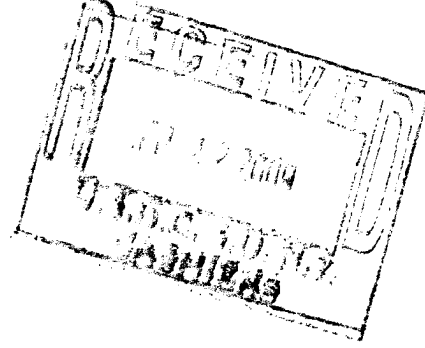


John L. Gardiner  
SKADDEN, ARPS, SLATE,  
MEAGHER & FLOM LLP  
Four Times Square  
New York, New York 10036-6522  
(212) 735-3000



Attorneys for Plaintiff  
Bassam Y. Alghanim

JUL 22 2014

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

\_\_\_\_\_  
BASSAM Y. ALGHANIM,  
  
Plaintiff,

09 Civ. 3098

v.

KUTAYBA Y. ALGHANIM and  
OMAR K. ALGHANIM,  
  
Defendants.

COMPLAINT  
[Jury Trial Requested]

Plaintiff Bassam Y. Alghanim ("Bassam" or "Plaintiff"), by his attorneys Skadden, Arps, Slate, Meagher & Flom LLP, as and for his complaint against defendants Kutayba Y. Alghanim ("Kutayba") and Omar K. Alghanim ("Omar") (together "Defendants"), alleges upon personal knowledge with respect to himself and his own acts, and upon information and belief with respect to all other matters, as follows:

**NATURE OF THE ACTION**

1. In the midst of a bitter family battle between Plaintiff and his brother (Defendant Kutayba) over the break-up of their multi-billion dollar business empire, Defendants embarked upon a covert program of industrial espionage designed to undermine Plaintiff's position and gain an unfair advantage in the ongoing negotiations and legal proceedings. Among

other things, Defendants hired private investigators to illegally “hack” into Plaintiff’s password-protected email accounts and steal privileged communications between Plaintiff and his attorneys in the United States and Kuwait. Defendants’ investigators copied confidential strategic and attorney-client privileged emails. Hoping to cover their tracks, they then printed out the emails, scanned them into PDF files and uploaded them to a secret, password-protected website (the “Covert Website”) that they had created specifically for the purpose of storing the stolen emails. Defendants and other co-conspirators were given the password to the Covert Website so that they could view the stolen emails and make copies of them.

2. Over the course of many months, hundreds of batches of confidential and privileged emails were stolen from Plaintiff’s email accounts and uploaded to the Covert Website. Defendants Kutayba, Omar and their co-conspirators repeatedly accessed the Covert Website using their secret password, viewed the batches of emails as they were uploaded and made copies for their use in the negotiations and proceedings. Defendants did so from a number of locations, including from their personal residence at 15 East 81<sup>st</sup> Street in New York City.

3. Through this covert program of illegal espionage, Defendants and their co-conspirators secured real-time access to Plaintiff’s strategic planning and the legal advice he was receiving from his attorneys in the United States and Kuwait. As a result, Defendants were able to derail the negotiations and continue their strategy of trying to force Plaintiff to take less than his fair share of the brothers’ joint assets by denying him access to his assets and income.

4. Defendants’ acts of industrial and personal espionage violated numerous federal statutes that provide both severe criminal penalties and private rights of action for wrongful interference with email communications. They also violated Plaintiff’s privacy rights under the laws of California where he was living during much of the period when he was

victimized. Plaintiff seeks injunctive relief, compensatory damages and punitive damages to deter Defendants, their co-conspirators and others from engaging in similar illegal and unethical conduct.

### **JURISDICTION AND VENUE**

5. The Court has jurisdiction over the federal claims under 28 U.S.C. § 1331 (federal question jurisdiction). Jurisdiction over the state law claims is based on 28 U.S.C. § 1367 (supplemental jurisdiction).

6. Jurisdiction over Defendants is proper because Defendants maintain at least two residences in New York: (i) their primary New York residence, a 16,000 square foot mansion located at 15 East 81st St., New York, New York; and (ii) a 48-acre estate on Long Island known as “Sassafras,” located at 19 Burma Road, Lloyd Harbor, New York. Both Defendants also are involved in a wide range of business activities in New York.

7. Venue is proper in this District under 28 U.S.C. § 1391(b) because both of the Defendants reside in this District and because a substantial part of the events giving rise to this action occurred in this District, including the use of the residence at 15 East 81st Street as a venue to download and review the stolen emails. In addition, Defendants stole Plaintiff’s emails to gain advantage in a dispute that concerns, in part, Kutayba’s breach of Plaintiff’s rights by improperly assuming control of two New York-based service companies (Green Drake Corporation N.V. and A.I. International Corporation (together the “Service Companies”)) that are required to act as agents for the two brothers in managing an almost half billion dollar investment portfolio and servicing their properties and interests throughout the world.

## **THE PARTIES**

8. Plaintiff Bassam Y. Alghanim is a Kuwaiti citizen who resides at 1005 Bel Air Court, Los Angeles, CA, 90077.

9. Defendant Kutayba Y. Alghanim is a Kuwaiti citizen who maintains a residence at 15 East 81st Street, New York, New York. Kutayba is the father of Defendant Omar K. Alghanim and the brother of Plaintiff, Bassam Y. Alghanim.

10. Defendant Omar K. Alghanim is a Kuwaiti citizen who maintains a residence at 15 East 81<sup>st</sup> Street, New York, New York. Defendant Omar is the President of Alghanim Industries Company W.L.L. ("Alghanim Industries"), one of the major businesses jointly owned by Plaintiff and Kutayba.

11. In addition to their residence at 15 East 81<sup>st</sup> Street, New York, New York both defendants, Kutayba and Omar, also maintain a 48 acre residence at 19 Burma Road, Lloyd Harbor, New York.

12. In taking the actions complained of in this complaint, Defendants acted in concert with a number of other people and entities. In so doing, each was the agent of the other and each is responsible for all the actions of the others in furtherance of their conspiracy. Plaintiff may subsequently amend this complaint to add some or all of the co-conspirators as additional defendants and add additional causes of action.

## **THE FACTS**

### **The Brothers' Business Dispute**

13. In the 1970s, Bassam and Kutayba jointly succeeded to the substantial business empire founded by their father, Yusef Ahmed Alghanim. The brothers beneficially held all of their assets as 50/50 partners. Over the intervening years, largely due to the business

decisions and actions of Plaintiff, that empire grew to consist of billions of dollars worth of business interests in Kuwait and elsewhere throughout the world, including in New York City.

14. In addition to Alghanim Industries, among the many assets and businesses jointly owned by the brothers are Yusef Ahmed Alghanim and Sons W.L.L. (“YAAS”) and other Alghanim family businesses located in Kuwait. In addition, Plaintiff and Defendant Kutayba own and owned a substantial stake in Gulf Bank, one of Kuwait’s most significant banks.

15. Plaintiff was primarily responsible for the successful development of the brothers’ joint businesses, including the acquisition of their stake in Gulf Bank. Until October 2008, Plaintiff was the Chairman of Gulf Bank. Indeed, during much of the time when Plaintiff was developing their joint businesses in Kuwait, Defendant Kutayba was absent from Kuwait, living in New York, among other places.

16. Beginning in and around 2007, after Defendant Kutayba’s eldest son, Defendant Omar, had become active in the businesses in Kuwait, disputes began to develop between Kutayba and Bassam concerning the future of their business empire. In or about 2008, Plaintiff and Defendant Kutayba reached an impasse in their business and personal relations and they decided to divide their joint assets and go their separate ways.

17. At or about this time, Kutayba, ignoring the fact that Plaintiff had built the enormous family wealth that he and Kutayba both enjoyed, asserted that he was entitled to more than the 50% share of the businesses that he had held up to that point in time. Plaintiff disagreed with his brother’s baseless assertion.

18. When Plaintiff and Defendant Kutayba were unable to resolve the dispute created by Kutayba’s baseless assertion, Kutayba orchestrated the involvement of high-ranking Kuwaiti officials to pressure BYA to reach an agreement with him. Two agreements were

entered into on March 12, 2008 (the “March 12 Agreements”) that provided for the division of the brothers’ empire. Subsequently, a Memorandum of Understanding (“MOU”) was prepared with respect to the implementation of the March 12 Agreements.

19. The brothers agreed that while they were in the process of dividing their empire all expenses would continue to be paid jointly as they had been in the past and that both brothers would continue to receive the same services from their Service Companies that they had in the past.

20. Unfortunately, ever since they entered into the March 12 Agreements, Defendant Kutayba has thwarted Plaintiff’s enjoyment of his assets. Among other unlawful acts, Kutayba has cut off Plaintiff’s access to the income from their jointly owned businesses and actively sought to prevent him from receiving any assets owned by him. To this end, he has, among other things, directed the brothers’ Service Companies to cease acting for Plaintiff. In addition, he has caused employees of those Service Companies to breach their fiduciary duties to Plaintiff and assist Defendant Kutayba in diverting joint assets to his personal use, including most recently diverting \$75 million to Kutayba from a jointly-owned portfolio of assets.

21. As a consequence of Defendant Kutayba’s shameful and illegal conduct toward his brother, Plaintiff and Defendant Kutayba have been embroiled in a contentious and acrimonious dispute over the division of their assets ever since the March 12 Agreements and subsequent MOU were entered into.

22. As a result, Plaintiff was required to engage lawyers in the United States and Kuwait to protect Plaintiff’s interests and to represent him in negotiations with Kutayba and Kutayba’s legal team. These negotiations have been ongoing since March 2008 and throughout 2009.

23. In the course of the negotiations and in preparation for the possibility of litigation with respect to the brothers' underlying business disputes, Plaintiff repeatedly consulted his attorneys in the United States and Kuwait. As an integral part of those consultations, Plaintiff and his attorneys have exchanged numerous privileged communications regarding the strategy to be followed in the negotiations and litigation and the legal advice regarding various aspects of the dispute. Almost all of this legal advice was sent to and received by Plaintiff at his password-protected AOL email addresses that Defendants caused to be hacked into as described herein.

**Plaintiff Learns That His Password-Protected Emails Have Been Intercepted**

24. During the last fifteen months, Plaintiff used email as his principal means of communication. Plaintiff had two private email addresses, both of which were password protected. With the sole exception of his confidential personal assistant with respect to only one of the two email accounts, Plaintiff did not provide the passwords to anyone and he did not authorize anyone else to use or access these email accounts.

25. Plaintiff used these email addresses to conduct his business and legal activities and correspond with his attorneys in the United States and Kuwait. He did so with the reasonable intention and expectation that all of his communications were private and confidential. Using these email addresses, Plaintiff received legal advice in relation to the dispute described above, as well as other legal matters and that advice critically impacted on the instructions he gave to his attorneys. Plaintiff also used these email addresses to conduct other confidential personal correspondence, including with respect to his medical and health matters and his personal financial transactions, among other things.

26. Plaintiff has recently learned that for many months all of the privileged emails between Plaintiff and his US counsel, as well as privileged communications with Plaintiff's counsel in Kuwait, have been stolen by Defendants.

27. Included among the matters covered by the stolen privileged emails are Plaintiff's strategy and legal advice with respect to negotiating positions and legal actions that will be commenced in Kuwait when the Kuwait courts return from recess in October. As a result, Defendants have achieved an unfair and illegal advantage in that litigation before it has even been commenced. Plaintiff has no way to redress that injury except through this action.

28. Specifically, in mid-August 2009, Plaintiff was informed by a third party that some of Plaintiff's private, confidential and privileged emails had shown up in a search the third party had conducted on the internet. It would appear that, due to a mistake either in the way the Covert Website was designed, or because of a glitch in the process of uploading the stolen emails described herein, some of the stolen emails on the Covert Website had become accessible through a Google search on the internet.

29. Upon discovering this information, Plaintiff changed the passwords on his AOL email accounts and took other measures to try to prevent the continued theft of his emails. Plaintiff also undertook urgent investigations to determine how his email communications had been compromised. Those investigations have left no doubt that the hacking of Plaintiff's emails was done by or at the direction of Defendants and others acting in concert with them.

#### **The U.K. Discovery Action**

30. The domain name of [www.jackshome.info](http://www.jackshome.info) was identified as the location of the stolen emails, *i.e.*, the Covert Website. The internet service provider for that website was identified as GX Networks Limited ("GX"), an internet service provider in the United Kingdom.



31. On or about August 25, 2009, Plaintiff brought an application in the courts of the United Kingdom in order to obtain all relevant information in the possession of GX relating to the jackshome.info website. Shortly thereafter, on August 28, the English High Court issued an Order, requiring GX, among other things, to (1) preserve all relevant information relating to the www.jackshome.info website hosted by GX, and to (2) produce all such information to Plaintiff. In addition, the Order barred GX from disclosing the application and order to anyone (except as required by law). GX subsequently produced its logs showing activity on the www.jackshome.info website.

#### **The AOL Logs**

32. Around the same time, Plaintiff obtained log files for each of his compromised AOL email accounts. The AOL log files contained, *inter alia*, each originating Internet Protocol (“IP”) address from which a user had connected to the particular AOL account and the date and time of the connection. An IP address is a numerical label assigned to a device that participates in a network of computers, such as the Internet, and identifies the device and its location.

#### **Plaintiff’s Emails Were Hacked and Posted to a Password-Protected Website**

33. Examination of information received from GX, AOL and other sources showed that:

(a) Plaintiff’s email accounts had been accessed without authorization and that the hacking had been done from a location in Reading, England. (Subsequent investigation revealed that the person likely to have done the hacking was a Timothy Zimmer),

(b) files containing Plaintiff's most privileged and confidential emails from the hacked email accounts were copied and converted to Portable Document Format ("PDF") files,

(c) the PDF files of Plaintiff's emails were then uploaded to the www.jackshome.info website, which was the Covert Website,

(d) the Covert Website had been created as a password-protected website intended to be accessed through File Transfer Protocol ("FTP") only, that is by a user who knew the website's unique record locator ("URL") address and not by someone browsing the web using Google or some similar search engine,

(e) the user of the Covert Website also had to know the correct username and the unique password required to gain entry to the site,

(f) following the site's creation, the default password issued with the site was changed to a new password which anyone accessing the site via FTP protocol would have to have known to access the site,

(g) once the PDF files of Plaintiff's emails had been uploaded to the Covert Website, Defendants and other users, who had the correct username and password, accessed that website, viewed the stolen emails and downloaded the copies of them, and

(h) shortly thereafter, Defendants or their agents deleted the stolen emails from the Covert Website in an effort to avoid detection.

34. Although the Covert Website was created in July 2008, Plaintiff does not presently know when Defendants and their agents began using it to upload copies of emails stolen from Plaintiff. Because Defendants or their agents routinely deleted the stolen emails shortly after they had been accessed, viewed and downloaded by Defendants and their associates,

at the time Plaintiff discovered its existence, many of the stolen emails had already been deleted from the site.

35. Further investigation located some records in Google's cache files of some additional emails that had been on the Covert Website but had subsequently been deleted from the website.

36. Information received from GX with respect to the Covert Website disclosed that Defendants' practice was to consecutively number each batch of stolen emails uploaded to the Covert Website. From that numbering convention it appears that at least 389 batches of stolen emails were uploaded to the Covert Website during the period from July 24, 2008 through August 12, 2009 when Plaintiff changed his email passwords. It also appears that the hacking and uploading of Plaintiff's emails occurred on almost a daily basis.

37. For example, based on information obtained through the English courts, from May 2, 2009 until August 12, 2009, the date Plaintiff changed the passwords on his email addresses, Plaintiff's email accounts were accessed 123 times from IP addresses in the United Kingdom, 103 of those times from a single U.K.-based IP address. During this period, no one in the United Kingdom was authorized to access Plaintiff's email accounts. A copy of the AOL logs for each of the hacked email accounts showing the times and dates of the unlawful accesses is attached hereto as Exhibit A, and is incorporated herein by reference. These logs show numerous unauthorized accesses made from a United Kingdom IP address, 84.12.61.188, as well as from other United Kingdom based IP addresses: 84.69.5.148; 86.136.121.190; 86.144.56.103; 86.28.177.79; 92.29.31.103; 149.254.49.166; 80.7.6.70; 81.153.157.238; and 81.153.157.31. Information obtained from the U.K. relating to these IP addresses indicates that a Mr. Timothy

Zimmer was most likely the person responsible for hacking into Plaintiffs email accounts. Mr. Zimmer had no authority to access these accounts.

38. Likewise information obtained to date demonstrates clearly that in the final six weeks of this time frame -- July 2, 2009 to August 12, 2009 -- a single IP address in the U.K. uploaded PDF files containing the stolen emails to the Covert Website almost immediately following instances when Plaintiff's email accounts were accessed without his authorization. A copy of an extract made from the GX logs showing the dates and times of the unlawful uploading is attached hereto as Exhibit B and incorporated by reference herein.

#### **Defendants Try To Cover Their Tracks**

39. On the day Plaintiff changed his AOL passwords, Defendants' agents attempted to access Plaintiff's email accounts but were unable to obtain access. Shortly thereafter, Defendants or their agents uploaded some public domain material to take the place of the stolen emails on the Covert Website and caused Google to remove from the Google cache file all of the stolen emails that had been stored there.

40. Although Defendants' agents scrubbed the Covert Website of the stolen emails, many communications among Defendants and their co-conspirators are likely to exist in their own files, including in their electronic communications. In addition, through examination of their computer hard drives, it may be possible to recover stolen emails that Defendants attempted to delete from their computers, or it may at least be possible to find evidence of their deletion.

#### **Defendants Repeatedly Accessed Plaintiff's Emails From Their New York Residence and Other New York Locations**

41. Once Plaintiff's stolen emails were intercepted and posted to the Covert Website, Defendants and their co-conspirators repeatedly accessed and downloaded them from

locations in New York and around the world. For example, in just the period between June 1, 2009 and August 20, 2009 Defendants and their co-conspirators downloaded PDFs from the Covert Website more than 250 times.

42. More than 100 of the downloads from the Covert Website were conducted from IP addresses in the United States, and nearly all of those were from IP addresses located in New York City.

43. The New York IP address most frequently used to view and download Plaintiff's confidential emails is an IP address associated with Defendants' Manhattan residence, 15 East 81st Street, New York, New York. For instance, over a two-month period this summer, between June 19, 2009 and August 20, 2009, files from the Covert Website were downloaded from this address at least 71 times. The files viewed and downloaded from this address include attorney-client privileged communications between Plaintiff and his attorneys concerning his ongoing dispute with Defendant Kutayba. A copy of an extract showing the times and dates of the downloads from the IP address associated with Defendants' Manhattan residence is attached hereto as Exhibit C and incorporated herein by reference.

44. The Covert Website also was accessed in June 2009 by IP addresses associated with Columbia Presbyterian Hospital in Manhattan, using the correct username and password. Defendant Omar was a patient at Columbia Presbyterian during that same period. Plaintiff is not aware of any other person, patient or otherwise, associated with Columbia Presbyterian who would be motivated to illegally access Plaintiff's confidential emails or would know of the existence of the Covert Website.

45. The Covert Website also was accessed from at least two additional New York locations that Plaintiff believes also were associated with Defendants or others acting at

their direction. Plaintiff's investigation is ongoing and may lead Plaintiff to bring claims against additional defendants once their identities are revealed.

46. The accumulated data demonstrates that Defendants' use of the Covert Website and repeated downloading of Plaintiff's emails was not casual or accidental but rather part of a coordinated scheme to steal and use Plaintiff's privileged and confidential information. Specifically, the data showed that the following pattern was repeated scores of times: (i) unauthorized users accessed Plaintiff's email accounts; (ii) shortly thereafter, PDF copies of the stolen emails were created and uploaded to the Covert Website; (iii) shortly thereafter, Defendants accessed the Covert Website and downloaded the newly-uploaded stolen emails using the unique user name and password associated with the Covert Website; and (iv) shortly thereafter, the co-conspirators deleted prior batches of stolen emails from the Covert Website.

47. The following timeline provides just one illustrative example of Defendants' unlawful activities:

- At 4:41 p.m. on July 27, 2009, Plaintiff was copied on a substantive email from his assistant to his New York attorneys, seeking legal advice on Plaintiff's behalf.
- At 4:44 a.m. the next morning, before Plaintiff checked this email, the U.K.-based hacker logged into Plaintiff's email account.
- At 9:32 a.m., a PDF file containing the email was uploaded to the Covert Website.
- At 9:40 a.m., the Covert Website was accessed and files were downloaded from one of the New York locations. At this point, Plaintiff had still not logged onto his email account. The wrongdoers thus had the first crack at Plaintiff's legal communications and strategy.
- At 4:42 p.m. that same day, the Covert Website was accessed from Defendants' East 81st Street IP address and files were downloaded from the site.

48. This and similar patterns were repeated dozens of times during the summer of 2009, and likely also throughout the period since July 2008, providing Defendants with real-time access to Plaintiff's privileged and confidential communications and legal strategy at the same time that Defendants were negotiating with him and his counsel.

### **Irreparable Harm**

49. Plaintiff has already been irreparably harmed by Defendants' actions. Defendants have illegally accessed and recorded Plaintiff's litigation and business strategy with respect to the multi-billion dollar disputes between them. There is no way to undo or redress that injury.

50. If Defendants are permitted to continue illegally accessing Plaintiff's emails that contain his strategic and attorney/client communications and using the information, Plaintiff will suffer additional irreparable harm, because as a result of this illegal disclosure of his privileged communications he will be unable to act effectively in his dispute with Kutayba, which affects every aspect of his life and nearly everything he owns.

51. Defendants have already begun to cover their tracks by deleting files of stolen emails from the Covert Website. If Defendants are not immediately enjoined from continuing these improper efforts, they will undoubtedly destroy additional evidence critical both to these underlying proceedings and to a full investigation of Defendants' illegal activities.

### **COMPENSATORY DAMAGES**

52. The unlawful conduct of Defendants and their co-conspirators has caused Plaintiff very substantial damages in an amount to be proven at trial. Not only has Plaintiff been required to expend large amounts of money to investigate the wrongdoing and attempt to protect his confidential communications, but it has allowed Defendants to parry all of his efforts to

obtain his assets and income and deprived him of the value of the legal advice for which he paid substantial sums. This has enabled Defendants to prolong their campaign of wrongfully barring Plaintiff from the use and enjoyment of his assets and allowing them to continue their wrongful use of Plaintiff's assets for their benefit. The losses Plaintiff is sustaining by reason of that campaign of obstruction and self-dealing are in the many hundreds of millions of dollars.

### **PUNITIVE DAMAGES**

53. The unlawful conduct of Defendants and their co-conspirators has been intentional, fraudulent, malicious and oppressive warranting the imposition of punitive damages in an amount sufficient to deter even a billionaire from employing such tactics.

### **FIRST CAUSE OF ACTION** **(Violation of the Stored Communications Act, 18 U.S.C. § 2701, et seq.)**

54. Plaintiff repeats and re-alleges each of the allegations set forth in the preceding paragraphs of the Complaint as if fully set forth herein.

55. To accomplish their theft of Plaintiff's highly confidential emails, Defendants and/or persons acting at their direction and for their benefit, intentionally accessed without authorization a facility through which an electronic communication service is provided, AOL and its email servers. This access to Plaintiff's emails and his email accounts was entirely without authorization and in violation of AOL's terms of service. To the extent Defendants' initial access of AOL's publicly available website was authorized, Defendants and their co-conspirators exceeded such authorized access and violated AOL's terms of service by using such access to hack Plaintiff's email accounts and obtain and steal information in the computers or facilities of AOL that Defendants were not entitled to obtain.



56. Defendants and/or persons acting at their direction and for their benefit, thereby intentionally obtained access to Plaintiff's confidential and proprietary emails while they were in temporary, intermediate storage incidental to their transmission and/or back-up storage in AOL's systems.

57. Plaintiff's emails affected interstate and/or foreign commerce.

58. This conduct violated 18 U.S.C. § 2701(a).

59. This offense was committed for purposes of commercial advantage or private financial gain and in furtherance of unlawful and tortious conduct.

60. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

61. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, but no less than the statutory \$1,000 for each violation, plus interest; any profits made by Defendants as a result of the violations; attorney's fees and costs; and punitive damages for these wrongful, intentional and malicious acts.

**SECOND CAUSE OF ACTION**  
**(Violations of the Computer Fraud  
and Abuse Act, 18 U.S.C. § 1030)**

62. Plaintiff repeats and re-alleges each of the allegations set forth in preceding paragraphs of the Complaint as if fully set forth herein.

63. Defendants stole Plaintiff's highly confidential emails by intentionally accessing, or directing others to access for their benefit, one or more computers, data storage

facilities or communication facilities owned by Plaintiff or his email provider, AOL. This access of Plaintiff's emails and his email accounts was entirely without authorization and in violation of AOL's terms of service, and Defendants thereby obtained and stole information in the computers or facilities of AOL or Plaintiff that Defendants were not entitled to obtain. To the extent Defendants' initial access of AOL's publicly available website was authorized, Defendants and their co-conspirators exceeded such authorized access and violated AOL's terms of service by using such access to hack Plaintiff's email accounts and obtain and steal information in the computers or facilities of AOL that Defendants were not entitled to obtain.

64. The computers, data storage facilities, or communication facilities that were improperly accessed were and are used in and/or affect interstate and/or foreign commerce and/or communication.

65. This conduct violated 18 U.S.C. § 1030(a)(2)(C).

66. Defendants carried out this theft of Plaintiff's highly confidential emails knowingly and with intent to defraud Plaintiff and by the means described above. By means of such conduct, Defendants furthered their intended fraud and obtained something of value -- Plaintiff's emails, the confidential information contained therein and Plaintiff's litigation and negotiating strategy.

67. The object of the fraud and the things obtained did not consist only of the use of the computer or computers; rather the goal was to surreptitiously obtain the confidential information contained in the emails to further Defendants' goal of depriving Plaintiff of his rightful assets.

68. This conduct violated 18 U.S.C. § 1030(a)(4).

69. Defendants -- or others acting at their direction and for their benefit -- transferred or otherwise disposed of Plaintiff's AOL email passwords to another person without authorization, or obtained control of them without authorization with intent to transfer or dispose of them. Defendants did this knowingly and with the intent to defraud Plaintiff. Defendants and/or those working at their direction used these passwords to steal Plaintiff's emails.

70. This conduct affected interstate or foreign commerce because Defendants and/or persons acting at their direction and for their benefit, were operating from New York and the United Kingdom at the time of the transfer or obtaining of control, Plaintiff and his computers were situated in California, and AOL's servers were located elsewhere in the United States.

71. This conduct violated 18 U.S.C. § 1030(a)(6).

72. This offense was committed for purposes of commercial advantage or private financial gain and in furtherance of unlawful and tortious conduct.

73. As a result of these multiple and egregious violations, Plaintiff has incurred costs aggregating far more than \$5,000 in responding to these violations since August 2009. Plaintiff's costs include, but are not limited to, the costs of assessing the damage to his computers and systems, protecting against further compromise, and determining the cause and source of the violations. He has also suffered the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

74. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, plus interest for these wrongful, intentional and malicious acts.

**THIRD CAUSE OF ACTION**  
**(Violation of the Wiretap Act,  
18 U.S.C. § 2510, et seq.)**

75. Plaintiff repeats and re-alleges each of the allegations set forth in preceding paragraphs of the Complaint as if fully set forth herein.

76. To accomplish their theft of Plaintiff's highly confidential emails, Defendants and/or someone procured by them for their benefit intentionally intercepted or endeavored to intercept Plaintiff's emails.

77. This conduct violated 18 U.S.C. § 2511(1)(a).

78. Defendants and/or persons acting at their direction and for their benefit intentionally disclosed, or endeavored to disclose, the contents of the stolen emails to other persons. Defendants and/or persons acting at their direction and for their benefit posted Plaintiff's highly confidential emails on the [www.jackshome.info](http://www.jackshome.info) website for the purpose of facilitating access to the emails by Defendants and their co-conspirators.

79. Defendants knew or had reason to know at the time that these emails had been wrongfully intercepted, in violation of 18 U.S.C. § 2511(1)(a).

80. This conduct violated 18 U.S.C. § 2511(1)(c).

81. Defendants and/or persons acting at their direction and for their benefit intentionally used, or endeavored to use, the contents of the stolen emails. Defendants and/or persons acting at their direction and for their benefit, accessed and downloaded Plaintiff's highly confidential emails from the [www.jackshome.info](http://www.jackshome.info) website for their use.

82. Defendants have used the information in those emails to gain an unlawful advantage in Defendants' disputes with Plaintiff.

83. Defendants knew or had reason to know at the time that these emails had been wrongfully intercepted, in violation of 18 U.S.C. § 2511(1)(a).

84. This conduct violated 18 U.S.C. § 2511(1)(d).

85. This offense was committed for purposes of commercial advantage or private financial gain and in furtherance of unlawful and tortious conduct.

86. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

87. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, but no less than the statutory amounts (the greater of \$100 a day for each day of violation or \$10,000), plus interest; any profits made by Defendants as a result of the violations; attorney's fees and costs; and punitive damages for these wrongful, intentional and malicious acts.

**FOURTH CAUSE OF ACTION**  
**(Conversion)**

88. Plaintiff repeats and re-alleges each of the allegations set forth in preceding paragraphs of the Complaint as if fully set forth herein.

89. Plaintiff owns or has a right to the exclusive possession or control of the highly confidential information contained in the stolen emails. Plaintiff also has a reasonable expectation of such exclusive possession or control in these communications and information.

90. Defendants and/or persons acting at their direction and for their benefit stole Plaintiff's emails through hacking or other means, and this theft resulted in a wrongful disposition of Plaintiff's property right.

91. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

92. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, plus interest, as well as punitive damages, because these actions constituted oppression, fraud, and/or malice under Cal. Civ. Code § 3294.

**FIFTH CAUSE OF ACTION**  
**(Aiding and Abetting Conversion)**

93. Plaintiff repeats and re-alleges each of the allegations set forth in preceding paragraphs of the Complaint as if fully set forth herein.

94. Plaintiff owns or has a right to the exclusive possession or control of the highly confidential information contained in his stolen emails. Plaintiff also has a reasonable expectation of such exclusive possession or control in these communications and information.

95. Defendants assisted presently unknown third-parties and/or each other, to accomplish the theft of Plaintiff's highly confidential emails. Defendants were aware of the scheme to steal Plaintiff's emails, and they actively provided substantial assistance in furtherance of the scheme. Defendants directed the unlawful taking and use of Plaintiff's passwords to his email accounts, the theft of Plaintiff's emails by hacking or other means, and the planning of these wrongful activities.

96. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

97. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, plus interest, as well as punitive damages, because these actions constituted oppression, fraud, and/or malice under Cal. Civ. Code § 3294.

**SIXTH CAUSE OF ACTION**  
**(Violation of the Right to Privacy**  
**Under California Law)**

98. Plaintiff repeats and re-alleges each of the allegations set forth in the preceding paragraphs of the Complaint as if fully set forth herein.

99. The unlawful access by Defendants and/or persons acting at their direction and for their benefit, to Plaintiff's emails was an unwanted intrusion into Plaintiff's private conversations and matters. The stolen emails contained highly confidential and privileged communications with counsel, as well as Plaintiff's confidential financial and medical information. Plaintiff has a reasonable expectation of privacy in these communications and information.

100. The malicious intrusion through hacking or other means would be highly offensive to any reasonable person, given the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion. Defendants' unlawful motives and objectives make the intrusion even more offensive.

101. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

102. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, plus interest, as well as punitive damages, because these actions constituted oppression, fraud, and/or malice under Cal. Civ. Code § 3294.

**SEVENTH CAUSE OF ACTION**  
**(Aiding and Abetting**  
**Violation of the Right to Privacy)**

103. Plaintiff repeats and re-alleges each of the allegations set forth in the preceding paragraphs of the Complaint as if fully set forth herein.

104. Defendants assisted presently unknown third-parties, and/or each other, to accomplish the theft of Plaintiff's highly confidential emails. Defendants were aware of the scheme to steal Plaintiff's emails, and they actively provided substantial assistance in furtherance of the scheme. Defendants directed the unlawful taking and use of Plaintiff's passwords to his email accounts, the theft of Plaintiff's emails by hacking or other means, and the planning of these wrongful activities.

105. The unlawful access to Plaintiff's emails was an unwanted intrusion into Plaintiff's private conversations and matters. The stolen emails contained highly confidential and privileged communications with counsel, as well as Plaintiff's confidential financial and medical information. Plaintiff has a reasonable expectation of privacy in these communications and information.



106. The malicious intrusion through hacking or other means would be highly offensive to any reasonable person, given the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion. Defendants' unlawful motives and objectives make the intrusion even more offensive.

107. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

108. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, plus interest, as well as punitive damages, because these actions constituted oppression, fraud, and/or malice under Cal. Civ. Code § 3294.

**EIGHTH CAUSE OF ACTION**  
**(Violation of the California Computer Data Access  
and Fraud Act, Cal. Penal Code § 502)**

109. Plaintiff repeats and re-alleges each of the allegations set forth in preceding paragraphs of the Complaint as if fully set forth herein.

110. Defendants and/or persons acting at their direction and for their benefit, knowingly accessed and without permission used one or more computers, computer systems, or computer network facilities owned by Plaintiff or AOL, in order to wrongfully obtain Plaintiff's emails and the information contained therein and to wrongfully obtain money and property.

111. This conduct violated Cal. Penal Code § 502(c)(1).

112. Defendants knowingly accessed and without permission took, copied, or made use of the information in Plaintiff's emails, or directed others to do so for their benefit,

from one or more computers, computer systems, or computer network facilities owned by Plaintiff or AOL, in order to wrongfully obtain Plaintiff's emails and the information contained therein.

113. Defendants, or persons acting at their direction and for their benefit, posted Plaintiff's highly confidential emails on a website, accessed that information, and used the information in those emails to gain an unlawful advantage in their disputes with Plaintiff.

114. This conduct violated Cal. Penal Code § 502(c)(2).

115. Defendants knowingly and without permission used or caused to be used computer services provided by AOL by improperly accessing one or more of Plaintiff's highly confidential emails through the unauthorized use of Plaintiff's AOL account.

116. This conduct violated Cal. Penal Code § 502(c)(3).

117. Defendants and/or persons acting at their direction and for their benefit, knowingly and without permission provided, or assisted in providing, a means of accessing one or more computers, computer systems or computer network facilities owned or used by Plaintiff or AOL, in violation of Cal. Penal Code § 502(c). Defendants and/or others acting at their direction and for their benefit took these actions in execution of their plan to unlawfully take and use Plaintiff's passwords to his email accounts and thereby access his highly confidential emails.

118. This conduct violated Cal. Penal Code § 502(c)(6).

119. To accomplish their theft of Plaintiff's highly confidential emails, Defendants and/or persons acting at their direction and for their benefit, knowingly and without permission accessed or caused to be accessed one or more computers, computer systems or computer network facilities owned or used by Plaintiff or AOL.

120. This conduct violated Cal. Penal Code § 502(c)(7).

121. Plaintiff has incurred substantial losses as a result of Defendants' conduct. Plaintiff's losses include, but are not limited to, the costs of assessing the damage to his computers and system, protecting against further compromise, and determining the cause and source of the violations, and the consequences flowing from the disclosure of privileged and confidential strategic legal advice.

122. As a result of these violations, Plaintiff is entitled to an award of damages in an amount to be determined at trial, plus interest; attorney's fees and costs; and punitive damages, because these actions constituted oppression, fraud, and/or malice under Cal. Civ. Code § 3294 and they were all done willfully.

WHEREFORE, Plaintiff hereby demands judgment:

A. Preliminarily and permanently enjoining Defendants from using in any way the information obtained from Plaintiff as a result of the alleged wrongdoing, and further preliminarily and permanently enjoining Defendants from accessing or attempting to access, or soliciting any third parties to access or attempt to access, any electronic communications made by Plaintiff and not directed to Defendants, if such action would violate any state or federal statutory or common law; and

B. Preliminarily and permanently enjoining Defendants from taking any action to erase or destroy any evidence of any of the activities described in this Complaint, or from directing or permitting any third-party from taking any such action, except as set out below; and

C. Ordering that, after the issuance of a final, non-appealable judgment in this action and then only with the express permission of this Court or Plaintiff, Defendants to

destroy all the information obtained from Plaintiff as a result of the alleged wrongdoing in their possession, custody or control; and

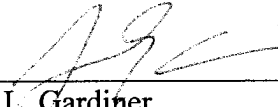
D. Awarding damages in an amount to be determined at trial, including any profits made by Defendants as a result of the alleged wrongdoing, plus interest, attorney's fees and costs, and punitive damages; and

E. Awarding such other, further and different relief as the Court shall deem proper.

**JURY DEMAND**

Plaintiff hereby demands trial by jury of all claims triable to a jury.

Dated: September 22, 2009  
New York, New York

  
\_\_\_\_\_  
John L. Gardiner  
SKADDEN, ARPS, SLATE,  
MEAGHER & FLOM LLP  
Four Times Square  
New York, New York 10036-6522  
(212) 735-3000  
john.gardiner@skadden.com

Attorneys for Plaintiff  
Bassam Y. Alghanim

Of Counsel:  
John A. Donovan  
SKADDEN, ARPS, SLATE, MEAGHER  
& FLOM LLP  
300 South Grand Avenue  
Suite 3400  
Los Angeles, CA 90071-3144  
(213) 687-5000