

68. In connection with that bid, Qatar has been credibly accused of bribery on a massive scale, offering to pay hundreds of millions of dollars to FIFA officials to secure hosting privileges.

69. Qatar's corrupt bid eventually led to the convictions or guilty pleas of over sixteen individuals,[12] and the criminal investigation is not yet over—a superseding indictment outlining additional bribery charges was filed as recently as April 2020.[13]

70. Indeed, the younger brother of the Qatari Emir, Sheikh Mohamad bin Hamad Al Thani, known as "MBH," told third parties that Qatar was indebted to Chalker for the work he had done on the World Cup.

71. Given the prior successes of GRA and Chalker in its covert work for Qatar, it only made sense that Qatar would approach Chalker about silencing Broidy when Broidy's criticism of Qatar peaked in 2017.

---

[11] Amnesty International, *The Dark Side of Migration: Spotlight on Qatar's Construction Sector Ahead of the World Cup* (Nov. 18, 2013), https://www.amnesty.org/download/Documents/16000/mde220102013en.pdf

[12] Press Release, U.S. Dep't of Justice, *Sixteen Additional FIFA Officials Indicted for Racketeering Conspiracy and Corruption* (Dec. 3, 2015), https://www.justice.gov/opa/pr/sixteen-additional-fifa-officials-indicted-racketeering-conspiracy-and-corruption.

[12] Press Release, U.S. Dep't of Justice, *Sixteen Additional FIFA Officials Indicted for Racketeering Conspiracy and Corruption* (Dec. 3, 2015), https://www.justice.gov/opa/pr/sixteen-additional-fifa-officials-indicted-racketeering-conspiracy-and-corruption.

[13] *See United States v. Webb, et al.*, No. 1:15-CR-00252 (E.D.N.Y.) (Apr. 6, 2020 Superseding Indictment).

72. At the time it won the World Cup hosting rights in 2010, and during the years that followed, Qatar's successful bid was met with enormous controversy, highlighting its precarious standing in the worldwide soccer community—a community that had never before voted to allow a Middle Eastern nation to host its premier event. Holding on to the 2022 World Cup—and the tremendous economic and reputational boost that goes along with it—was a matter of desperate national urgency.

73. In August 2012, a formal inquiry was launched to investigate Qatar's corrupt winning bid two years earlier by the International Federation of Association Football ("FIFA"), which is the global body governing competitive soccer, including the World Cup.

74. The investigation FIFA launched in 2012 documented extensive corruption, including bribery and astroturfing, utilized by Qatar to win the 2010 bid for the 2022 World Cup, and it was detailed in a 353-page report, known publicly as the "Garcia Report," based on the name of the lead investigator, former U.S. Attorney Michael J. Garcia. Even though the Garcia Report was submitted to FIFA in or around November 2014, it was not released to the public until a German news outlet in June 2017 published a leaked copy of the PDF of the full report.

75. GRA was paid handsomely by Qatar for their work supporting the corrupt World Cup 2022 Bid.

76. GRA's work for Qatar grew to expand beyond the World Cup. GRA was retained in part to target Qatar's political enemies through cyber operations and public relations, to protect Qatar's geopolitical interests. According to former GRA personnel, Qatar retained GRA to execute these larger-scale programs on its behalf and entered into consultancy arrangements with GRA worth at least $100 million, primarily for covert conduct.

77. GRA's covert cyber operations for Qatar involved a pattern of attacks against political targets involving similar fake news alerts, malicious Google login pages, email addresses designed to mimic legitimate Google security addresses, falsified two-factor authentication messages, and the use of Mail.ru to control victims' accounts.

78. As has been publicly reported in *The New York Times* and other media outlets, forensic evidence indicates that Qatar, and therefore GRA, were likely involved in targeting over 1,000 people and entities via cyberattacks similar to those deployed against Plaintiffs here, including prominent officials from countries like Egypt and the UAE, and the United States, including an American political columnist and activist, Rabbi Shmuley Boteach, all of whom are known as outspoken critics of Qatar.[14]

79. One of the targeting projects was highly successful and has particular salience here: GRA's hacking and surveillance of the UAE Ambassador to the United States. In or around April and May 2017, approximately a half-year before it attacked Broidy, GRA conducted similar cyberattacks against the UAE Ambassador, who has extensive interactions with politically active Americans in an effort to improve Qatar's image with the United States by not only discrediting him, but also intimidating (and ultimately silencing) U.S. government officials and other Americans who were either critics or potential critics of Qatar.

80. As with Broidy, hacked emails were disseminated to the media by an anonymous "source" identified only by an alias— "GlobalLeaks"—in an effort to embarrass not just the primary target, but also politically active associates, ultimately silencing active critics and preventing others from voicing their own criticisms.

[14] *See* Shmuley Boteach, "Qatar's War to Destroy Pro-Israel Jews," Jerusalem Post, Oct. 8, 2018, https://www.jpost.com/Opinion/Qatars-war-to-destroy-pro-Israel-Jews-568942; Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," Bloomberg, Sept. 18, 2018, https:/www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-onesto-worry-about.

81. Mandich was the mastermind behind the Global Leaks operation, overseeing the execution of every phase of the operation. On information and belief, John Sabin and Defendants Garcia and Kevin Chalker also worked with Mandich in carrying out the Global Leaks campaign.

82. In June 2017, *The Huffington Post* wrote one of the first stories under the headline "Someone Is Using These Leaked Emails To Embarrass Washington's Most Powerful Ambassador."[15] The article stated that, "In private correspondence, [UAE Ambassador] Otaiba—an extremely, powerful figure in Washington, D.C., who is reportedly in 'in almost constant phone and email contact' with Jared Kushner."

83. Another article, published in *The Intercept*, was titled "Diplomatic Underground: The Sordid Double Life of Washington's Most Powerful Ambassador,"[16] and was clearly designed to embarrass the UAE Ambassador. The article relied on hacked emails, and notes that the emails "began to dribble out just as a geopolitical row between the UAE and its neighbors in Qatar came to a head."

84. An article in *The New York Times*, based on hacked emails was likewise intended to embarrass the UAE. The article states: "Anonymous hackers have provided a long series of leaked emails from Ambassador Yousef al-Otaiba's Hotmail account to The New York Times and other news organizations over the past two years in an apparent campaign to embarrass the U.A.E. and benefit Qatar."[17]

85. There are striking similarities to the attack on Elliott Broidy. Both operations relied on producing highly curated and specifically-themed PDFs, which were disseminated to some of

[15] Akbar Shahid Ahmed, *Someone Is Using These Leaked Emails To Embarrass Washington's Most Powerful Ambassador*, The Huffington Post (June 3. 2017).
[16] Ryan Grim, Diplomatic Underground: The Sordid Double Life of Washington's Most Powerful Ambassador, *The Intercept* (Aug. 30, 2017).
[17] David D. Kirkpatrick, *Persian Gulf Rivals Competed to Host Taliban, Leaked Emails Show*, N.Y. Times (July 31, 2017).

the same friendly reporters, including Ryan Grim (*The Intercept*), Bradley Hope (*The Wall Street Journal*), and David Kirkpatrick (*The New York Times*), with stories based on hacked materials still being published well over a year after the publication of the first such article. There are no publicly-known other similar campaigns that disseminated hacked materials via curated, themed PDFs, let alone over many months to those same reporters. Additionally, Howard was among the public relations professionals pitching stories based on the hacked material, just as he would later do with the Broidy hack. And the execution of the two attacks included several tactics in common, such as: (I) use of messages from Gmail accounts that appeared to be official; (2) messages that displayed a correct but redacted phone number for the victim; (3) deployment of evasion tactics to help bypass automatic spam filter and other security alerts; (4) use of private registration services and "throw away accounts" from the Mail.Ru group; and (5) maintenance of multiple phishing sites but hosting them on their own dedicated servers, using different subdomains for different campaigns.

86. Indeed, the similarities were lost on no one. The BBC quoted an unnamed "source familiar" with the hack as saying that the Broidy attack was "rinse and repeat on Otaiba."[18]

87. Moreover, the UAE Ambassador hack was successful in silencing certain critics of Qatar. For example, the Foundation for the Defense of Democracies (FDD) had consistently criticized Qatar's support for Islamic extremism and terrorism. On May 23, 2017, FDD hosted (with Plaintiffs' involvement) a conference largely focused on exposing Qatar's misdeeds. Less than a week later, after learning that their communications had been intercepted in the UAE Ambassador hack, FDD executive director Mark Dubowitz informed Mr. Broidy that the think tank would no longer publicly criticize the wealthy emirate because they feared potential Qatari

[18] Suzanne Kianpour, Emails show UAE-linked effort against Tillerson (Mar. 5, 2018). https://www.bbc.com/news/world-us-canada-43281519

reprisal. Two months later, the only FDD scholar whose work had substantially focused on Qatar left the think tank, and no one was hired or reassigned to replace his work relating to Qatar.

88. GRA's numerous cyberattacks have extended over several years and represent a pattern of unlawfully accessing victims' computer systems to extract private information or other items of value with which to attack or damage the enemies of its clients, typically for the purpose of silencing criticisms of Qatar's support for terrorist groups or its abysmal record on human rights.

89. In addition to cyberattacks in which information was stolen. Qatar has used unlawful and unauthorized access to computer systems to plant documents that would appear to incriminate their purported enemies.

90. These cyberattacks are all part of the pattern of racketeering activity in which the Enterprise conspirators have engaged with the common purpose of silencing critics of Qatar.

91. GRA's work for Qatar extended well beyond the World Cup. Even though Qatar had gained notoriety in the years following its successful 2010 bid to host the 2022 World Cup as a high-tech "dirty tricks" operator engaged in astroturfing and hacking, Qatar lacked the internal capability to carry out sophisticated hacking and surveillance operations. This void in Qatar's capabilities was why the tiny emirate paid GRA Defendants millions of dollars in and around 2018 to conduct "Operation Deviant," whose primary purpose was teaching members of Qatar's Special Forces and Intelligence services both defensive and *offensive* cybersecurity skills, including advanced, sophisticated skills that trained former U.S. intelligence and military operatives are typically barred from sharing or conferring unto foreign governments. According to former GRA personnel, Chalker and GRA routinely ignored U.S. legal requirements to obtain International Traffic in Arms Regulations (ITAR) and other regulatory approvals, despite the lifetime ban on former CIA agents conferring tradecraft knowledge and skills to foreign

governments. Chalker divulged classified information on tradecraft, as well as sensitive equipment and dual-use technology to the Qataris in support of this illicit work. According to former GRA personnel, these disclosures harmed U.S. national security by helping enhance the covert, illicit capabilities of a known supporter of terrorist groups, including al Qaeda and Hezbollah.

92. In the years immediately following Qatar's winning World Cup bid, GRA's role with the wealthy emirate grew to encompass protecting Qatar's geopolitical interests primarily by planning and executing covert operations to target Qatar's political enemies through cyber operations and public relations. According to former GRA personnel, Qatar retained GRA to execute these larger-scale programs on its behalf and entered into consultancy arrangements with GRA worth at least $100 million, primarily for covert conduct.

93. Phone records show that in the weeks leading up to the Broidy hacks, Shep had multiple calls with Joey Allaham—one of the public relations officials who was involved in the media dissemination and use of the Broidy hacked materials.

94. Tarek Hashem, Shep's senior adviser, acted as Shep's "eyes and ears" to ensure the progress of the hack-and-smear campaign and to relay information between GRA and Qatar.

C. GRA Hacks BCM's Server, Resulting in Thousands of Malicious Connections to Broidy's Email Accounts.

95. Beginning in December 2017, Broidy's family and associates began receiving spear phishing emails.

96. The GRA Defendants first targeted people who were close to Broidy—including his wife and his executive assistant—to obtain their respective log-in credentials to BCM's private server where the confidential documents were stored.

97. "Spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons."[19]

98. On December 27, 2017, four spear phishing emails were sent to Broidy's wife, Robin Rosenzweig, and a Broidy Associate. In the following week, Rosenzweig and the Broidy Associate received at least another dozen spear phishing emails.

99. Chalker celebrated the launch of the spear phishing campaign that very night, on Wednesday, December 27, 2017, by taking associates to the Sapphire Gentlemen's club in New York City.

100. The emails were disguised to appear as though they were Google security alerts, and they asked the Broidy Associate and Rosenzweig to enter their Gmail login credentials into a malicious link embedded in the emails. Unfortunately, Rosenzweig unwittingly complied.

101. The link in the spear phishing email was designed to appear as if it would direct Ms. Rosenzweig to a legitimate URL on Google.com, but (not readily apparent without viewing the underlying source code) the link was in fact a TinyURL link that directed her to a professionally designed website that was intended to trick victims into believing it was actually an authentic Google account login page. TinyURL is a redirecting service that provides shortened URLs that redirect a website visitor to the website associated with the longer, masked URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. When Rosenzweig clicked the TinyURL link, she was redirected to a website that contained Google's logo and appeared to be an authentic Google account update page—but it was in fact a fraudulent login page.

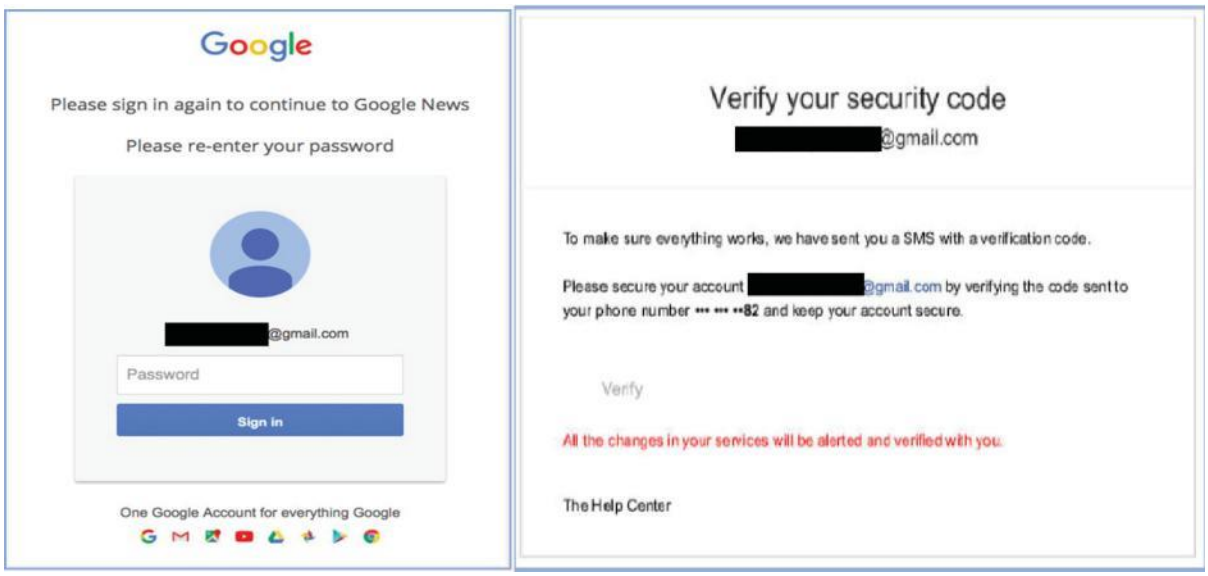
[19] *See* https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

102. On or about January 3, 2018, the GRA Defendants used the "Mail.ru" service to access and modify Ms. Rosenzweig's Gmail account without her consent. "Mail.ru" signifies a Russian email service that publishes an app that can be operated by users physically located around the world, including in the United States, to send and receive emails on Mail.ru or other email services like Gmail. Here, the GRA Defendants used the "Mail.ru" to read, send, delete, and manage emails and other documents in Ms. Rosenzweig's Gmail account, without her knowledge or consent, which in turn enabled them to obtain her log-in credentials for the BCM server.

103. Indeed, the GRA Defendants even modified Ms. Rosenzweig's account settings so as to keep her from discovering that her email had been hacked. They arranged for emails containing "Mail.ru," "viewed," or "alert" to be marked as read and moved immediately to her trash folder. The GRA Defendants did this to ensure that any legitimate security alerts would not be viewed by Ms. Rosenzweig. And unbeknownst to Ms. Rosenzweig, on January 4, 2018, she received a true security alert—that went directly to her trash folder—notifying her that a user or users of the Mail.ru app had obtained access to read, send, delete, and manage her Gmail account, all without her awareness or consent.

104. On January 14, 2018, another Broidy associate, Erica Hilliard ("Hilliard"), received two spear phishing emails, which were similarly disguised to look like security alerts from Google. Like her colleagues, Hilliard unwittingly entered her Gmail login credentials, thereby compromising her account.

105. Examples of the highly sophisticated spear phishing emails are shown below:



106. Without authorization, Defendants logged into Rosenzweig's Gmail account on January 4, 7, 9, and 17, and they logged into Hilliard's Gmail account on January 14, 15, 16, and 17.

107. By accessing the Gmail accounts of Rosenzweig and Hilliard, Defendants obtained the login credentials for the Gmail account of another BCM employee, Jenna Pressley Caganap and used those credentials to access Caganap's Gmail account on January 4.

108. Through the Gmail accounts of Rosenzweig, Hilliard, and/or Caganap, Defendants obtained the login credentials for several BCM email accounts.

109. On January 16, Defendants accessed the BCM server, without authorization, through the BCM email accounts of Broidy, Caganap, and Hilliard, as well as other BCM employees Michelle Levi, James Sexton, and Jessica Stephens.

110. BCM has an exchange server physically located in Los Angeles, California, that is connected to the internet and used to engage in commerce and communications throughout the country. The server allows BCM employees to send and receive business and occasional personal emails. Broidy and other employees, including those identified in the preceding paragraph, have

secure email accounts on the BCM server containing private communications that require at least a username and password for access.

111. From January 16 to February 25, 2018, BCM's server was subjected to approximately 325,000 malicious connections from 59 unique internet protocol ("IP") addresses.

112. Two of these connections were traced to a single IP address in Qatar. Eight of the connections were traced to an IP address belonging to a hotel in Killington, Vermont. Four of the connections were traced to an IP address belonging to an acupuncture business in Wallingford, Vermont.

113. The remaining hundreds of thousands of connections were disguised by VPNs and are untraceable.

114. During these attacks, numerous email communications and documents were viewed, stolen, and/or altered without authorization. These included, among other things, Broidy's personal emails and documents, contacts file, business calendar, business emails and documents, signed contracts, attorney-client privileged communications and documents, attorney-client work product, usernames, and passwords to access other non-Google accounts, including email accounts on the computer network of BCM, including Broidy's corporate email account, financial information, and confidential business process and methods information. The server also contained corporate and personal documents, copyrighted material, contracts, business plans, and other confidential and sensitive proprietary information, to which Defendants had full access.

115. Broidy filed a lawsuit shortly after the hacking occurred. The lawsuit triggered a panic within GRA, which was eager to destroy the evidence inculpating it in the hacking scheme. Kevin Chalker instructed GRA's Chief Security Officers, also a GRA Research hacker in the Reston Group, Anthony Garcia, to wipe GRA's computers, phones and other devices clean of any

damaging evidence. Garcia not only complied with that instruction, but he removed certain hard drives, phones and devices with incriminating evidence from GRA's offices, and brought them to a remote location, where the devices were destroyed and ultimately discarded. Courtney Chalker knowingly assisted Garcia with the destruction of evidence.

D. Former GRA Employees and Associates Confirmed That Chalker and GRA Were Responsible for the Hack-and-Smear of Broidy and BCM.

116. Chalker told GRA personnel that Chalker and GRA were responsible for the hack-and-smear operation targeting Broidy/BCM.

117. Chalker also told GRA personnel that Chalker, Garcia, and Courtney Chalker had destroyed electronic devices and other materials containing evidence of the Broidy/BCM hacking as soon as this litigation was filed. This was done to conceal the role of GRA and Kevin Chalker in the hacking.

118. In addition to the hacking, Chalker and GRA also directed the electronic and physical surveillance of Broidy, according to former GRA personnel.

119. Attached as Exhibit A is a declaration from a former GRA employee attesting to well-founded knowledge of GRA's involvement in the Broidy / BCM hack-and-smear operation. The declaration is anonymous to protect the security and safety of this whistleblower from retaliation from Defendants. Defendants have a history of threatening former employees. Plaintiffs have also offered to submit to the Court for *in camera* review a copy of the original, signed declaration for the Court to verify the signature and the identity of the declarant. In addition, undersigned counsel have interviewed other former GRA employees and can attest to his credibility as to the statements made in the declaration.

E. In the Months Leading up to the Hack-and-Smear Operation, Chalker's Off-Shore Companies Received Massive Payments from Qatar.

120. According to information provided by former GRA personnel, Qatar paid Chalker through three off-shore entities, Bernoulli Limited ("Bernoulli"), Toccum Limited ("Toccum"), and GRA EMEA, all of which are based in Gibraltar. This was done to maintain the clandestine nature of the operations and avoid the appearance of any official connection between Qatar and GRA.

121. During all relevant times, Chalker owned and controlled Bernoulli, Toccum, and GRA EMEA.

122. Indeed, the connection between GRA and the three off-shore entities is shown in the New York Department of State's records.

Selected Entity Name: BERNOULLI LIMITED

Selected Entity Status Information

Current Entity Name: BERNOULLI LIMITED
DOS ID #: 5419853
Initial DOS Filing Date: OCTOBER 03, 2018
County: NEW YORK
Jurisdiction: ALL OTHERS
Entity Type: FOREIGN BUSINESS CORPORATION
Current Entity Status: ACTIVE

Selected Entity Address Information

DOS Process (Address to which DOS will mail process if accepted on behalf of the entity)
GLOBAL RISK ADVISORS LLC
ONE WORLD TRADE CENTER
83RD FLOOR
NEW YORK, NEW YORK, 10007

Registered Agent
NONE

Selected Entity Name: TOCCUM LIMITED

Selected Entity Status Information

Current Entity Name: TOCCUM LIMITED
DOS ID #: 5419846
Initial DOS Filing Date: OCTOBER 03, 2018
County: NEW YORK
Jurisdiction: ALL OTHERS
Entity Type: FOREIGN BUSINESS CORPORATION
Current Entity Status: ACTIVE

Selected Entity Address Information

DOS Process (Address to which DOS will mail process if accepted on behalf of the entity)
GLOBAL RISK ADVISORS LLC
ONE WORLD TRADE CENTER
83RD FLOOR
NEW YORK, NEW YORK, 10007

Registered Agent
NONE

Selected Entity Name: GLOBAL RISK ADVISORS EMEA LIMITED

Selected Entity Status Information

Current Entity Name: GLOBAL RISK ADVISORS EMEA LIMITED
DOS ID #: 5455345
Initial DOS Filing Date: DECEMBER 07, 2018
County: NEW YORK
Jurisdiction: ALL OTHERS
Entity Type: FOREIGN BUSINESS CORPORATION
Current Entity Status: ACTIVE

Selected Entity Address Information

DOS Process (Address to which DOS will mail process if accepted on behalf of the entity)
GLOBAL RISK ADVISORS LLC
ONE WORLD TRADE CENTER,
83RD FLOOR
NEW YORK, NEW YORK, 10007

Registered Agent
NONE

123. The publicly available financial statements for Bernoulli, Toccum, and GRA EMEA further show that they received combined payments approximately totaling at least $30 million in the months leading up to the launch of the hack-and-smear operation in December 2017.

Bernoulli Limited

Registered Number: 107153

REGISTRY OF COMPANIES GIBRALTAR 7th November 2018

BALANCE SHEET as at 31 December 2017

	31-Dec-17 USD	31-Dec-16 USD
FIXED ASSETS	-	-
CURRENT ASSETS		
Debtors due within one year	1,212,194	8,100,148
Cash at Bank and in Hand	21,156,490	13,586,133
	22,368,684	21,686,281

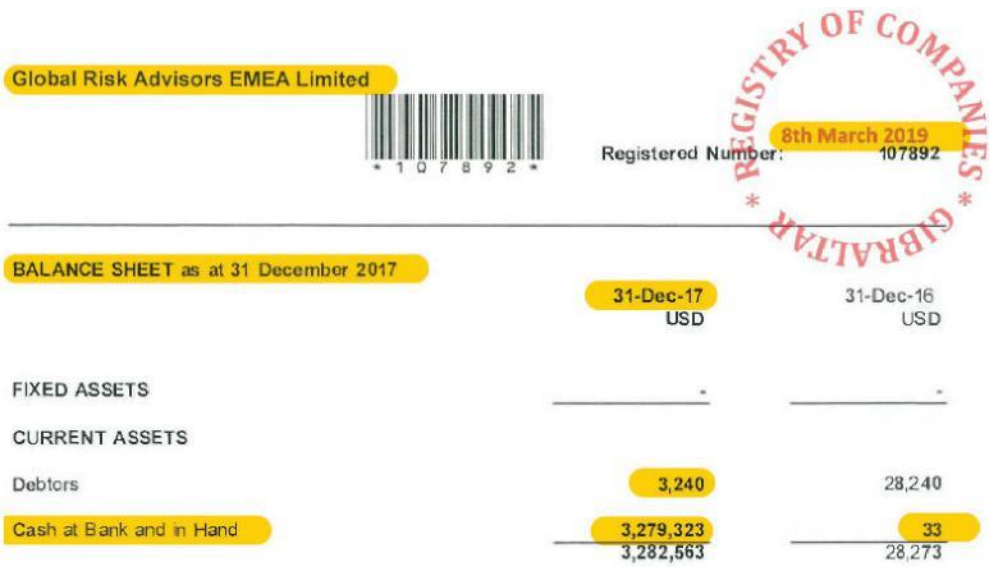
Toccum Limited

Registered Number: 108685

REGISTRY OF COMPANIES GIBRALTAR 8th March 2019

BALANCE SHEET as at 31 December 2017

	31-Dec-17 USD	31-Dec-16 USD
FIXED ASSETS	-	-
CURRENT ASSETS		
Debtors	45,213	45,473
Cash at Bank and in Hand	18,602,095	29
	18,647,308	45,502



Global Risk Advisors EMEA Limited

* 1 0 7 8 9 2 *

REGISTRY OF COMPANIES GIBRALTAR

8th March 2019

Registered Number: 107892

BALANCE SHEET as at 31 December 2017

	31-Dec-17 USD	31-Dec-16 USD
FIXED ASSETS	-	-
CURRENT ASSETS		
Debtors	3,240	28,240
Cash at Bank and in Hand	3,279,323	33
	3,282,563	28,273

124. According to former GRA personnel, who had knowledge of GRA's finances, this money was paid by Qatar, which was GRA's only meaningful client and source of overseas funds.

125. Also according to former GRA personnel, GRA held weekly status meetings to track unpaid invoices. The invoices were not related to the work that GRA held itself out as doing for Qatar, i.e. standing up an intel fusion center in Doha. During these same conversations, GRA employees discussed GRA conducting "dark" operations for Qatar.

126. Another GRA employee, Dan Emory, who was also involved in the "special projects," was responsible for getting the invoices paid by Ali al-Thawadi—the Chief of Staff to MBH, the Qatari Emir's younger brother.

F. To Complete Their Plan of Silencing Broidy's Criticisms, Defendants Provided the Hacked Materials to Media Outlets That Published Salacious Stories.

127. Qatar's objective to effectively stifle Broidy's First Amendment freedoms was not complete until the materials stolen by GRA and Chalker could be twisted and publicized to smear Broidy's reputation.

128. Thus, after the hacking was completed and the materials had been stolen from Broidy and BCM, Defendants carefully packaged the hacked materials into a series of PDFs, each

with a unique theme designed to inflict maximum damage through highly precise curation and alteration, then leaked those PDF files to the media, with the help of third parties.

129. The PR strategist members used by Qatar include, among others, Nicholas Muzin, Joseph Allaham, Gregory Howard, Ahmad Nimeh, BlueFort Public Relations LLC, Spark Digital, Stonington Strategies, and Lexington Strategies.

130. Through all times relevant to this Second Amended Complaint, Nicolas D. Muzin was the Chief Executive Officer of Stonington Strategies LLC, a public relations and lobbying firm incorporated under the laws of Delaware, and a political lobbyist who signed FARA documents on behalf of Stonington as a registered foreign agent for the State of Qatar. On August 24, 2017, he was officially retained by the State of Qatar for "consulting services," and on September 3, 2017, Stonington registered under FARA as a foreign agent providing "strategic communications" for the State of Qatar. Stonington Strategies has been reorganized into Stonington Global LLC, whose website states that "[i]n launching the new firm, Nick Muzin & his team plan to build on their success representing the State of Qatar."

131. Joseph Allaham was the co-founder of Stonington Strategies, where he served as partner for all relevant times. He has worked for Qatar, originally as an unregistered foreign agent until he eventually filed a registration statement under FARA on June 15, 2018, in response to a subpoena from Plaintiffs in a related action. He is also the CEO of Lexington Strategies.

132. Gregory Howard is a media placement expert, an agent who, through his relationships with members of the media, provides information and materials to the media to generate stories desired by the agent's client. In 2017 and 2018, Howard worked as a Vice President and Senior Media Strategist at the firm of Conover & Gould ("Conover"), based in Washington, DC. From July 2017 until January 18, 2018, Howard was a registered foreign agent

of Qatar through Conover, but continued working for months afterwards placing stories in the media based on Broidy's hacked materials, despite terminating his status as a registered agent of Qatar. Beginning no later than May 10, 2018, Howard worked in Washington, DC, as Vice President of Mercury Public Affairs, a public strategy firm, which he left in April 2019. In each of his positions at Mercury, despite FARA filings that did not mention Qatar, Howard worked as a media placement strategist for Qatar.

133. Qatar specifically retained Messrs. Muzin, Allaham, and Howard in an attempt to influence the Republican, American-Jewish community and other conservative supporters of the President, with the end goal of influencing White House policy. Their work included identifying Broidy and other Americans as critics to be silenced.

134. Muzin began working for Qatar sometime in 2017, and in late August of that year, the Qatari Embassy in Washington, DC, officially retained Stonington and Muzin to influence public opinion regarding Qatar. Their agreement specified that Muzin and Stonington were to provide "consulting services" including the "development and implementation of a government relations strategy for Qatar, as requested and directed by the Embassy." The initial agreement that Muzin submitted to the U.S. Department of Justice provided that Qatar would pay Muzin and Stonington Strategies $50,000 a month for these services.

135. The initial agreement further limited Muzin and Stonington Strategies from acting as "a representative, spokesperson or agent on behalf of the Embassy or the State of Qatar in any meeting or communication with any person, or in any public or private statement, or in any communications with the media" "[e]xcept as directed by the Embassy."

136. Allaham also began working for Qatar in 2017, according to his initial FARA disclosures in his capacity as the CEO of Lexington Strategies.[20] According to his (subsequently filed) FARA registration, he worked directly for the Emir of Qatar, Sheikh Tamim bin Hamad Al Thani, and his brother Sheikh Mohamad bin Hamad Al Thani (the Emir's brother is commonly referred to as "MBH") Allaham's FARA filing listed MBH's chief of staff, Ali Al-Thawadi, as his official point of contact responsible for overseeing his work on behalf of Qatar—meaning his supervisor in the chain of command was the same as for the GRA Defendants. GRA worked with these same individuals and referred to them for purposes of their covert operations by code names.

137. In the fall of 2017, in the weeks leading up to the attack, phone records show that Allaham had five separate phone calls with MBH's chief of staff, Ali al-Thawadi. GRA also worked very closely with Thawadi and gave him the code name, "Shepherd," or "Shep," for short.

138. Also working in fall of 2017 with both GRA and the DC Defendants was Ahmad Nimeh, the person behind "Blue Fort PR," the firm that paid Muzin and Allaham at least $3.9 million in a span of three weeks from mid-September through early October 2017.

139. Nimeh was someone with whom GRA worked closely, to the extent that GRA gave him the code name "Botany." Nimeh is the principal of a company that worked alongside GRA on the World Cup projects and who was publicly reported to be part of the Qatar "black ops" team hired to undermine rival bidders (including the eventual runner-up, the United States). According to both reporting in the *Sunday Times of London* and someone who has seen Nimeh's communications from during and around 2010, Nimeh worked with PR agents, as well as Chalker, in furtherance of Qatar's "dirty tricks" operations—and Nimeh did so under the direct supervision of Ali Al-Thawadi, aka "Shep."

[20] https://efile.fara.gov/docs/6563-Registration-Statement-20180615-2.pdf

140. On or around September 17, 2017, Chalker met with Shep and Hashem in New York City. Shortly thereafter, Chalker flew to Doha in the first week of October 2017 to have a follow-up meeting with Shep and Hashem. These meetings Chalker had with Shep and Hashem coincided with Blue Fort PR's two payments of $1.95 million each to Muzin on September 18 and October 10, 2017, as well as Qatar's payment of $1.45 million in "October 2017" to Allaham.

141. Chalker flew again to Doha to meet with "Shep" and Hashem during the first week of February 2018, right around the halfway point of the hacking phase of the hack-and-smear operation.

142. Muzin has admitted that he identified and described Broidy to the Qatari government as impediments to Qatar's foreign policy interests in the United States. In connection with his work for Qatar, Muzin or his employees or agents participated in weekly meetings at the Qatari Embassy in Washington, DC, where they discussed with Qatari officials and other Qatari agents the ongoing efforts against Broidy. Muzin specifically mentioned Broidy in these meetings as an obstacle that needed to be dealt with for his lobbying on behalf of Qatar to succeed.

143. As plans for the upcoming hack were underway, increased payments flowed to these key public relations strategists. On December 15, 2017, shortly before the hacks on Plaintiffs' computers began, Qatar gave a $500,000 balloon payment to Messrs. Muzin and Allaham's firm, Stonington Strategies, and increased the monthly retainer from $50,000 to $300,000.[21]

i. Qatari Public Relations Contractors Push Certain Reporters to Publish Damaging Stories Based on Hacked Materials

144. Howard's phone calls following the hacking show that he was in close and frequent communication with journalists in the early months of 2018 before those same reporters began publishing stories that relied on information stolen from Plaintiffs' computer systems and servers.

[21] https://efile.fara.gov/docs/6458-Exhibit-AB-20171221-2.pdf

In some instances, Howard communicated with journalists for weeks before they published these articles. The intensity of those contacts often increased in the days prior to publication. During this same period, Howard closely communicated with public relations experts, research groups, and registered agents of Qatar to coordinate the media disinformation campaign against Broidy.

145. Starting on January 7, 2018, just hours after the first sustained hacker access of Ms. Rosenzweig's Gmail account (and thus hundreds of Plaintiffs' confidential documents), Howard engaged in a flurry of calls with his then-colleagues at Conover & Gould and outside public relations professionals, as well as exchanging five phone calls with Amb. Patrick Theros, who is Nimeh's father-in-law and business partner. In the half-year before January 7, 2018, Howard's phone records indicate no calls or text messages with Theros.

146. From January 18 through at least July of 2018, Howard participated in more than two hundred phone calls with reporters who contributed to stories regarding Broidy and Qatar or regularly covered Qatari-related issues. These included extensive, and at times, almost daily calls with now-former Associated Press ("AP") reporter Tom LoBianco, all leading up to the time he authored several stories regarding Broidy in March and May, 2018, based on the contents of Broidy's hacked emails. In addition, in the same time frame, Howard conducted more than 100 calls with the *New York Times*, *McClatchy*, the *Wall Street Journal*, and the *Washington Post*, all of which were focusing on stories regarding Broidy's hacked emails.

147. Messrs. Muzin and Allaham were in close contact with high-ranking members of the Qatari government (including GRA contacts Apex (the Emir), Mightier (MBH, the Emir's brother), and Shep (Al Thawadi) in the weeks leading up to the attack. Muzin then flew to Qatar within a few days of GRA's first successful hack into Plaintiffs' systems. Messrs. Muzin and

Allaham's text messages with each other demonstrate their direct and prior knowledge of the hacking and their knowing use of stolen documents.

148. On January 25, 2018, shortly after GRA's successful hacking of BCM began, Muzin sent Allaham a message on WhatsApp, stating, "It's very good. . . . We got the press going after Broidy. I emailed you."

149. That same day, prior to the first public reports in the United States of materials stolen from Plaintiffs, Ben Wieder, a reporter for *McClatchy*, a Washington, DC publication focused on politics, emailed Muzin to tell him, "I'm working on a story about Elliott Broidy and was hoping to talk." Muzin, who was still in Qatar, forwarded this message to Allaham and commented, "Time to rock." Less than an hour after sending the email to Muzin, Wieder called Howard, and they spoke for more than 10 minutes. Wieder would go on to write extensively about Broidy on the basis of carefully curated emails and other documents stolen from Broidy's servers.

150. On March 1, 2018, the contents of emails stolen from Plaintiffs' computer accounts and servers appeared for the first time in media accounts. The *Wall Street Journal* credited its source as "a cache of emails from Broidy's and his wife's email accounts that were provided to the Journal."

151. Muzin shared the *Wall Street Journal* article with Allaham over WhatsApp that same day. Muzin then commented, "He's finished."

152. Other media outlets continued to publish more of the stolen emails, including the *Huffington Post* on March 2, 2018, and the BBC on March 5, 2018. The Huffington Post cited "[e]mails and documents an anonymous group leaked to HuffPost."

153. On March 13, 2018, Muzin remarked to Allaham via WhatsApp that recent news stories about Broidy have "[p]ut[] him in [M]ueller[']s crosshairs." This communication

demonstrates one of the central goals of the Qatari-Funded Criminal Enterprise—to portray Broidy as a target of special counsel Robert Mueller's investigation.

154. That same day, Allaham wrote to Muzin on WhatsApp that a former U.N. official working under contract with the Qatari government, Jamal Benomar, had gone to Qatar prior to the date of the message "to get the emails. That what [*sic*] I think he was doing there [in Qatar]." Muzin responded by referencing Broidy by name.

155. On March 14, 2018, Muzin told Allaham on WhatsApp that he'd "get some intel about the Broidy event soon." This comment likely refers to a March 13, 2018, Republican fundraiser headlined by the President of the United States, for which Broidy had been listed as an event host.

156. The next day, on March 15, 2018, Muzin exclaimed to Allaham, via WhatsApp, "Elliott Broidy was not at the fundraiser!" The two were clearly excited at the prospect of having damaged Broidy's political standing.

157. Multiple additional news stories followed that expressly relied on the stolen documents. On March 21, 2018, the *New York Times* published a front-page article noting that an "anonymous group critical of Broidy's advocacy of American foreign policies in the Middle East" has been distributing "documents, which included emails, business proposals and contracts," belonging to Plaintiffs. On March 23, 2018, *Bloomberg* published an article about Broidy, which noted that it had "received two separate documents this week purporting to be versions" of materials belonging to Broidy.

158. On March 25, 2018, a front-page story in the *New York Times* reported extensively on Broidy's fundraising and business activities. The story reported that Broidy had agreed not to attend the March 13 fundraiser. The story was based, in part, on "[h]undreds of pages of Broidy's

emails, proposals and contracts" received from what the *Times* euphemistically termed "an anonymous group critical of Broidy's advocacy of American foreign policies in the Middle East." This "anonymous group" is the Qatari-Funded Criminal Enterprise.

159. On March 26, 2018, *McClatchy* published a story authored by Ben Wieder that used hacked materials to denigrate Broidy, House Foreign Affairs Chairman Ed Royce, and the Congressman's wife, Marie Royce—just four days before the Senate was scheduled to vote on her appointment to be Assistant Secretary of State for Educational and Cultural Affairs. Also at that time, Chairman Royce's House Foreign Affairs Committee was attempting to advance H.R. 2712, known as the "Hamas Sanctions Bill," which specifically named Qatar as a sponsor of Hamas subject to sanctions. It was only one of a series of articles hostile to Broidy authored by Wieder following contact with Muzin and Howard, who also had extensive communications with Wieder's editor, Viveca Novak.

160. And on May 4, 2018, in a WhatsApp message to Allaham, Muzin summed up the very obvious objective the Enterprise had pursued for months, stating: "our new friends can make Broidy go away altogether."

161. Media outlets in the United States and abroad threatened to publish—and continued to publish—materials stolen from Plaintiffs well into 2019.

162. GRA's extensive hacking and packaging of curated PDFs with hacked materials, as well as its intentional coordination with public relations professionals, ensured that the Enterprise inflicted maximum damage on Broidy and BCM.

ii. Misleading and Malicious News Articles based on the Stolen Materials Damage Plaintiffs.

163. As an example, one news article using the hacked materials appeared on March 1, 2018, in *The Wall Street Journal*, and was titled "Trump Ally Was in Talks to Earn Millions in

Effort to End 1MDB Probe in U.S. Emails indicate Republican donor and wife were negotiating fee if the Justice Department closed its investigation."

164. A deluge of articles followed, as demonstrated by these examples:

a. 3/2/18 – *Huffington Post*, "Leaked Emails Appear to Show a Top Trump Fundraiser Abusing His Power"

b. 3/3/18 – *The New York Times*, "Mueller's Focus on Adviser to Emirates Suggests Broader . . ."

c. 3/5/18 – *BBC News*, "Emails Show UAE-Linked Effort Against Tillerson"

d. 3/5/18 – *The New York Times*, "A Top Trump Fund-Raiser Says Qatar Hacked His Email"

e. 3/6/18 – *Bloomberg*, "Trump Fundraiser's Email Breach Shows Risks Before Midterms"

f. 3/9/18 – *Huffington Post*, "Leaked Memo"

g. 3/12/18 – *Hollywood Reporter*, "Mueller Probe Expands to Hollywood as Trump Arrives . . ."

h. 3/21/18 – *The New York Times*, "How 2 Gulf Monarchies Sought to Influence the White House"

i. 3/23/18 – *Bloomberg*, "Trump Fundraiser Offered to Help Lift Sanctions on Russian Firms"

j. 3/29/18 – *Newsweek*, "Top Trump Fundraiser Helped Congressman's Wife Land State Department Job"

165. The *Huffington Post*'s March 2, 2018 article expressly stated that it was based on "[e]mails and documents an anonymous group leaked." The same article also included a screenshot of what purported to be a leaked email.

166. Similarly, the *BBC News* article from March 5, 2018 admitted that "BBC has obtained leaked emails" from Broidy.

167. Additionally, *The New York Times* article from March 5, 2018 made assertions based on "three sets of documents that appear to have been hacked from Broidy's personal email."

G. Although the Hack-and-Smear Campaign Did Not Silence Broidy, It Caused Broidy and BCM to Suffer Significant Harm and Business Losses.

168. The hack-and-smear campaign by GRA and Chalker did not accomplish its primary objective of silencing Broidy, whose opposition to Qatar's support for terrorism is now stronger than ever.

169. Nonetheless, the unlawful and tortious conduct of GRA and Chalker has caused Broidy and BCM to suffer significant economic losses in the form of lost business relationships and lost contracts.

170. For example, BCM lost out on contract opportunities with at least two foreign governments as a direct result of the hacked materials being disseminated.

171. Broidy personally has been damaged in his broader business affairs, as business partners and others have not wanted to associate themselves with someone who, following the press onslaught, had such high visibility as a result of being the subject of deceptive, unflattering media coverage. For example, investment and commercial banks with whom Broidy had long-term relationships suddenly ceased doing business with him, following the hacks and associated media campaign. BCM had at least one financial institution that also ceased doing business with BCM as a direct result of the hacked materials being disseminated.

172. One element of this harm is that BCM has lost significant revenue and goodwill. BCM makes investments in, among other things, privately held defense contracting companies. In the defense contracting space, discretion is very important and highly valued. The projects of BCM portfolio companies involve sensitive counterterrorism and intelligence initiatives. The work is both

highly confidential and proprietary. BCM clients rely on the company to protect information that is highly sensitive, and the fact that BCM was hacked—and that the fruits of the hack were spread through the media—has, quite predictably, caused counterparties and others to flee, and resulted in a substantial loss in business.

173. In addition to the harmful effects on Plaintiffs' business, BCM and Broidy also incurred significant losses in the form of investigating the hacks, repairing the damage to BCM's systems caused by the hacks, updating the security protocols, and installing the necessary protections to prevent GRA and Chalker from committing similar hacks in the future. These costs, which were directly caused by the hacking, amounted to hundreds of thousands of dollars paid out by Broidy and BCM.

CLAIM I
Violation of the Stored Communications Act, 18 U.S.C. § 2701, et seq.
(GRA and Chalker)

174. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

175. The Stored Communications Act ("SCA") imposes criminal penalties on "whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided. . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a).

176. The SCA also provides that "a person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity" damages, along with equitable and declaratory relief. *Id.* § 2707.

177. Broidy and BCM are "persons" within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a).

178. GRA and Chalker are directly liable under the SCA because they directed and controlled the hacking of Plaintiffs' email servers, facilities, and computer systems.

179. GRA and Chalker willfully, flagrantly, and intentionally accessed without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, as well as Google's servers, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).

180. The cyberattack was a willful, flagrant, and intentional violation of the SCA.

181. GRA and Chalker willfully and intentionally accessed the email accounts of, at a minimum, Broidy, Caganap, Hilliard, Rosenzweig, Levi, Sexton, and Stephens by transmitting fake spear phishing emails with links to malicious websites enabling GRA and Chalker to steal the login credentials.

182. GRA and Chalker used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email accounts. Beginning on or about January 16, 2018, Defendants intentionally accessed or caused to be accessed BCM's servers without authorization, including emails and documents physically located on those servers, as well as Google servers, specifically by accessing, or causing others to access, the accounts of Broidy and other BCM employees, without authorization and obtaining emails and other items.

183. GRA and Chalker also implemented identifiable obfuscation techniques, such as VPN, to engage in efforts to hide the origin of their spear phishing attacks and unauthorized access

to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google. GRA and Chalker used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt.

184. GRA and Chalker intentionally, willfully, unlawfully, and without authorization accessed Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack.

185. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and

(f) additional harm and damages to be proven at trial.

186. GRA and Chalker intentionally and willfully caused such damage to Plaintiffs.

187. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars.

188. As provided for in 18 U.S.C. § 2707(b) & (c), Plaintiffs are entitled to an award of the greater of the actual damages suffered or the statutory damages, as well as punitive damages, attorneys' fees and other costs of this action, and appropriate equitable relief.

CLAIM II
Violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2) and (a)(5)
(All Defendants)

189. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

190. The Computer Fraud and Abuse Act ("CFAA") creates a cause of action against whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2).

191. The CFAA also creates a cause of action against whoever "(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." *Id.* § 1030(a)(5).

192. The CFAA also creates a cause of action against "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section." *Id.* § 1030(b).

193. A "protected computer" is one that "is used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).

194. BCM's computer systems and email servers are used in and affect interstate and foreign commerce or communication and are therefore "protected computers."

195. GRA and Chalker willfully and intentionally accessed the email accounts of, at a minimum, Broidy, Caganap, Hilliard, Rosenzweig, Levi, Sexton, and Stephens by transmitting fake spear phishing emails with links to malicious websites enabling GRA and Chalker to steal the login credentials.

196. GRA and Chalker are directly liable under the CFAA because they directed and controlled the hacking of Plaintiffs' email servers, facilities, and computer systems.

197. GRA and Chalker willfully and intentionally accessed Plaintiffs' computer networks and email accounts without authorization.

198. Thereafter, GRA and Chalker used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email accounts. Beginning on or about January 16, 2018, GRA and Chalker intentionally accessed or caused to be accessed BCM's servers without authorization, including emails and documents physically located on those servers, as well as Google servers, specifically by accessing, or causing others to access, the accounts of Broidy and other BCM employees, without authorization.

199. GRA and Chalker also implemented identifiable obfuscation techniques, such as VPN, to engage in efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google. GRA and Chalker used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt.

200. GRA and Chalker intentionally, willfully, unlawfully, and without authorization accessed Plaintiffs' protected computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack.

201. Defendants intentionally conspired to cause damage to BCM's protected computers through the attack.

202. They knowingly caused the transmission of a program, information, code, or command, and as a result, intentionally caused damage without authorization, to BCM's protected computers.

203. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and

(f) additional harm and damages to be proven at trial.

204. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars.

205. GRA and Chalker intentionally and willfully caused such damage to Plaintiffs.

CLAIM III
Violation of CA Comprehensive Computer Data Access & Fraud Act, Cal. Pen. Code § 502
(GRA and Chalker)

206. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

207. The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2).

208. CDAFA imposes criminal penalties on anyone who "[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network." *Id.* § 502(c)(4).

209. CDAFA imposes criminal penalties on anyone who "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of" Section 502. *Id.* § 502(c)(6).

210. CDAFA imposes criminal penalties on anyone who "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." *Id.* § 502(c)(7).

211. CDAFA imposes criminal penalties on anyone who "[k]nowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network." *Id.* § 502(c)(9).

212. CDAFA provides that "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id.* § 502(e)(1).

213. CDAFA provides for award of reasonable attorneys' fees. *Id.* § 502(e)(2).

214. GRA and Chalker are directly liable under CDAFA because they directed and controlled the hacking of Plaintiffs' email servers, facilities, and computer systems.

215. GRA and Chalker knowingly and unlawfully accessed computers, computer systems or computer networks at Plaintiff BCM and Google, all of which were located in California. GRA and Chalker knew at the time that they did not have the authorization to access Plaintiffs' computers, computer systems, and networks. This knowledge is demonstrated by their use of spear phishing attacks and attempted spear phishing attacks to disguise their intentions and obtain login credentials through fraudulent misrepresentations. The spear phishing emails imitated Google's profile in order to obtain login credentials. GRA and Chalker caused damage to Plaintiffs' electronic files and emails through their cyber intrusions.

216. GRA and Chalker knowingly and unlawfully conducted the hacking of BCM's computer systems and email servers, and are therefore directly liable under CDAFA.

217. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks; and

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information and other intellectual property. and losses associated with protecting the foregoing from future misappropriation; and

(f) additional harm and damages to be proven at trial.

218. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars. These losses include significant costs that were reasonably necessary to verify whether and how Plaintiff's computer systems and data were altered, damaged or deleted by GRA and Chalker's unlawful access.

219. GRA and Chalker's actions were willful and malicious, and Plaintiffs are entitled to punitive damages under § 502(e)(4).

CLAIM IV
Receipt and Possession of Stolen Property in Violation of Cal. Penal Code § 496
(All Defendants)

220. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

221. California law imposes criminal penalties on any "person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling or withholding any property from the owner, knowing the property to be so stolen or obtained." Cal. Penal Code § 496(a).

222. California law further provides that "[a]ny person who has been injured by a violation of [Section 496] may bring an action for three times the amount of actual damages, if any, sustained by plaintiff, costs of suit, and reasonable attorney's fees."

223. GRA and Chalker are directly liable because they directed and controlled the hacking of Plaintiffs' email servers, facilities, and computer systems located in California.

224. GRA and Chalker knowingly received property, including private communications, documents, trade secrets and intellectual property housed on Plaintiffs' and Google's servers, and in emails and documents physically located on those servers located in California.

225. This property was stolen from Plaintiffs in California or otherwise obtained from Plaintiffs in California in a manner that constitutes theft.

226. GRA and Chalker received the property knowing that it was stolen property and obtained through theft. They knowingly and intentionally concealed, sold, withheld—and aided in the concealing, selling and withholding—of Plaintiffs' stolen property.

227. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and

(f) additional harm and damages to be proven at trial.

228. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

CLAIM V
Intrusion Upon Seclusion
(GRA and Chalker)

229. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

230. Plaintiffs have a legally protected privacy interest in their information. This includes their Google login information, their emails, and documents contained on BCM's servers

and computer systems. Plaintiffs' email servers and computer systems contained private information and secrets that Plaintiffs had secluded away from public attention and prying eyes.

231. GRA and Chalker are directly liable under CDAFA because they directed and controlled the hacking of Plaintiffs' email servers, facilities, and computer systems.

232. GRA and Chalker purposefully and repeatedly hacked Plaintiffs' computer systems and email servers over a period of weeks. In doing so, they intruded upon Plaintiffs' secluded documents and private communications, viewing them through electronic means and then printing them out.

233. Much of the information GRA and Chalker illegally obtained in the hacking concerned Broidy's private matters and is not of public interest. GRA and Chalker's tortious scheme—committing repeated cybercrimes to facilitate the publishing of a private citizen's secrets—is highly offensive and shocking to any reasonable person. GRA and Chalker were retained specifically as part of an effort to harm Broidy's business and public standing. They accomplished that end through illegal means, by stealing and conspiring to publish private facts about his personal life and matters.

234. GRA and Chalker intruded upon Broidy's seclusion between January 16, 2018 and February 25, 2018 and other times within two years of the commencement of this action.

235. The stealing and subsequent public disclosure of misleading and curated information has caused Plaintiffs to suffer monetary damages, in an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs. The injury to Plaintiffs' privacy is ongoing, and thus the damages Plaintiffs seek may not be finally set. Because GRA and Chalker's actions are intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

236. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and

(f) additional harm and damages to be proven at trial.

237. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

CLAIM VI
Civil Conspiracy
(All Defendants)

238. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

239. GRA, Kevin Chalker, Mandich, Garcia, and Courtney Chalker formed and operated a conspiracy.

240. Defendants willfully, intentionally, and knowingly agreed to violate the SCA, the CFAA, and CDAFA, to receive and possess stolen property, and to intrude upon Broidy's seclusion, all as further described above and incorporated herein. Defendants operated their conspiracy to accomplish these ends.

241. GRA and Chalker willfully, intentionally, and knowingly directed and controlled the illegal acts, as described above.

242. Mandich furthered the illegal acts by willfully, intentionally, and knowingly designing and strategizing the "special projects" including covert operations at Chalker's direction.

243. Garcia and Courtney Chalker furthered the illegal acts by willfully, intentionally, and knowingly destroying evidence of the conspiracy's unlawful and tortious conduct at Chalker's direction. Defendants wiped GRA's computers, phones and other devices clean of any damaging evidence; removed certain hard drives, phones and devices with incriminating evidence from GRA's offices' and brought those devices to a remote location where Defendants destroyed them.

244. Each of the Defendants actively participated in the above-described civil conspiracy, and therefore each Defendant is responsible for each tortious and otherwise unlawful action of any co-conspirator.

245. As a direct and proximate result of the conspiracy, including the conduct of Mandich, Garcia, and Courtney Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and

(f) additional harm and damages to be proven at trial.

246. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

CLAIM VII
Violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1831, 1832, 1836
(All Defendants)

247. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

248. The Defend Trade Secrets Act ("DTSA") creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

249. The DTSA imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *See id.* § 1832(a)(5).

250. The DTSA also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." *Id.* § 1831(a)(1).

251. The DTSA imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). *See id.* § 1831(a)(5).

252. "An owner of a trade secret that is misappropriated may bring a civil action. . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." *Id.* § 1836(b)(1). The owner may seek remedies including, *inter alia*, injunctive relief and "damages for actual loss caused by the misappropriation of the trade secret." *Id.* § 1836(b)(3)(A-B).

253. The BCM computer systems and email servers stored trade secrets, including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; information concerning business strategies and opportunities; and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

254. BCM stored trade secrets that were used in interstate and foreign commerce.

255. Plaintiffs have taken and continue to take reasonable measures to maintain the secrecy of their trade secrets. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

256. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Broidy, BCM, and clients. These contracts, proposals, and estimates contained sensitive information about Broidy's clients and his company's confidential technology and methods.

257. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

258. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

259. Defendants unlawfully conspired to take, appropriate, and obtain Plaintiffs' trade secrets without authorization, by means of a cyberattack against Plaintiffs. Defendants knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs.

260. GRA and Chalker directed and controlled the misappropriation of Plaintiffs' trade secrets during the hacking of their computer systems and email servers, while the other Defendants conspired in the same misappropriation by taking acts to design the strategy for the misappropriation and subsequently destroy evidence of it.

261. These trade secrets included confidential business plans, stored on plaintiffs' servers, cost proposals and service projections, information concerning business strategies and opportunities, and contacts for important business relationships.

262. GRA and Chalker improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated, or caused to be widely disseminated, those trade secrets to the media through intermediaries. At the time of such

disclosures, GRA and Chalker knew or had reason to know that the information disclosed consisted of trade secrets.

263. GRA and Chalker misappropriated Plaintiffs' trade secrets intentionally for the benefit their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign government of Qatar.

264. Defendants' conspiracy, and the acts of misappropriation by GRA and Chalker, have affected interstate commerce.

265. As a direct and proximate result of the actions of Defendants' conspiracy, including the acts of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

266. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I).

267. As a direct consequence of Defendants' unlawful actions, Defendants have unjustly benefited from their possession of Plaintiffs' trade secrets. Defendants were paid money by Qatar to conspire to misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of Defendants' profits pursuant to 18 U.S.C. § 1836(b)(3)(B)(i)(II).

268. Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C), equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(C).

269. Defendants' conduct constitutes criminal conduct in violation of 18 U.S.C. §§ 1831 and 1832. As such, it constitutes predicate racketeering activity under the Racketeer Influenced and Corrupt Organizations ("RICO") Act, 18 U.S.C. § 1962.

CLAIM VIII
Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426
(GRA and Chalker)

270. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

271. The California Uniform Trade Secrets Act ("CUTSA") provides a cause of action for damages and injunctive relief in response to the misappropriation of trade secrets. Cal. Civ. Code §§ 3426.2; 3426.3. (While Plaintiffs believe this claim is governed by California law, in the

alternative, Plaintiffs hereby allege, based on the same facts, that Defendants have committed misappropriation of trade secrets under New York common law.)

272. GRA and Chalker directed and controlled the misappropriation of a "trade secret" as defined by Cal. Civ. Code § 3426.1 to include "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

273. The BCM server stored trade secrets, including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; information concerning business strategies and opportunities; and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

274. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Broidy's clients and his company's confidential technology and methods.

275. Plaintiffs have taken and continue to take reasonable measures to maintain the secrecy of their trade secrets. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

276. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

277. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

278. GRA and Chalker directed and controlled the misappropriation of Plaintiffs' trade secrets by committing and supervising a hack into BCM's computer systems and email servers.

279. GRA and Chalker improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari-Funded Criminal Enterprise and to media organizations for publication. At the time of such disclosure, GRA and Chalker knew or had reason to know that the information disclosed consisted of trade secrets.

280. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

281. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

282. As a direct consequence of the GRA and Chalker's unlawful misappropriation of Plaintiffs' trade secrets, GRA and Chalker have unjustly profited from their possession of Plaintiffs' trade secrets. GRA and Chalker were paid money from Qatar to steal and misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of GRA and Chalker's profits.

283. GRA and Chalker's conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to Cal. Civ. Code § 3426.3, equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to Cal. Civ. Code § 3426.4.

CLAIM IX
Violation of the RICO Act, 18 U.S.C. §§ 1962(c) and 1964
(All Defendants)

284. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

285. The federal RICO statue provides, "It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c).

286. The RICO statute further provides that "Any person injured in his business or property by reason of a violation of section 1962 of this chapter may sue therefor in any

appropriate United States district court and shall recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney's fee . . . ." *Id.* § 1964(c).

287. At all relevant times, Plaintiffs and each Defendant are persons within the meaning of 18 U.S.C. §§ 1961(3), 1962(c), and 1964(c).

288. Defendants are a group of people and entities associated together in fact with several other individuals and entities, including members of the Qatari government, for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs (the "Enterprise"). Specifically, the Enterprise has engaged in a pattern of illegal and covert operations designed to silence and neutralize people who are perceived to be enemies or critics of Qatar.

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

290. Together, Defendants and their co-conspirators form an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). Each Defendant has knowingly, willfully, and unlawfully participated in the operation or management of the Enterprise, directly or indirectly, as described in the foregoing paragraphs and as identified further below.

291. The Enterprise consists of, at least, GRA, Chalker, Mandich, Garcia, Courtney Chalker, GRA EMEA, GRA Maven, GRA Quantum, GRA Research, Qrypt, Bernoulli, Toccum, Howard, Muzin, Shep, Hashem, and Nimeh, and numerous other known and unknown individuals, including cyber hackers, public relations professionals, lobbyists, political actors, and other members of the Qatari government.

292. Defendants and their co-conspirator members of the Enterprise have functioned, and continue to function, as a unit in carrying out their multi-year, ongoing pattern of racketeering activity through a campaign to neutralize critics of Qatar. Defendant Chalker is responsible for oversight and management of the hacking operations that are instrumental to the Enterprise's common purpose. Defendants Mandich and Garcia are key operatives who at times shared oversight and management responsibility with Chalker. By stealing the types of confidential information that could harm individuals who are perceived to be threats to Qatar, these individuals provide the Enterprise with the necessary content to be manipulated, falsified and widely disseminated to inflict maximum damage on the victim. Through those operations, they manage and/or facilitate the Enterprise's activities. Defendants GRA, GRA Maven, GRA Quantum, GRA EMEA, Qrypt, and GRA Research, on information and belief, are co-conspirator entities that employ hackers who help develop the plans to attack perceived critics of Qatar and ultimately carry out the operations of the Enterprise. They operate as separate but intertwined departments of a single company whose finances are thoroughly comingled. As a result, they also help manage and/or facilitate the Enterprise's activities.

293. Defendants' co-conspirators each helped manage and direct different aspects of the Enterprise in pursuit of the same common objective: to silence Qatar's critics. Their specific roles involved identifying individuals who were perceived to be threats to Qatar's standing in the world community; instructing Defendants to conduct cyberattacks on those targets; obtaining the confidential information stolen by Defendants; manipulating and falsifying that content; and then disseminating it widely to members of the national and international media for the purpose of harming Plaintiffs and other victims of Defendants' cyberattacks.

294. All Defendants and their co-conspirators have worked together, and continue to work together, to develop, orchestrate and implement their plans to silence and neutralize individuals who criticize Qatar and thereby threaten its standing in the world community.

295. The Enterprise is an enterprise under the RICO Act that is separate and distinct from Defendants and their co-conspirators. The activities of the Enterprise are separate and distinct from the ordinary and legitimate business operations of the individual Defendant entities and those of their co-conspirator entities, as well as the ordinary business operations of GRA, Chalker, Mandich Garcia, and Courtney Chalker and other individual participants in the racketeering activity who also happen to work for a Defendant entity and/or serve in an officer, director or beneficiary capacity for such an entity.

296. Defendants and their co-conspirators committed the above and below-described tortious and criminal acts as part of a common purpose to serve the Enterprise. These actions were separate and distinct from any lawful work they may have performed under contract for Qatar.

297. The Enterprise engaged in tortious conduct that crossed state and international lines, spanning from Qatar to California, New York, and Washington, DC, among other areas.

298. Plaintiffs hereby allege and set forth the following predicate racketeering activities as defined under 18 U.S.C. § 1961. Defendants jointly and individually committed each separate set of predicate acts alleged below.

299. Defendants each participated in the "pattern of racketeering activity" described in the foregoing paragraphs within the meaning of 18 U.S.C. §§ 1961(1) & (5). They committed multiple acts of wire fraud, in violation of 18 U.S.C. § 1343; multiple acts of criminal money laundering, in violation of 18 U.S.C. § 1957; multiple misappropriations of trade secrets, in violation of the DTSA, 18 U.S.C. §§ 1832(a)(1) and (a)(5); and multiple acts of economic

espionage, in violation of 18 U.S.C. §§ 1831(a)(1) and (a)(5). These predicate acts are not isolated incidents but instead form a continuous, related pattern of racketeering activity with the common purpose of conducting covert and illegal operations to silence and neutralize Qatar's critics.

300. Together, these numerous predicate acts are part of an open-ended, multi-year scheme of racketeering that continues through the present. The Enterprise has inflicted numerous injuries against many victims over a period of multiple years. Its campaign to silence its critics is ongoing, and it continues to commit acts of racketeering to shield Qatar from public scrutiny. Media organizations are still to this day relying on information stolen from Broidy's computer systems and email servers to publish stories to damage his image. For example, media outlets have continued to falsely claim that Broidy was a target in the investigation of special counsel Robert Mueller into Russian interference in U.S. elections, whereas in reality he was never interviewed by Mueller's team and does not appear once in the Mueller Report. If left unchecked, the Enterprise presents a distinct threat of long-term racketeering activity.

301. Alternatively, the predicate acts outlined herein are part of a multi-year closed-ended scheme of racketeering that began no later than April 2017 and ended no earlier than August 2019.

302. Federal law imposes criminal penalties on "[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." 18 U.S.C. § 1343.

303. As described in detail above, from December 2017 through February 2018, Defendants engaged in multiple spear phishing attempts, followed by unauthorized access to Plaintiffs' computers and networks. The spear phishing attempts were efforts to obtain access to Broidy and BCM's computers and networks, under fraudulent pretenses, so as to steal Plaintiffs' confidential information. The operations were conducted in furtherance of the Enterprise's purpose of silencing Qatar's political opponents.

304. Defendants sent at least one such fraudulent email to Robin Rosenzweig. On December 27, 2017, she received an email at her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. It was sent from a Gmail address and had been disguised to look like an authentic security alert from Google. The email purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

305. On or around January 14, 2018, Defendants sent other fraudulent spear phishing emails to Broidy's Executive Assistant. These emails were disguised as Google security alerts, which bore Google trademarks used without Google's permission, and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

306. One of the fraudulent spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone number. The email was sent from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on

the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

307. Defendants sent numerous spear phishing emails like the ones described above using interstate wires, and these transmissions crossed state lines.

308. Defendants used the above-described spear phishing emails to make material misstatements with the specific intent that the targeted individuals would rely on those false representations to their detriment and surrender their valuable login credentials so that they could then use those credentials to hack into Plaintiffs' computer systems. Defendants did so while contemplating the harm that they would cause these targets and ultimately cause Broidy. They succeeded.

309. Having fraudulently obtained those credentials through material misstatements, Defendants commenced an illegal cyberattack against Broidy and BCM's computer systems and servers. These cyber transmissions used interstate wires and crossed state lines—for example, forensic investigation has revealed that some transmissions traveled from Vermont to California. Defendants and their co-conspirators initiated thousands of intrusions into Plaintiffs' computer systems and email servers.

310. Defendants thereby obtained Plaintiffs' valuable electronic information, including but not limited to emails, private information, contracts, trade secrets, and business plans. Defendants launched the spear phishing attempts with the specific intent of fraudulently depriving Plaintiffs of their valuable property.

311. Defendants each perpetrated several acts of wire fraud by committing and supervising the spear phishing efforts against associates of Broidy in order to obtain their valuable login credentials to BCM's computer systems and email servers.

312. As detailed above, Defendants' actions have directly and proximately caused Plaintiffs to suffer injury to their business or property, including (without limitation) damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

313. Under certain defined circumstances, federal law imposes criminal liability on any person who "knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity." 18 U.S.C. § 1957(a). A "monetary transaction" means the "deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument ... by, through, or to a financial institution." 18 U.S.C. § 1957(f)(1). "Criminally derived property" means "any property constituting, or derived from, proceeds obtained from a criminal offense." 18 U.S.C. § 1957(f)(2). The term "specified unlawful activity" includes any act or offense that constitutes "racketeering activity" under 18 USC § 1961(1), such as each of the various predicate acts identified herein. *See* 18 U.S.C. § 1957(f)(3).

314. As outlined above, in furtherance of the Enterprise, Defendants engaged in a pattern of racketeering activity that included multiple acts of wire fraud. By intentionally and knowingly making multiple fraudulent misrepresentations, Defendants induced individuals to provide their log-in credentials to Plaintiffs' computers and servers, and then used those credentials to hack into and steal Plaintiffs' confidential material. The Qatari government and/or their agents paid Defendants millions of dollars for directing and engaging in these criminal acts of wire fraud.

315. On information and belief, these offenses took place in the United States. Alternatively, to the extent certain acts took place outside the United States, Defendants who conducted those acts were U.S. persons, within the meaning of 18 U.S.C. § 3077.

316. In the fall of 2017, Chalker held over $40 million in accounts affiliated with Bernoulli, Toccum, and GRA EMEA—offshore shell companies formed in Gibraltar for which Chalker served as the sole director. By late 2018, the accounts for both Bernoulli and Toccum held under $98,000.

317. On information and belief, Defendants knowingly used portions of their illicit proceeds, valued at greater than $10,000, to pay the individual hackers whom they employed to carry out these complex acts of wire fraud.

318. On information and belief, each of those monetary transactions was by, through or to a financial institution within the meaning of 18 U.S.C. §§ 1956(c)(6) and 1957(f)(1), affected interstate or foreign commerce, and constituted an act of criminal money laundering that forms part of the pattern of racketeering activity in which Defendants engaged.

319. The DTSA imposes criminal penalties against anyone who "knowingly . . . with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly … steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;. . . [or] without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; [or] receives, buys, or

possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization." 18 U.S.C. § 1832(a).

320. The DTSA also imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *Id.* § 1832(a)(5).

321. Through their hacking of Broidy's and BCM's computers and networks, Defendants and other members of the Enterprise repeatedly violated the DTSA, 18 U.S.C. § 1832, *et seq.* The BCM servers stored trade secrets including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; vendor lists; requests for proposals and responses thereto; information concerning business strategies and opportunities; and contacts for important business relationships. BCM is a sophisticated investment management and services firm that possesses and uses its trade secrets to serve its customers and create a competitive market advantage.

322. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Broidy's clients and his company's confidential technology and methods.

323. These trade secrets are of substantial value to Plaintiffs, and they were used and intended for use in relation to products and services in interstate and foreign commerce.

324. Plaintiffs take and have taken reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

325. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

326. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

327. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

328. Defendants unlawfully and without authorization appropriated, obtained, and stole Plaintiffs' trade secrets. They knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs and economically benefit both themselves and Qatar. Defendants were paid substantial amounts to misappropriate and publish Plaintiffs' trade secrets, and Qatar hoped to use those trade secrets to its economic benefit. Defendants thereby committed multiple violations of the DTSA.

329. Defendants' knowing and intentional violation of the DTSA has materially injured Plaintiffs. It has deprived them of valuable trade secrets, and caused them to expend resources to defend against further cyberattacks.

330. The Enterprise's misappropriation of Plaintiffs' trade secrets began in January of 2018 and is ongoing.

331. As detailed above, Defendants' actions have directly and proximately caused Plaintiffs to suffer injury to their business or property, including (without limitation) damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

332. Federal law provides that "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret . . . [or] (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization" violates 18 U.S.C. § 1831(a)(1).

333. Federal law also imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" a violation of § 1831(a)(1). *Id*. § 1831(a)(5).

334. Defendants each unlawfully and without authorization took, appropriated, and obtained Plaintiffs' trade secrets through the cyberattack against Plaintiffs' computers and servers. Defendants and other members of the Enterprise knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs. They misappropriated Plaintiffs' trade secrets intentionally for the benefit of their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign nation of Qatar.

335. Defendants used an artifice and fraud—the fake Gmail spear phishing emails—to take, appropriate, and obtain Plaintiffs' trade secrets.

336. Defendants used fake spear phishing emails to induce targets to surrender their valuable login credentials. Multiple targets did provide their login credentials in reliance on these false material statements.

337. As detailed above, Defendants' actions have directly and proximately caused Plaintiffs to suffer injury to their business or property, including (without limitation) damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs'

trade secrets and confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

338. The Enterprise has substantially affected interstate commerce by (1) committing multiple acts of wire fraud and money laundering involving transactions that cross state and international lines, as described above; and (2) causing damage to Plaintiffs and other victims of these attacks by harming property and business, including loss of valuable electronic information, business plans, contracts, vendor lists, requests for proposals, consumer good will, and substantial expense in protecting Plaintiffs' and other victims' computer systems and email servers from additional cyberattack. Plaintiffs regularly conduct business in interstate commerce, and Defendants' cyber-hacking has substantially disrupted that business.

339. As a direct and proximate result of Defendants' racketeering activity, Plaintiffs incurred substantial and concrete financial loss and damage to their business and property, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries,

rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

340. Defendants' racketeering activity has further directly and proximately caused loss to Plaintiffs' business by deliberately and foreseeably harming the confidence and trust of its existing and potential clients in Plaintiffs' ability to maintain the security and secrecy of client data. Plaintiffs' business involves sensitive work in the government contract space where discretion and security are critical. A highly public hacking scheme like this one has naturally caused significant lost revenue and other harm. In other words, Defendants' racketeering activity has directly and proximately caused damage to Plaintiffs' goodwill and business relationships, causing loss to the value of Plaintiffs' business and lost profits, among other damages.

341. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

CLAIM X
Conspiracy to Violate the RICO Act, 18 U.S.C. § 1962(d)
(All Defendants)

342. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

343. The RICO Act provides that "[i]t shall be unlawful for any person to conspire to violate any of the provisions" of the Act. 18 U.S.C. § 1962(d).

344. Defendants knowingly and voluntarily agreed with other members of the Qatari-Funded Criminal Enterprise to engage in the above-mentioned racketeering activity with the common objective of silencing Qatar's critics. In so doing, they intentionally and willfully conspired to commit, and ultimately committed, the above-described predicate acts.

345. GRA and Chalker knew about and agreed to participate in the conspiracy when they began their collective and illicit efforts to help Qatar hold on to hosting World Cup 2022. All the GRA Defendants knew about and agreed to participate in the conspiracy many years ago, when their criminal operations described above were first launched.

346. Defendants and other members of the Qatari-Funded Criminal Enterprise committed the above-referenced racketeering acts in furtherance of their racketeering conspiracy.

347. Defendants each committed numerous acts of racketeering knowingly in furtherance of the conspiracy, including wire fraud, money laundering, misappropriation of trade secrets, and economic espionage.

348. As a direct consequence and by reason of Defendants' racketeering conspiracy, Plaintiffs have suffered injury to their business and property, which includes, but is not limited to, concrete financial loss, discussed above.

349. These injuries to Plaintiffs' business and property were the natural, foreseeable, and intended result of the GRA Defendants' RICO conspiracy and the acts committed in furtherance thereof.

350. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

PRAYER FOR RELIEF

351. Plaintiffs repeat and re-allege the allegations contained in each and every preceding paragraph.

352. Wherefore, Plaintiffs request that this Court order the following relief against Defendants:

(a) Grant judgment in favor of Plaintiffs and against Defendants on all claims;

(b) Declare that Defendants' conduct violates the statutes and common law cited above;

(c) Award Plaintiffs an appropriate amount in monetary damages as determined at trial, including but not limited to compensatory damages, lost profits, statutory damages, and treble damages under RICO, 18 U.S.C. § 1964 and Cal. Pen. Code § 496;

(d) Award Plaintiffs punitive damages under 18 U.S.C. § 2707, Cal. Pen. Code § 502, and Plaintiffs' common-law claims, as well as exemplary damages under Cal. Civ. Code § 3426.3 and 18 U.S.C. § 1836(b)(3)(C);

(e) Award Plaintiffs their reasonable attorneys' fees and the costs of bringing this action;

(f) Award Plaintiffs pre- and post-judgment interest;

(g) Award damages to be proven at trial; and

(h) Grant Plaintiffs such other relief as is just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a jury trial on all issues so triable.

Dated: March 1, 2022

Respectfully submitted,

KASOWITZ BENSON TORRES LLP

By: /s/ *Daniel R. Benson*

Daniel R. Benson
Sarah G. Leivick
Andrew R. Kurland
1633 Broadway
Tel.: (212) 506-1700
New York, New York 11019
dbenson@kasowitz.com
sleivick@kasowitz.com
akurland@kasowitz.com

Henry B. Brownstein
1399 New York Avenue, Suite 201
Washington, D.C. 20005
Tel.: (202) 760-3400
hbrownstein@kasowitz.com

Counsel for Plaintiffs Elliott Broidy and Broidy Capital Management, LLC

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELLIOTT BROIDY and BROIDY CAPITAL MANAGEMENT, LLC, Plaintiffs, —v.— GLOBAL RISK ADVISORS LLC, GRA QUANTUM LLC, GRA RESEARCH LLC, GLOBAL RISK ADVISORS EMEA LIMITED, GRA MAVEN LLC, QRYPT, INC., KEVIN CHALKER, DENIS MANDICH, ANTONIO GARCIA, and COURTNEY CHALKER Defendants.	Case No. 1:19-CV-11861

DECLARATION OF GRA WHISTLEBLOWER

I, GRA Whistleblower, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am over the age of 18 and competent to testify in this matter.

2. I have personal knowledge about the matters stated in this declaration.

3. I have reviewed the First Amended Complaint filed by Plaintiffs Elliott Broidy and Broidy Capital Management, LLC in the above-captioned matter, and I am generally familiar with the subject matter of the lawsuit and the claims being made.

4. I was employed by GRA and/or its affiliates from XX through XX.

5. Kevin Chalker controlled GRA and its affiliated entities.

6. I was in a position to obtain knowledge that Kevin Chalker had knowledge of the Broidy hacking and GRA was responsible for the hacking.

7. I was in a position to obtain knowledge that Kevin Chalker and GRA engaged in physical and electronic surveillance of Broidy.

8. I was in a position to obtain knowledge that Kevin Chalker and others at GRA took steps to hide and destroy electronic devices that contained information that would show involvement with the Broidy hacking.

9. Based on my knowledge of Kevin Chalker's capabilities and history of him threatening individuals and retaliating against them for disclosing potentially harmful information, I now fear for the safety and myself and/or my family should my identity become known to GRA and Kevin Chalker.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 28 day of May, 2021.

/s/ GRA Whistleblower
GRA Whistleblower