UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

LEOR EXPLORATION & PRODUCTION LLC, et al.,

Plaintiffs,

vs.

GUMA AGUIAR,

Defendant.
_____/

CASE NO. 09-60136-CIV-SEITZ/O'SULLIVAN

GUMA AGUIAR,

Plaintiff,

vs.

WILLIAM NATBONY, et al.,

Defendants.
_____/

CASE NO. 09-60683-CIV-SEITZ/O'SULLIVAN

MOTION FOR SANCTIONS AGAINST GUMA AGUIAR AND FOR EXPEDITED EVIDENTIARY HEARING

Guma Aguiar, together with his co-conspirators at a small Israeli technology company called PCIC Group Ltd. ("PCIC"), directed the unlawful "hacking" of Thomas Kaplan's only email account. This hacking occurred through the server files of PCIC and through the use of Aguiar's email address **guma@mail.pcic.co.il** hosted on a PCIC server in Israel, where Aguiar currently lives and spends a substantial amount of his time. The hacking allowed Aguiar unfettered access, without Kaplan's consent, to Kaplan's entire email account, including thousands of sensitive and confidential emails. Among these were almost every written, privileged communication Kaplan has had with his legal counsel in this case and related cases, including communications about litigation strategy, claims, defenses, and discovery. Guma

Aguiar now knows, or had the ability to learn, his adversary's most confidential information.

Despite having already been admonished by this Court for tampering with witnesses -- indeed, the Court enjoined Aguiar from further witness tampering [D.E. 55] -- Aguiar told the Israeli press in an interview published on August 21, 2009 that he intended to engage in industrial espionage against Kaplan.[1] Compelling evidence establishes that Aguiar made good on that threat by illegally accessing Kaplan's most confidential and privileged communications. This type of behavior is reprehensible and disruptive, and there is no remedy that would enable Kaplan and the other parties in these cases to litigate on an even playing field. Accordingly, the only appropriate sanction is to strike Aguiar's pleadings.

The Eleventh Circuit has approved the sanction of default and dismissal for this very sort of misconduct, which completely undermines the judicial process. *Eagle Hospital Physicians, LLC v. SRG Consulting, Inc.*, 561 F.3d 1298, 1306 (11th Cir. 2009). Given the severity of Guma Aguiar's misconduct and its resulting irreparable harm, coupled with Aguiar's prior misconduct and recent threat to engage in industrial espionage, this Court should conduct an immediate evidentiary hearing and compel Guma Aguiar to testify regarding that misconduct with the result that this Court should sanction Guma Aguiar by striking his pleadings, dismissing his claims, and entering a default judgment against him.[2]

I. FACTS

1. For the past seven years, Kaplan has used as his sole email address

[1] *See Maariv Weekend*, Aug. 21, 2009, at 14 (translation attached as Exhibit "A").

[2] This motion requests relief on behalf of the Plaintiffs (the "Leor Plaintiffs") in Case No. 09-60136-CIV-SEITZ (the "*Leor* Case") and all of the Defendants in Case No. 09-60683-CIV-SEITZ (the "*Katten* Case"). Thomas Kaplan is the controlling principal and/or beneficiary of the Plaintiffs in the *Leor* Case, is a defendant in the *Katten* Case, and has a joint litigation agreement with all of the parties in both the *Leor* Case and the *Katten* Case. The interception of Kaplan's emails has therefore affected, and materially prejudiced, all of these parties.

Kaplan600@aol.com (the "Kaplan Email Address"), a web-based email account supplied by his internet service provider, America Online ("AOL"). Kaplan maintains his personal and business emails -- totaling more than 45,000 -- on his AOL email account (the "AOL Email Account"). *See* Declaration of Thomas Kaplan ("Kaplan Decl."), ¶ 2 (attached as Exhibit "B").

2. All written communications between Kaplan and his attorneys in the *Leor* Case, the *Katten* Case, and the other pending lawsuits filed by or against Guma Aguiar (which discuss the specifics of confidential and privileged litigation strategy, including the analysis of claims, defenses and discovery), and between Kaplan and his bankers, brokers and business associates (which discuss Kaplan's confidential personal, business and financial interests), have been through emails using the Kaplan Email Address, and all such emails are stored in Kaplan's AOL Email Account. Kaplan Decl., ¶¶ 2-3.

3. Kaplan has kept confidential his password to access the emails in his AOL Email Account, and has never granted authorization to Guma Aguiar or anyone else to use or access Kaplan's AOL Email Account. Kaplan Decl., ¶ 2.

4. Between at least August 17, 2009 and September 7, 2009, Kaplan's AOL Email Account was breached without Kaplan's authorization or consent using a PCIC server and a PCIC email mailbox, **guma@mail.pcic.co.il,** owned or used by Guma Aguiar. *See* Declaration of Andrew P. Obuchowski, Jr. ("Obuchowski Decl."), ¶¶ 2-19 (attached as Exhibit "C"). After illegally gaining access to Kaplan's AOL Email Account, Aguiar -- through PCIC -- copied materials in Kaplan's account onto a PCIC server in one of two ways:

> [T]he Hacker copied all of the e-mail messages in the E-mail Account [or] . . . the Hacker copied information about all of the e-mail messages in the E-mail Account (the headers of the e-mail messages and perhaps even additional accompanying information), but only copied specific e-mail messages in their entirety. . . . Either way, the Hacker -- throughout the Penetration Period had full access to all of the e-mail messages in the E-mail Account -- or at some point had information

on all the e-mail messages that were in the E-mail Account that was penetrated. *See infra* Report of Maglan Information Defense & Intelligence (the "Maglan Report"), § 2, ¶ 3 (attached as Exhibit "D").

5. Not coincidentally, the hacking first occurred at least as early as August 17, 2009, which is contemporaneous with Guma Aguiar's statement to the Israeli press that he intended to engage in "industrial espionage" against Kaplan (*see* attached Exhibit "A"). *Id*. at § 2, ¶ 2.

6. The hacking was discovered by Kaplan in September 2009 when he learned that "read receipts" had been transmitted by a previously unknown email address that had accessed 14 emails sent to Kaplan -- 13 from his securities broker, Ronald Rothenberg, and one from his head of security, Itzhak Dar. Kaplan Decl., ¶ 3; Obuchowski Decl., ¶ 3; Maglan Report, § 1, ¶ 4. As explained below, the read receipts were generated by **guma@mail.pcic.co.il,** an email address owned or used by Guma Aguiar and hosted on PCIC's email server. Obuchowski Decl., ¶¶ 8, 10, 13-17; Maglan Report, § 1, ¶ 3-4.

7. A "read receipt request" is an email messaging option that allows the sender of an email to request the recipient of such email to confirm receipt of the email via an electronically-generated "read receipt." The recipient of such email has the ability to automatically or manually transmit a read receipt back to the sender's email address. The ability to automatically or manually respond to a read receipt request is established by configuring the settings in the recipient's email software. When the recipient configures his email software to generate read receipts, an email message is transmitted to the sender's email account that requested the read receipt. Obuchowski Decl., ¶ 5.

8. When Kaplan suspected that a third person had wrongfully hacked into his AOL Email Account, Kaplan through his counsel retained an IT/computer expert, Andrew

Obuchowski, employed by Kroll Ontrack, Inc., an IT consulting and forensics firm. Kaplan Decl., ¶ 4. Obuchowski examined the metadata[3] associated with the 14 emails for which read receipts had been generated by **guma@mail.pcic.co.il.**

9. Based on an examination of the metadata associated with the read receipts, Obuchowski concluded that a person using the email address **guma@mail.pcic.co.il** had hacked Kaplan's AOL Email Account, including emails between Kaplan and his broker and Kaplan and his head of security. Obuchowski Decl., ¶¶ 2-3.

10. The "read receipts" establish the following facts:

a. On September 7, 2009, **guma@mail.pcic.co.il** accessed Kaplan's AOL Email Account from a computer in Israel, using an email program in connection with a Microsoft Exchange environment;

b. The person using **guma@mail.pcic.co.il** had complete access to, and the ability to download, all of Kaplan's emails (not just the emails from Rothenberg and Dar), including his confidential and privileged communications with his attorneys in these lawsuits;

c. At least 14 emails containing read receipt requests were opened and read by the hacker using **guma@mail.pcic.co.il**;

d. The "read receipt" messages were sent from **guma@mail.pcic.co.il** using computers in Israel; and

e. The "read receipt" messages were being generated from a Microsoft Exchange email platform, which is different from the AOL email platform used by

[3] Metadata describes information embedded in an electronic file that shows how, when, and by whom a particular set of data was collected, and how the data is formatted. Obuchowski Decl., ¶ 7 n.1.

Kaplan. The most relevant difference is that the Microsoft Exchange email platform -- on which the **guma@mail.pcic.co.il** email address operates -- is configured to send read receipts; the AOL platform is not. Kaplan's web-based AOL Email Account is not configured to issue or process read receipt requests or to issue read receipts. Therefore, when Kaplan opens an email in his AOL Email Account, no "read receipt" response email is sent despite a request for one from a sender. Obuchowski Decl., ¶¶ 2-19; Maglan Report, at 3-6.

11. The email address **guma@mail.pcic.co.il** is not a sender or intended recipient of any emails in Kaplan's AOL Email Account. Kaplan has never heard of such an email address and has never permitted anyone at that email address to access his emails. Kaplan Decl., ¶ 2.

12. In an effort to protect Kaplan's confidential information and redress the injury caused by the theft of this information, Kaplan initiated legal proceedings in Israel against PCIC, the company that facilitated the hacking, and PCIC's owners. *See* Urgent Motion for Appointment of Receiver, filed in Jerusalem District Court, Civil Case 3485/09, attached as Exhibit "E" (without exhibits). The Israeli court appointed an independent receiver to search, copy and seize PCIC's computers and computer data to find information copied from Kaplan's AOL Email Account and/or information regarding the hacking into Kaplan's AOL Email Account.

13. Significantly, the Israeli court-appointed receiver has issued a preliminary report to the Israeli Court that, *inter alia*, concludes that the mailbox **guma@mail.pcic.co.il** belongs to Guma Aguiar and that "in the EXCHANGE file of the user guma@mail.pcic that was found on the server, there was unequivocal and unambiguous evidence that those exchanges of e-mail correspondence that were set forth in the Petition for Temporary Relief did in fact pass through

this server." *See* Seizure and Receivership Report ("Receiver's Report"), attached as Exhibit "F", ¶¶ 37, 39. The Receiver's Report further states that Guma Aguiar -- who was not a party to the Israeli receivership action -- contacted the receiver by telephone and indicated that he would invite "100 press representatives" to examine the receiver's work. *Id. at* ¶ 25.

14. Independent computer forensic experts in Israel have confirmed that Kaplan's emails were hacked using the email address **guma@mail.pcic.co.il.** *See* Receiver's Report, ¶ 37.

15. This is not the first time that Guma Aguiar has been involved in underhanded and possibly illegal acts. On May 15, 2009, the Plaintiffs in the *Leor* Case moved for an order enjoining Guma Aguiar from tampering with or harassing material witnesses in this lawsuit. [D.E. 55.] The Court on June 22, 2009, granted Kaplan's motion, holding that "Mr. Aguiar is enjoined from witness intimidation including prohibiting Mr. Aguiar or anyone on his behalf from coming within twenty (20) feet" of certain material witnesses or parties and their families. [D.E. 88.] At that time, Guma Aguiar was placed on notice by Kaplan's counsel and the Court that future improper conduct would be dealt with seriously. *See* June 22, 2009 Hearing Tr. at 18 ("[Y]ou need to have a sit down with this fellow and let him know how serious this is and how it could affect his lawsuit in the end if he continues with this."). Separately, Guma Aguiar has threatened to use other improper means to further his financial and litigation agenda, including industrial espionage. Guma Aguiar has executed on that threat.

II. ARGUMENT

"A court may impose sanctions for litigation misconduct under its inherent power." *Eagle Hospital*, 561 F.3d at 1306. *See also Chambers v. Nasco, Inc.*, 501 U.S. 32, 43-45 (1991) (explaining the Court's broad inherent powers). "The court's inherent power derives from the

court's need to 'manage [its] own affairs so as to achieve the orderly and expeditious disposition of cases.'" *Eagle Hospital*, 561 F.3d at 1306 (citation omitted). "A court may use its inherent powers to preserve the integrity of the judicial process and prevent the perpetration of fraud on the court." *Eagle Hospital Physicians, LLC v. SRG Consulting, Inc.*, No. 1:04-CV-1015-JOF, 2007 WL 2479290, *3 (N.D. Ga. Aug. 28, 2007), *aff'd*, 561 F.3d 1298 (11th Cir. 2009). *See also Smith v. Armour Pharm. Co.*, 838 F. Supp. 1573, 1578 (S.D. Fla. 1993) (same). Fraud on the court exists where "a party has essentially set in motion some unconscionable scheme calculated to interfere with the judicial system's ability impartially to adjudicate a matter by improperly influencing the trier or unfairly hampering the presentation of the opposing party's claim or defense." *Eagle Hospital*, 2007 WL 2479290, at *3 (citation omitted). *See also Allapattah Servs., Inc. v. Exxon Corp.*, 373 F. Supp. 2d 1344, 1373 (S.D. Fla. 2005) (striking defenses based on fraud on the Court).

Here, Kaplan has incontrovertible evidence that Guma Aguiar accessed Kaplan's emails, including privileged and confidential attorney-client communications. Such misconduct constitutes a fraud upon the Court and upon Kaplan and the other parties in these actions. Courts have not hesitated in such circumstances to dismiss the wrongdoer's claims and to strike the wrongdoer's defenses. In fact, "a court's inherent power to dismiss a case and protect the sanctity of the judicial process is never more compelling than in a situation of individuals who engage in fraud on the court." *Perna v. Elec. Data Sys., Corp.*, 916 F. Supp. 388, 397 (D.N.J. 1995).

In *Eagle Hospital*, the Eleventh Circuit upheld striking a party's pleadings for accessing privileged communications -- the same conduct present here -- because no lesser sanction could remedy such a profound harm. The individual defendant in *Eagle Hospital*, Dr. Gerst, the owner

of the two closely-held corporate defendants, had access to and improperly obtained plaintiff's privileged internal email communications. *Eagle Hospital*, 2007 WL 2479290, at *2. Plaintiff requested the District Court to sanction the defendants by, *inter alia*, striking defendants' answer and counterclaims and entering a default judgment against defendants. *Id*. at *1. The District Court, recognizing that Dr. Gerst "has already been privy to at least some communications protected under attorney-client privilege [and] [h]e cannot 'unlearn' that information," and noting the important deterrent effect of its ruling, determined that Dr. Gerst "has acted in bad faith in the litigation and that the nature of his activities mandates that no sanction lesser than striking of Defendants' answer and counterclaims will suffice." *Id*. at *6-7. In affirming the sanctions, the Eleventh Circuit explained that striking the defendants' "answer and counterclaims and entering a default judgment were commensurate with the level of misconduct and the district court did not abuse its discretion." *Eagle Hospital*, 561 F.3d at 1307.

Other courts have not hesitated to dismiss the claims of parties who improperly gained access to their opponents' materials. *See, e.g., Jackson v. Microsoft Corp.*, 211 F.R.D. 423, 432 (W.D. Wash. 2002), *aff'd*, 78 Fed. Appx. 588 (9th Cir. 2003) (court, in dismissing the claims of party who improperly obtained compact discs containing opponent's emails, explained that "[t]he Court can conceive of no sanctions which would cure plaintiff's extensive access to defendant's privileged and confidential materials and which would assure plaintiff's honesty"); *Perna*, 916 F. Supp. at 400-401 (dismissal of claims of party who gained unauthorized access to opponent's documents was "the only sanction severe enough to penalize him for his improper conduct, as well as preserve the integrity of the judicial process."); *Lipin v. Bender*, 644 N.E.2d 1300, 1304 (N.Y. 1994) (in affirming dismissal of plaintiff's complaint as sanction for plaintiff's

misappropriation of defendant's confidential materials, the court noted that because information improperly gained could not be unlearned, no other lesser sanction would suffice).

Given the egregious nature of wrongful conduct directed toward Kaplan -- conduct that is far from isolated or unintentional -- the privileged and confidential nature of the accessed materials, and the resulting irreparable prejudice, the movants respectfully request the Court to conduct an immediate evidentiary hearing compelling Guma Aguiar to testify as to his wrongful conduct in hacking Kaplan's email and to sanction Guma Aguiar by striking his pleadings and dismissing his claims in the *Katten* Case and entering a default judgment against him in the *Leor* Case.[4] As noted by the Eleventh Circuit in *Eagle Hospital*, once a party wrongfully obtains confidential communications of its adversary, it is impossible to "unlearn" the information, and "no lesser sanctions than striking [the party's] answer and counterclaim would suffice." *Eagle Hospital*, 561 F. 3d at 1303.

III. CONCLUSION

For the reasons set forth above, Kaplan and the other movants respectfully request the entry of an order:

a. scheduling an immediate evidentiary hearing in this matter relating to the hacking conducted by Guma Aguiar and requiring Guma Aguiar to submit to questioning in person at such hearing;

b. requiring the preservation of all hard drives, disk drives, emails and related metadata stored on computers owned or controlled by Guma Aguiar and his affiliates, representatives and agents in Israel and elsewhere or relating to the email account **guma@mail.pcic.co.il**, and the production of copies of the same to movants;

[4] Guma Aguiar's conduct also violates federal and state law.

c. enjoining any interception, interference, communication, use or hacking by Guma Aguiar and his affiliates, representatives or agents of the email accounts of the parties, their attorneys, advisers and representatives;

d. imposing sanctions against Guma Aguiar, including the entry of a default judgment against Guma Aguiar in the *Leor* Case, the striking of Guma Aguiar's pleadings and the dismissal of his claims in the *Katten* Case, the disgorgement of any of Kaplan's intercepted emails provided to Guma Aguiar's counsel, affiliates, agents and representatives by Guma Aguiar, and the imposition of monetary fines or penalties; and,

e. granting such additional relief as the Court deems just and proper.

Dated: October 1, 2009

Respectfully submitted,

s/ Brian J. Stack
Brian J. Stack, Esq. (Fla. Bar No. 0476234)
STACK FERNANDEZ ANDERSON & HARRIS, P.A.
1200 Brickell Avenue, Suite 950
Miami, Florida 33131
Tel. (305) 371-0001
Fax. (305) 371-0002

Attorneys for William Natbony

Respectfully submitted,

s/ Harley Shepard Tropin
Harley S. Tropin, Esq. (Fla. Bar No. 241253)
hst@kttlaw.com
Thomas A. Tucker Ronzetti, Esq. (Fla. Bar No. 965723)
tr@kttlaw.com
KOZYAK TROPIN & THROCKMORTON, P.A.
2525 Ponce de Leon Boulevard, 9th Floor
Coral Gables, Florida 33134
Tel: (305) 372-1800
Fax: (305) 372-3508

Attorneys for Leor Exploration & Production LLC, Pardus Petroleum L.P., Pardus Petroleum LLC, and William Natbony, as Trustee of the Dafna Kaplan 2003 Eight-Year Grantor Retained Annuity Trust and Thomas Kaplan 2004 Ten-Year Grantor Retained Annuity Trust, Thomas Kaplan, and William Natbony

CERTIFICATE OF SERVICE

I hereby certify that on this 1st day of October 2009, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record or pro se parties identified on the attached Service List in the manner specified, either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those counsel or parties who are not authorized to receive electronically Notices of Electronic Filing.

s/ Harley Shepard Tropin
Harley S. Tropin, Esq. (Fla. Bar No. 241253)