

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BASSAM Y. ALGHANIM,

Plaintiff,

v.

KUTAYBA Y. ALGHANIM, OMAR K.
ALGHANIM, ALGHANIM INDUSTRIES
COMPANY W.L.L., YUSUF AHMED
ALGHANIM AND SONS W.L.L., and
WALEED MOUBARAK,

Defendants.

:
:
: 09 Civ. 8098 (NRB)
:
:

**DECLARATION OF JOHN L.
GARDINER IN OPPOSITION
TO MOTION TO DISMISS
AND/OR STAY ACTION IN
FAVOR OF ARBITRATION**

JOHN L. GARDINER, an attorney duly admitted to practice before this Court,
declares under penalties of perjury pursuant to 28 U.S.C. §1746 as follows:

1. I am a partner in the law firm of Skadden, Arps, Slate, Meagher & Flom LLP, counsel to Plaintiff Bassam Y. Alghanim (“Bassam” or “Plaintiff”) in this action. I submit this declaration in opposition to the motion of defendants Kutayba Y. Alghanim (“Kutayba”), Omar K. Alghanim (“Omar”) and Waleed Moubarak (“Moubarak”) to dismiss this action in favor of arbitration and to place before the Court certain facts relevant to the motion

2. As alleged in the First Amended Complaint, this case involves an unlawful scheme orchestrated by the Individual Defendants,¹ and paid for by companies they control, to hack into the Plaintiff’s private password protected email accounts at AOL. It is these

¹ As used herein, “Individual Defendants” refers to Kutayba, Omar and Moubarak collectively.

allegations and the causes of action that arise from them that the Individual Defendants assert should be dismissed in favor of arbitration before the Kuwait Prime Minister.

3. In considering Defendants' arguments we ask the Court to carefully consider the specific facts underlying the First Amended Complaint and the causes of action that Plaintiff brings in seeking redress for such wrongdoing. This is something that the Individual Defendants all but ignore in their moving papers. For this reason, I submit this transmittal declaration to place before the Court some of the evidence gathered to date that supports the allegations made in the First Amended Complaint.

Summary of Facts Established Through the English Proceedings

4. On November 2, 2009, Plaintiff filed his Particulars of Claim in the English action that he commenced against Mr. Timothy Zimmer ("Zimmer"), Mr. Steven McIntyre ("McIntyre") and certain companies owned or affiliated with Mr. McIntyre arising out of their role in the alleged email hacking scheme. In his Particulars of Claim, which were based on the results of the investigation conducted to date in England, including on sworn statements filed by Messrs. Zimmer and McIntyre in that action, Plaintiff set forth detailed facts of those defendants' roles in the email hacking scheme. (A copy of the Plaintiff's Particulars of Claim is attached hereto as Exhibit A.)

5. In response to these Particulars, Mr. Zimmer submitted a defense in which he has admitted to hacking into Plaintiff's email accounts and to stealing the contents of his emails and has sought to apologize to Plaintiff. (See Exhibit B hereto, Defence of Mr. Timothy Zimmer dated November 20, 2009).

6. In contrast, although Mr. McIntyre has acknowledged that the documents obtained by Mr. Zimmer were delivered to him or his company 2-3 times a week for over one

year and that he arranged for delivery of those documents to Omar and Moubarak, he asserts that he never actually read any of the documents he received from Mr. Zimmer and that he believed they contained only publicly available information concerning Plaintiff. (See Exhibit C hereto, Defence of Steven McIntyre, Verify Limited and Cerule Limited dated November 30, 2009, at ¶¶ 1-5).

7. However, Mr. McIntyre has stated that he made the documents obtained from Mr. Zimmer (which Mr. Zimmer concedes comprised the stolen emails) available to Defendants Omar and Moubarak. As stated in his Defence, Exhibit C hereto, “[Mr. Zimmer] would produce material up to several times a week during the course of the investigation. Initially, in July 2008, this information was hand delivered to Mr. Alghanim. However, later, to facilitate the information transfer it was scanned at the offices of [Cerule Ltd.] and uploaded by ftp to a website set up by [Mr. Zimmer] to which Mr. Alghanim was given access.” (Exhibit C at ¶ 4; see also id. at ¶ 16xi). Mr. McIntyre has also submitted an affidavit in which he swore that “Cerule Limited scanned and provided documents supplied by Tim Zimmer to an FTP website known as www.jackshome.info. www.jackshome.info was accessible by Omar Alghanim and Waleed Mubarak.” (See Exhibit D hereto, Affidavit of Steven McIntyre sworn to October 2, 2009 (hereafter “McIntyre Aff.”), at ¶ 8).

8. A forensic analysis conducted by Stroz Friedberg, a forensic consultancy firm retained by Plaintiff, has identified multiple accesses to the website from an Internet Protocol (“IP”) address associated with defendants Omar and Kutayba’s residence in New York. (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.) (See Exhibit E hereto, Report of Investigation, dated September 20, 2009 (the “SF Report”), at pp. 15-17).

9. In addition, Stroz Friedberg has stated that access to the website occurred from IP addresses that could be associated with Moubarak. (*Id.* at p. 15-16).

10. Stroz Friedberg also noted that as of September 7, 2009 the content of the jackshome.info website had changed and that the PDF files that previously had been available on the site (*i.e.*, the stolen emails) no longer were available on the site and that publicly available information had been uploaded in its place. (*Id.* at p. 8).

Summary of Causes of Action Alleged in the First Amended Complaint

11. Based upon these alleged facts, additional evidence in support of which is laid out below, the first three counts in the First Amended Complaint allege violations of United States federal criminal laws specifically related to computers and/or information protection. As set out in the First Amended Complaint, these are Count I (Violation of the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*); Count II (Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030); Count III (Violation of the Wiretap Act, 18 U.S.C. § 2510, *et seq.*).

12. Counts IV and V allege violations of United States federal racketeering laws. Specifically, Count IV is for a Violation of RICO, 18 U.S.C. § 1962(c) and Count V is for a Violation of RICO, 18 U.S.C. § 1962(d).

13. The First Amended Complaint also contains two causes of action based on the common law of conversion and on the wrongful disposition of a right to property. These are Count VI (Conversion) and Count VII (Aiding and Abetting Conversion). The allegedly converted property consists of the hacked emails (and information contained in them) that were obtained by the Individual Defendants.

14. Count VIII is for a Violation of the Right to Privacy Under California Law. This is a common law tort cause of action for an improper intrusion into plaintiff's private places, conversations, or matters in a manner highly offensive to a reasonable person and Count IX is for Aiding and Abetting Violation of the Right to Privacy Under California Law. This is a common law tort cause of action against persons who knowingly substantially assist an invasion of privacy.

15. The First Amended Complaint contains one further cause of action, for violation of a California state criminal statute. This is Count X (Violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502).

16. Each of these causes of action is based on the email hacking scheme alleged in the First Amended Complaint. Some of the evidence in support of these causes of action already obtained by Plaintiff is set forth below.

The Email Hacking Engaged In By Mr. Zimmer

17. Mr. Zimmer has sworn that he “obtained [Bassam’s] email password via the website ‘Invisible Hacking Group’. . . .” (See Exhibit F hereto, Affidavit of Timothy Zimmer, sworn to October 2, 2009, (hereafter, “Zimmer Aff.”) at ¶ 12).

18. Mr. Zimmer also has sworn that he “obtained [Bassam’s] password in July 2008 and [he] accessed his email accounts shortly afterwards.” (Id. at ¶ 22).

19. Mr. Zimmer has sworn that he “continued to access the accounts regularly until 12 August 2009.” (Id.)

20. August 12, 2009 is when Plaintiff changed his email passwords.

21. The record further shows that immediately after Plaintiff changed his AOL email passwords, on August 12, 2009, Mr. Zimmer attempted to obtain the new passwords from

the Invisible Hacking Group so that he could continue to hack Plaintiff's emails. For example, on August 12, 2009, Mr. Zimmer emailed the Invisible Hacking Group about the password changes (Exhibit G hereto):

"I have two addresses that you did for me a long time ago, they have changed there [sic] password and I can not get back in, please can you try again.

berryhoney@aol.com
old password was: bas22sam

bassam101@aol.com
old password was: ahlam18

... Please try your best urgently ..."

22. On August 17, 2009, Mr. Zimmer sent a follow-up email to Invisible Hacking Group about the password changes (Exhibit G hereto):

"I am willing to pay more for these ones, please keep trying very urgent."

23. On August 29, 2009, Mr. Zimmer sent another follow-up email to the Invisible Hacking Group about the password changes (Exhibit H hereto):

"Any news the aol ones are very urgent. Thanks"

24. On August 31, 2009, Mr. Zimmer reiterated that he was willing to pay an increased amount for the new email passwords (Exhibit I hereto):

"My offer still stands £500 for each of the aol ones I gave you, very very urgent. Please keep trying."

25. In short, the record shows that Mr. Zimmer had no intention of stopping his activities just because Plaintiff had changed his AOL passwords.

Mr. Zimmer Delivered the Fruits of His Hacking to Mr. McIntyre and His Companies for Onward Transmittal to the Individual Defendants

26. Mr. Zimmer has sworn that he delivered the fruits of his hacking of Plaintiff's emails to "Cerule Limited and Steven McIntyre trading as Cerule both of 6 Malthouse Lane, Reading RG17JA." (See Exhibit F, Zimmer Aff., at ¶ 21).

27. He has also sworn that: "Prior to May 2009 I printed hard copies of various emails from the Claimant's inbox, which I supplied to Cerule. After May 2009 I also created copies (in PDF format) of certain emails." (Id. at ¶ 8).

28. Mr. McIntyre has sworn that "[d]ocuments relating to the Applicant were provided to Cerule Limited by Timothy Zimmer" (See Exhibit D, McIntyre Aff., at ¶7).

29. Mr. McIntyre has further sworn that Cerule "received documents from Tim Zimmer approximately every 2-3 days over the period from July 2008 to August 2009. The quantity supplied on each occasion varied but as far as I am aware, having made enquiries of the office staff, on average would have been about 20 pages." (Id. at ¶ 9).

30. Mr. McIntyre swore that on July 20, 2008, he personally delivered over 300 pages of Mr. Zimmer's work product to defendant Omar on one of the Defendants' yachts, which was moored in Capri at the time. (Id. at ¶ 9(a)).

31. According to Mr. McIntyre, another personal delivery of Mr. Zimmer's work product took place four days later when, on July 24, 2008, Mr. Steven Hullah, one of Mr. McIntyre's employees, delivered another batch of Mr. Zimmer's work product to Omar on his yacht, this time when it was moored in Sardinia. (Id. at ¶ 9(b)).

The Individual Defendants' Access to the Covert Website

32. It appears that having to personally deliver the fruits of Mr. Zimmer's labors to Omar as he moved around on his yacht was considered cumbersome in this electronic age. As a result, Mr. Zimmer established a website that was used to host Mr. Zimmer's work product (which Mr. Zimmer, at least, concedes, consisted of the stolen emails).

33. As reported in the SF Report, Mr. Zimmer established a website known as www.jackshome.info under the name of a purported person called Jack Jones of 25 Church Road, Rustington, Bognor BN16 3NN as registrant, and an email address of harryj665@yahoo.co.uk, which email address subsequently turned out to be under the control of Mr. Zimmer. (See Exhibit E, SF Report, at pp. 7-8).

34. The website itself was hosted by a company called GX Networks Limited ("GX") and it was created as a website utilizing File Transfer Protocol ("FTP") for the use and exchange of data. The website utilized user based password authentication. (*Id.* at pp. 11-12).

35. Documents recently discovered on Mr. Zimmer's computer suggest that there was some problem with access to the website at some point in time which caused Mr. Zimmer to email Bryan Miller and Steven Hulland, both of whom were employed by Mr. McIntyre's company, Cerule Ltd., on May 1, 2009 stating:

"Hi Bryan

Sorted. New address: <ftp://jackshome.info>

UserName: ftp@jackshome.info

Password: aceshigh11

All working"

(See Exhibit J hereto).

36. As set forth in the SF Report, the documentary evidence confirms that IP addresses associated with the Individual Defendants repeatedly accessed the

www.jackshome.info website using the correct user name and password from at least June 1, 2009 until August 20, 2009. (See Exhibit E, SF Report, at pp.13-17).

37. In this respect, Plaintiff has obtained from AOL the AOL log on files for each of his compromised AOL email accounts for the period June 1, 2009 through August 20, 2009. (See Exhibit K hereto). As Stroz Friedberg notes, the AOL log files contained, *inter alia*, each originating IP address from which a user had connected to the particular AOL account, either berryhoney@aol.com or bassam101@aol.com, during this time period and the date and time of the connections. (See Exhibit E, SF Report, at pp. 8-10).

38. Plaintiff also has obtained log-on information to jackshome.info from GX. (See Exhibit L hereto). As Stroz Friedberg notes, these logs show the IP addresses from which persons logged on to the FTP site, www.jackshome.info, for which a user needed to have a password. (See Exhibit E, SF Report, at pp. 10-12).

39. Stroz Friedberg has examined these logs, and other physical evidence. In their Report, which was issued before Mr. Zimmer and Mr. McIntyre submitted their respective affidavits and defenses referred to above, Stroz Friedberg concluded that during the period May 2009 to August 12, 2009:

- (A) Plaintiff's AOL email accounts were repeatedly accessed from a location in Reading, England which appeared to be associated with Timothy Zimmer. (*Id.* at pp. 8-10). (As noted above, Mr. Zimmer has since admitted that he is the person who did the accessing and has sought to apologize to Plaintiff).
- (B) Files containing emails from the hacked email accounts were copied and converted to PDF files, which were then uploaded to the www.jackshome.info website from an IP address that appeared to come back to Verify Ltd., a company associated with Mr. McIntyre. (*Id.* at pp. 12-13). (As noted above, although he denies reading the documents supplied by Mr. Zimmer, Mr. McIntyre has since admitted that he and his employees were, in fact, responsible for uploading the documents they got from Mr. Zimmer to the website.)

- (C) The website had been created as a website likely intended to be accessed through FTP only, that is by a user who had the correct username and password. (Id. at p.11).
- (D) 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 gain entry to the site. (Id.) (As noted above, Mr. McIntyre has since sworn that he supplied the user name and password to Omar and Moubarak so that they could access the website.)
- (E) Once the PDF files of Plaintiff's emails had been uploaded to the website, users, who had the correct username and password, accessed that website, viewed the stolen emails and downloaded the copies of them. (See id. at pp. 13-17).

40. As noted in the SF Report at pages 8-10, from May 2, 2009 until August 12, 2009, 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, IP 84.12.61.188. The AOL logs for each of the hacked email accounts show numerous additional accesses made 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. confirms that most, if not all, of these IP addresses were associated with Mr. Zimmer.

41. Likewise, as noted in the SF Report at pages 13-17, information obtained to date demonstrates clearly that in the final six weeks of this time frame -- June 2, 2009 to August 12, 2009 -- a single IP address in the U.K. uploaded PDF files containing the stolen emails to the www.jackshome.info 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 M).

42. Invoices from Cerule Ltd. to Alghanim Industries and YAAS and other accounting records were found in Cerule's offices. On a single project entitled "IT Security," Cerule billed a total of almost \$200,000 for just the period April-September 2009. (See Exhibit D, McIntyre Aff., at Exs. 1-6).

43. As noted in the SF Report, in just the eleven week period between June 1, 2009 and August 20, 2009, PDFs from the website were downloaded more than 250 times. (See Exhibit E, SF Report, at pp. 13-17). More than 100 of the downloads from the website were conducted from IP addresses in the United States, and nearly all of those were from IP addresses located in New York City. (Other downloads were made from IP addresses located in California, Lebanon, Kuwait and the U.K.) (Id.)

44. As noted in the SF Report, the New York IP address most frequently used to view and download Plaintiff's confidential emails is an IP address associated with Defendants Kutayba's and Omar's Manhattan residence, 15 East 81st Street, New York, New York. (Id. at p. 16). For instance, over a two-month period between June 19, 2009 and August 20, 2009, files from the website were downloaded from this address at least 71 times. (Id. at p.15). (A copy of an extract showing the times and dates of the downloads from the IP address associated with the Manhattan residence is attached hereto as Exhibit N.)

45. Evidence gathered to date demonstrates that IP addresses associated with defendant Moubarak were used to access the website. For example, guest lists produced in this action by Gramercy Park Hotel indicate that Moubarak was staying at the hotel on dates when access to the website occurred from an IP address associated with that hotel. In addition, the Stroz Friedberg Report identifies other IP addresses used to access the website from locations in

San Diego. Stroz Friedberg concludes that such access may have been from the home of Moubarak's family. (See Exhibit E, SF Report, at pp.14-15).

46. In sum, the accumulated data shows that the following pattern was repeated scores of times: (i) Mr. Zimmer unlawfully accessed Plaintiff's email accounts for over a year; (ii) PDF copies of the stolen emails were created and uploaded to the jackshome.info website; (iii) the user name and password to the website were provided by Mr. McIntyre to Omar and Moubarak; and (iv) IP addresses associated with the Individual Defendants accessed the jackshome.info website and downloaded the newly-uploaded stolen emails using the unique user name and password associated with the website.

The Attempted Cover-Up

47. By early September 2009, it appears that Mr. Zimmer understood that the contents of the www.jackshome.info website might have been indexed by Google and that, therefore, the contents might have become visible through web searches and not just to persons who had been provided the secret FTP passwords. This meant that others could access the website and that the unlawful scheme was capable of detection.

48. As noted above, Stroz Friedberg stated in its September 20, 2009 Report, Exhibit E hereto, that the content of the website had been removed in early September 2009. Stroz Friedberg has now prepared a Supplemental Report, dated December 17, 2009, a copy of which is attached hereto as Exhibit O (the "SF Supplemental Report"), for the limited purpose of summarizing the electronic evidence found in the review performed in the UK.

49. In the SF Supplemental Report, Stroz Friedberg states that its analysis of the GX Networks logs and additional data obtained off computers seized in the UK indicates

purposeful deletion of material from the website during the period September 4, 2009 through September 6, 2009. (Ex. O, SF Supplemental Report at 8-9).

50. As Stroz Friedberg notes, Mr. Zimmer reported the outcome of his cover-up activities to Mr. McIntyre and Mr. Hulland stating:

“I have attached an idea for the report re what happened this weekend technical issue, it’s safe to send to you as no references to anything. Let me know if you want to go down this route for the report, it’s a bit weak but certainly viable, let me know and I can beef it up in the morning.”

The Attachment states:

“Firstly, everything has been removed, we have checked Google, Yahoo, AOL, AltaVista, Bing, Metacrawler and Ask Jeeves from multiple locations around the world and none of these search engines display any of the product.”

(Ex. O, SF Supplemental Report at pp. 8-9 & Exs. S15, S16; see also Exhibit P hereto).


51. As set forth in the SF Supplemental Report at pages 9-10, this explanation appears implausible. It appears more likely that the results of Mr. Zimmer’s hacking activity became known through the uploading process when files appear to have been loaded to a directory that permitted public access to uploaded material on the website.

The September 16, 2009 Meeting in New York

52. It appears that following these events a meeting was held in New York between representatives of Cerule and “the client.” (See Ex. O, SF Supplemental Report at pp. 10-11).

53. Shortly after this meeting, Plaintiff filed his Complaint and this Court issued a Temporary Restraining Order preventing the destruction of evidence by Kutayba and Omar.

Dated: December 18, 2009
New York, New York



John L. Gardiner