UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION

IN RE: ABILIFY (ARIPIPRAZOLE) PRODUCTS LIABILITY LITIGATION This Document Relates to the Following Cases: *Perez v. Bristol-Myers Squibb Company, et al.*, 3:16-cv-251 *Viechec v. Bristol-Myers Squibb Company, et al.*, 3:16-cv-291 *Lyons v. Bristol-Myers Squibb Company, et al.*, 3:16-cv-414 *Lilly v. Bristol-Myers Squibb Company, et al.*, 3:17-cv-186 *Marshall v. Bristol-Myers Squibb Company, et al.*, 3:17-cv-172	MDL No. 3:16-md-2734 Chief Judge M. Casey Rodgers Magistrate Judge Gary Jones

RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO COMPEL THE PRODUCTION OF PLAINTIFFS' ONLINE GAMBLING RECORDS AND FOR INSPECTION

Defendants have moved to compel forensic inspection of Plaintiffs' computers, cellular telephones, and other devices for accessing the internet, purportedly to determine the scope and duration of Plaintiffs' online gambling activities. As justification for this request, they assert that certain bellwether trial Plaintiffs have failed to disclose significant online gambling activity. Wholesale, unfettered access to all data on all of Plaintiffs' electronic devices is the most intrusive invasion of privacy in today's digital age. Defendants' proposal allows

them to create a mirror image of all computers, smart phones, email accounts, other mobile electronic devices (Kindle, iPad, etc.), hard drives, thumb drives and online accounts.[1] It also allows them access to all of the data that is retrieved from these devices, whether or not it is relevant to the issues in this case.[2] Defendants have not sufficiently shown that allowing this level of intrusiveness will provide them with information not readily available from other sources, and absent such a showing, forensic examination by a third party is overly burdensome, not proportional to the needs of the case, and overly intrusive.

I. ISSUES APPLICABLE TO ALL PLAINTIFFS

a. Applicable Discovery Rules

Federal Rule of Civil Procedure 26(b)(1) requires the production of discovery materials that are non-privileged, relevant to a claim or defense, and proportional to the needs of the case. At issue here is whether Defendants' request for a forensic examination of Plaintiffs' personal computing devices is relevant to a claim of defense and proportional to the needs of the case. Factors to consider, according to Rule 26(b)(1), include the importance of the information sought to the issues at stake in the action, the parties' relative access to the relevant information, the importance of the discovery in the resolution of the litigation, and the burden of

[1] *See* Exhibit 1, Defendants' Forensic Preservation and Inspection Protocol.
[2] *Id.*

producing the discovery relative to the benefit. Even when discovery is otherwise allowed by Rule 26, courts have held that the extent of discovery can be limited when the discovery sought is unreasonably cumulative or duplicative or can be obtained from a source or method that is less burdensome.[3]

There are certainly less intrusive ways to obtain the requested information. Under Rule 34(a), a party may request the responding party to produce and permit the requesting party to inspect and copy any designated documents.[4] Rule 34(a) does not provide unrestricted access to a producing party's electronically stored information.[5] "[O]n a motion to compel, a responding party need not provide discovery of electronically stored information from sources that the responding party identifies as not reasonably accessible because of undue burden or cost."[6]

The advisory committee notes to the 2006 amendment to Rule 34(a) state that inspection of a responding party's hard drive is not routine, and such unfettered access should be tempered:

> Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should

[3] *Hespe v. City of Chicago*, No. 13 C 7998, 2016 WL 7240754, at *3 (N.D. Ill. Dec. 15, 2016).
[4] Fed. R. Civ. P. 34(a).
[5] *In re Ford Motor Co.*, 345 F.3d 1315, 1316 (11th Cir. 2003).
[6] *U & I Corp. v. Advanced Med. Design, Inc.*, 251 F.R.D. 667, 674 (M.D. Fla. Mar. 26, 2008); Fed. R. Civ. P. 26(b)(2)(B)

> guard against undue intrusiveness resulting from inspecting or testing such systems.

It follows that "[t]he failure to produce discovery as requested or ordered will rarely warrant unfettered access to a party's computer system."[7]

Mirror imaging of Plaintiffs' electronic devices, as sought in Defendants' proposed protocol, will provide unrestricted access to Plaintiffs' accounts. "[W]hen weighing the propriety of mirror imaging, a court should consider such factors as (1) the needs of the case, (2) the amount in controversy, (3) the importance of the issues at stake, (4) the potential for finding relevant material, and (5) the importance of the proposed discovery in resolving the issues."[8]

Defendants cite *Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp.*, 280 F.R.D. 681, 687 (S.D. Fla. Mar. 5, 2012) in support of their request for forensic examination of Plaintiffs' electronic devices. This reliance is misplaced. In *Wynmoor*, unlike the current case, the plaintiffs were "either unwilling or unable to conduct a search of their computer systems for documents responsive to Defendant's discovery requests."[9] Additionally, the plaintiffs in *Wynmoor* claimed that the hard drive containing electronic copies of work orders had crashed during

---

[7] *Bennett v. Martin*, 928 N.E.2d 763, 776 (Ohio 10th DCA, Nov. 24, 2009) (citing *Bank of Mongolia v. M & P Global Fin. Serv's., Inc.*, 2009 WL 1117312, at *6 (S.D. Fla. Apr. 24, 2009) (courts usually order the appointment of an independent expert to retrieve any responsive files from the producing party's computers).

[8] *In re American Med. Sys., Inc.*, 2016 WL 6666890, at *4–5 (S.D.W. Va. Nov. 10, 2016) (citing *United Factory Furniture Corp. v. Alterwitz*, 2012 WL 1155741, at *3–5 (D. Nev. Apr. 6, 2012).

[9] 280 F.R.D. at 687.

a hurricane and made no efforts to recover the work order data.[10] The facts of *Wynmoor* bear no resemblance to the facts here where Plaintiffs are willing and capable of performing an ESI search upon instruction and with assistance of counsel and their consultants.

Direct access to another party's databases and devices may be warranted in some circumstances, such as non-compliance with discovery rules, but is not warranted if a party is simply engaging in a "fishing expedition."[11]

b. <u>The records currently available to Defendants are sufficient to defend against Plaintiffs' claims, and the request is unreasonably cumulative and duplicative.</u>

Before permitting an invasive forensic examination, the Court must look at whether the information Defendants seek is known to exist, and if it does exist, whether that information can be obtained from another source.[12] Where "it is highly probable, if not certain, that the discovery sought [through a forensic examination of a computer system] would be cumulative or duplicative of what has already been obtained," Defendants cannot establish "good cause" as required under Rule 26.[13]

[10] *Id*.
[11] *Balfour Beatty Rail, Inc. v. Vaccarello* at *3.
[12] *Bradfield v. Mid-Continental Cas. Co.*, 2014 WL 4626864, at * 4 (M.D. Fl. Sept. 15, 2014).
[13] *Id.*

According to Defendants' Motion to Compel, the primary purpose of the proposed forensic inspection of Plaintiffs personal devices is to search for evidence that Plaintiffs engaged in gambling activity before they started or after they discontinued treatment with Abilify. The timing of Plaintiffs' compulsive gambling generally (not internet gambling specifically) is relevant to the issue of specific causation. A secondary purpose, according to Defendants, is to obtain information relevant to the calculation of damages.

Defendants have not demonstrated that they are likely to find any evidence that Plaintiffs engaged in internet gambling over a different time period than they engaged in other forms of gambling, such as casino gambling, for which records have been produced. More importantly, any evidence Defendants obtain through the intrusive protocol they have proposed is likely to be duplicative or cumulative of information already provided by Plaintiffs, including financial records and casino gambling records. In fact, in their motion, Defendants cite to medical and financial records that they claim indicate Plaintiffs were gambling prior to and/or after taking Abilify, and such records are sufficient to raise a specific causation defense. To the extent that Defendants argue that they are seeking information relevant to damages, that is Plaintiffs' burden, and therefore, of no consequence to Defendants. Presumably, Plaintiffs' strongest evidence will be evidence of

financial losses caused by gambling and the onus will be on them to collect and present this evidence.

Further, unlike physical gambling, internet gambling simply cannot be done with cash. Rather, internet gambling requires an electronic financial transaction using credit cards, debit cards, wire or ACH transfers from bank accounts, etc. All of these types of electronic financial transactions already appear in the financial records plaintiffs have produced or provided authorizations for Defendants to obtain. Plaintiffs can, if the Court believes necessary, lengthen the time period covered by such financial records, to address Defendants' concerns both with regard to the time period at which Plaintiffs began or ended their gambling activity, and the dollar amounts of such gambling activity, without the need for the type of intrusive and burdensome search and production of Plaintiffs' devices asked for by Defendants.[14]

c. <u>Defendants Have Failed to Show that a Forensic Inspection of Personal Devices is Necessary and Proportional to the Needs of the Case.</u>

In determining whether a request for forensic inspection of personal computers and devices is proportional, privacy and confidentiality interests are

[14] To bolster their argument for obtaining internet gambling records, Defendants argue that Plaintiffs' financial records indicate payments to many different gambling sites. However, the fact that financial records show transfers of funds to many different web-based addresses is not indicative that Plaintiffs actually gambled on that number of gambling sites. It is very common for a single portal site to use multiple back-end sites and financial transaction processors in order to avoid scrutiny/shutdown by United States authorities.

factors to consider when weighing the burden.[15] Defendants seek to duplicate and inspect individuals' personal computers, phones, and cloud storage, all of which contain vast amounts of private information concerning both the Plaintiffs and other people not party to this suit; such an exercise is not proportional to the needs of the case. "This is not a case in which the information is unavailable from another source. . . Defense counsel simply believes there is something more to find. Moreover, this is not a case in which the particular information sought is known to actually exist."[16]

As noted above, according to Defendants' Motion to Compel, the primary purpose of the proposed forensic inspection of Plaintiffs personal devices is to search for evidence that Plaintiffs engaged in internet gambling activity before they started or after they discontinued Abilify. In support of the necessity of performing a forensic inspection, however, Defendants state only that certain Plaintiffs failed to fully disclose participation in internet gambling, without pointing to any evidence that Plaintiffs have been untruthful or evasive about the timing of the onset or cessation of their compulsive gambling. As discussed in more detail below with regard to each individual Plaintiff, Defendants' allegation has no merit.

---

[15] *John B. v. Goetz*, 531 F. 3d 448, 460 (6th Cir. 2008) ("the district court's compelled forensic imaging orders here fail to account properly for the significant privacy and confidentiality concerns present in this case."); *Hespe v. City of Chicago,* at *4 (citing the Advisory Committee's Notes to Rule 34, which states, in part, "Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.").

[16] *Bradfield v. Mid-Continental Cas. Co.*, 2014 WL 4626864, at * 4 (M.D. Fl. Sept. 15, 2014).

It appears that Defendants do not suspect, but merely hope, that some of the internet gambling in which Plaintiffs engaged will have occurred outside of the time period during which they used Abilify and/or engaged in other forms of compulsive gambling and for which they do not currently have financial records. As one court noted when faced with a similar request: "defendants essentially seek a warrant to search plaintiff's devices for statements with which to impeach her."[17] That court denied the request. Similarly, in a Florida case, the court held that direct access to another party's databases and devices is not warranted if a party is simply engaging in a "fishing expedition."[18] The information Defendants purport to need is available from other sources, and they point to no evidence that they will find internet gambling inconsistent with the timeline established by other gambling records. Defendants are simply on a fishing expedition.

Although Plaintiffs believe that financial and other records will provide sufficient evidence to regarding the relevant issues, Plaintiffs also believe there is a more proportional, less invasive way to conduct a computer and device search, if the Court believes that a search of personal devices is warranted. Plaintiffs are willing to voluntarily produce the information sought regarding online casino activity, to the extent that it exists and remains in their custody and control.

[17] *Hespe v City of Chicago,* at *5.
[18] *Balfour Beatty Rail, Inc. v. Vaccarello,* at *3.

Defendants argue that a forensic inspection is warranted based upon Plaintiffs' past failure to produce the ESI discovery they sought. With regard to this issue, the Court should consider the extent to which their failure to satisfy Defendants "is due to an innocent lack of sophistication in retrieving responsive ESI" rather than negligence or intentional manipulation of evidence.[19] There is no evidence in this litigation that Plaintiffs "have intentionally destroyed relevant ESI in the past. . . [or] are unwilling, or will refuse, to preserve and produce all relevant ESI in the future."[20]

Plaintiffs in this litigation have not, to date, been given any coaching or instructions on searching their electronic devices for evidence of internet gambling. If Defendants feel a more thorough search of computers, electronic devices, and cloud-based storage is warranted, Plaintiffs should be provided the opportunity to voluntarily apply a protocol and conduct a search of their own computers, phones, and other devices, as well as cloud-based storage, under the direction of or with technical support from an ESI consultant retained by Plaintiffs if necessary.

d. <u>The Protocol proposed by defendants is overbroad, overreaching and overly invasive.</u>

Defendants' proposed protocol is disproportionate and overreaching to address any perceived discovery needs of Defendants. Rather than restate the

[19] *Hespe v. City of Chicago,* at *5.
[20] *John B. v. Goetz* at 460.

specific shortcomings of Defendants' proposed protocol, Plaintiffs refer the Court to the Declaration of Jonathan Jaffe, attached hereto as Exhibit 2 and the proposed alternative staged discovery plan contained therein if the Court believes that additional production of Plaintiffs' records is necessary.

e. Unfettered access to Plaintiffs' data is contrary to the discovery precedent requested and set by Defendants.

While asking for something completely different from Plaintiffs in their Motion to Compel, Defendants have taken exactly the same position with regard to Defendants' own production in response to Plaintiffs' requests for production as Plaintiffs take here. Defendants have been allowed to limit the custodians searched, make their own selection of the sources of data for each custodian, have conducted their own search of that data using agreed to search terms, have produced those records only after manual review for relevance and privilege, and have produced those records in the non-native format pursuant to the ESI protocol entered into in this litigation.

Further, even in the limited instances that Plaintiffs' sought native production of data to Plaintiffs' ESI expert, as, for example, in the case of the Defendants' adverse event databases, Defendants strenuously objected to Plaintiffs request. Defendants vehemently opposed a complete production of Defendants' adverse event database with regard to Abilify to Plaintiffs' ESI consultant in native format,

instead, asking this Court to narrowly limit the data produced. In final form, Defendants were only required to search their database for specific search terms, followed by Defendants' manual review and redaction of records, followed by production in non-native B2B format, rather than native format. There is no reason why a different standard should apply to the search, review, and production of Plaintiffs' records as that applied to Defendants' records.

f. Any Order entered by the Court with regard to this issue should be limited to Plaintiffs Lilly and Marshall.[21]

Defendants have requested that this Court apply any relief granted to all future cases in this litigation. Plaintiffs oppose this request because the question of whether a forensic examination is relevant to the needs of a case is an individualized inquiry and Defendants are required to show good cause for any such relief on a case-by-case basis.

Defendants also request that Plaintiffs Viechec and Lyons "certify that they did not use electronic devices to gamble at any time." There is simply no basis to request this type of certification. There is nothing in the record to suggest that Plaintiffs Viechec and Lyons have withheld any information about online gambling. Furthermore, Judge Jones already denied Defendants' request for Ms. Lyons cell phone number and cell phone service provider because "there is no

[21] While Defendants' Motion also addressed Plaintiff Perez, the Perez case is in the process of being dismissed, so Defendants' issues as to her inconsistencies are now moot.

claim that she used her phone to gamble" and the information is "not relevant and proportional to the needs of the case." ECF 575, pgs. 9-10.

II. JENNIFER LILLY

In addition to the general reasons stated above, Plaintiff Jennifer Lilly opposes this motion for several reasons: 1) contrary to Defendants' assertion, Ms. Lilly did disclose online gambling activity to Defendants, in 145 pages of bank statements attached as exhibits to her Plaintiff Fact Sheets; 2) the requested forensic inspection would, in her case, provide an incomplete picture of her online gambling activity, as she no longer owns the computer on which most of her online gambling was conducted; 3) other, more complete, sources of information about online gambling activity, such as financial records indicating transfers of funds to and from online gambling sites, are available; and 4) Ms. Lilly is willing to voluntarily conduct, with the help of Plaintiffs' ESI consultant, her own searches for relevant internet gambling records, and produce any relevant, non-privileged, records found. For these reasons, a forensic inspection of her personal computers, phones, and other devices according to Defendants' proposed protocol is not proportional to the needs of the case.

a. Jennifer Lilly Did Disclose Internet Gambling Activity

Defendants are incorrect in stating that "Lilly has not disclosed any online gambling activity to Defendants."[22] Attached to her Plaintiff's Fact Sheet and Amended Fact Sheet, Ms. Lilly voluntarily produced to Defendants five years of monthly bank statements (2010-2014), Bates stamped NCS000001-NCS000145. On each bank statement, she circled the funds transferred to online casinos, and at the top of each bank statement which included a transfer to one or more online casinos, ***Ms. Lilly hand-wrote "online gambling."*** Contrary to Defendants' assertion that Ms. Lilly did not voluntarily disclose any online gambling in her original Fact Sheet and answers to interrogatories, the documentation provided to Defendants in conjunction with her Fact Sheets clearly demonstrates that Ms. Lilly did not overlook or conceal her online gambling history; she both disclosed it and provided evidence that she had transferred funds to internet gambling websites.

Plaintiffs note that the Plaintiff's Fact Sheet contains a single question (question IV.J) which asks Plaintiffs to "identify the frequency with which you gambled, where you gambled, dates of gambling, type of gambling, and any gambling winnings or debts." The Fact Sheet does not ask specifically about internet gambling. In answering this question, Ms. Lilly focused her response on scratch off lottery tickets (her primary form of gambling after she moved to Florida), and listed a raceway and two casinos (her primary form of gambling

[22] Motion to Compel at 5.

when she lived in Connecticut). Although she accidentally omitted listing online gambling in her narrative response to this question, her history of internet gambling, including the dates, amount spent, and billing web addresses of internet gambling sites, was unambiguously provided in the bank statements attached to the Fact Sheet as Bates NCS000001-NCS000145. As described above, hand-written notes specifically alerted Defendants to the internet gambling activity documented in those statements, and funds transferred to internet casinos by bank debit were circled. In response to Interrogatory Nos. 5, 6, and 7, which ask Plaintiffs to identify each "establishment, website, online application, or other location at which you gambled," Ms. Lilly answers by reference to her "Plaintiff's Profile Form, Plaintiff's Fact Sheet, and any Amendments thereto." There was no intent to conceal her history of internet gambling, which was documented in the attachments to her Fact Sheet.

In addition, Defendants assert that Ms. Lilly failed to disclose the existence of a PayPal account, which they speculate may have been used for internet gambling. However, Ms. Lilly's PayPal account is linked to her primary bank account, and therefore any transfers of funds using PayPal are reflected in the bank records with Bates numbers NCS000001-NCS000145, which were provided to Defendants with the Fact Sheets. The bank statements indicate both "PayPal" and the entity to which funds were transferred using the PayPal service. Ms. Lilly does

not recall using her PayPal account for gambling. However, her bank statements, which list any transfers using her PayPal account, were provided to Defendants with the Plaintiff's Fact Sheet and Amended Fact Sheet.

b. Forensic Inspection of the Devices Currently in Plaintiff Lilly's Possession and Control Would not Provide Complete Information

The proposed protocol drafted by Defendants requires, among other things, certification that the devices provided to the forensic examiner "are the only Devices owned or possessed or used by Plaintiff wherein any alleged gaming information existed or may exist or be stored, or were used to access gambling providers."[23] Ms. Lilly cannot so certify because the computer she used for online gambling beginning in late 2003 or early 2004 was discarded sometime around 2014.[24] She has owned a second computer since 2012, which she also used for online gambling while taking Abilify, but Plaintiffs believe that the bank records Ms. Lilly has provided are a better source of information about her online gambling than that computer.

Ms. Lilly also reports that her iPhone 6 crashed during a software update approximately one month ago, and was reset when she took it for repair. Her data was not backed up to cloud storage before being reset.

[23] See Ex. 1 at 1.
[24] Ms. Lilly believes she began taking Abilify in or around December 2003.

Because her devices will not provide a complete record of her internet gambling, whereas her bank records will provide complete documentary evidence of her history of internet gambling, the request for a forensic examination of her devices should be denied.

c. **Defendants Have Failed to Show that a Forensic Inspection of Personal Devices is Necessary and Proportional to the Needs of the Case**

As noted previously, Florida Courts have held that the Court must weigh privacy concerns against the potential utility of a search such as the forensic examination proposed by Defendants.[25] Balancing Ms. Lilly's privacy concerns against the Defendants' discovery concerns, it is clear that her privacy concerns outweigh any need to apply the proposed protocol to her personal computer and devices. Ms. Lilly has consistently complied with discovery requests, she has provided bank records and other evidence of all forms of gambling in which she engaged, and she has not expressed unwillingness or inability to search her personal devices for the requested information. She has demonstrated no deliberate non-compliance with discovery rules.[26] Thus, her conduct in this litigation does not

[25] 2009 WL 10670333, at *1

[26] *See Balfour Beatty Rail, Inc. v. Vaccarello*, 2007 WL 169628 (M.D. Fla. Jan. 18, 2007). Her failure to specifically mention internet gambling in her narrative response to PFS question IV.J was merely an oversight, and instances of internet gambling were clearly pointed out to Defendants in the attachments to the PFS.

suggest any attempt to conceal relevant information and Defendants demonstrate no need for an invasive forensic search of her personal computers and devices.

Moreover, where "it is highly probable, if not certain, that the discovery sought [through a forensic examination of a computer system] would be cumulative or duplicative of what has already been obtained," Defendants cannot establish "good cause" as required under Rule 26.[27] According to Defendants' Motion to Compel, the primary purpose of the proposed forensic inspection of Plaintiffs personal devices is to search for evidence that Plaintiffs engaged in gambling activity before they started or after they discontinued Abilify. In support of the necessity of performing a forensic inspection of Ms. Lilly's devices, however, Defendants fail to point to any evidence that Ms. Lilly has been untruthful or evasive about the timing of the onset or cessation of her compulsive gambling. Furthermore, Defendants do not demonstrate that a review of the financial transactions and other evidence of participation in gambling which Ms. Lilly has produced is insufficient to establish the time frame in which she gambled. Because the invasive protocol is unnecessary and likely to provide only cumulative and duplicative evidence, Defendants' Motion should be denied.

Defendants also argue that the relationship between Plaintiffs' claims and their computers is indisputable. Ms. Lilly disagrees. The claims in this case involve

[27] *Bradfield v. Mid-Continental Cas. Co.*, 2014 WL 4626864, at *4 (M.D. Fla. Sept. 15, 2014).

a pharmaceutical, Abilify, causing an injury, compulsive gambling. Gambling takes many forms. For Ms. Lilly, the most powerful compulsions involved casino gambling and scratch-off lottery cards. No evidence of these compulsions will be found on her computers or personal devices. She did, at times, also engage in internet gambling, as she has disclosed, but a neutral forensic inspection of her computer is not necessary to obtain information about her internet gambling practices.

If the Court believes that further disclosure of information stored on personal computers and devices is warranted, Ms. Lilly is willing to voluntarily apply a protocol and conduct a search of her own computer and phone under the direction of or with technical support from an ESI consultant retained by Plaintiffs if necessary. It is possible for Ms. Lilly to produce relevant documents, such as emails indicating registration with online gambling websites, account statements, and other pertinent information, such as screen shots of gambling applications, without giving Defendants access to her online accounts or resorting to use of a neutral forensic examiner and the invasive examination protocol Defendants have proposed. While Plaintiffs continue to believe that even this is not necessary, given the financial records already produced, Plaintiffs are willing to do so if required by the Court. The burden and invasion of privacy involved in a neutral forensic examiner's search of personal computers, smart phones, and other devices,

however, is certainly not necessary to obtain the information sought, and such an exercise would not be proportional to the needs of the case.

III. BRYAN MARSHALL

In addition to the general reasons stated above, Plaintiff Bryan Marshall opposes Defendants' Motion for several reasons: (1) contrary to Defendants' assertion, Mr. Marshall did not omit the names of online gambling websites, as evidenced in his Plaintiff Fact Sheet and 340 pages of bank statements produced on RecordTrak; (2) such an inspection would, in his case, provide an incomplete picture of his online gambling activity, as he no longer owns the computers and cell phones on which most of his online gambling was conducted; (3) other, more complete sources of information about online gambling activity, such as bank records indicating transfers of funds to and from online gambling sites are available, and (4) Mr. Marshall has committed to conducting his own searches for relevant internet gambling records. Thus, a forensic inspection of personal computers, phones, and other devices is not proportional to the needs of the case.

a. Bryan Marshall previously disclosed his internet gambling activity.

Defendants are incorrect in stating that Plaintiff Marshall "omitted" the names of online gambling websites.[28] Plaintiff Marshall provided information regarding online gambling websites he recalled in Section IV.K of the Plaintiff

[28] Motion to Compel at 7.

Fact Sheet. Also, Mr. Marshall produced approximately 760 pages of bank statements which include the transfer information for online gambling websites. Many of these transactions took place in 2009. With respect to the recent transactions in 2017, Plaintiff will supplement his Fact Sheet. The mere fact that Plaintiff has recent gambling activity does not justify the invasive protocol proposed by Defendants. Indeed, recent gambling activity seems something that is more appropriately explored during Plaintiff's deposition *and should come as no surprise as continued gambling was noted Section IV.L of Plaintiff's Fact Sheet.*

In response to the Plaintiff Fact Sheet, Mr. Marshall provided the name of a casino and four online gambling websites. Although he may have overlooked other online gambling websites (e.g. Playtika and bldcard.com), his history of online gambling, including the dates, amount spent, and billing web addresses of the internet gambling sites, ***was unambiguously provided to Defendants in the bank statements produced*** on RecordTrak (specifically from Academy Bank and Campus USA Credit Union).

Notwithstanding, Defendants suggest that Mr. Marshall breached a duty to preserve relevant data which, according to Defendants, was triggered in December 2014.[29] However, this premise is based on the flawed assumption that Mr. Marshall was aware or should have been aware of a potential claim and/or had

[29] Motion to Compel at 11.

reason to believe that such a claim existed. Mr. Marshall did not retain counsel with respect to his Abilify claim until late 2016 and had no reason to be aware that he had a potential claim against Defendants until that time. A party's duty to preserve evidence arises once the party can reasonably anticipate that the particular issue will be the subject of future litigation.[30] In Mr. Marshall's case, this did not occur until late 2016.

b. Forensic Inspection of the Devices Currently in Plaintiff Marshall's Possession and Control Would Not Provide Complete Information.

As a threshold matter, absent a "[f]actual finding of some non-compliance with [the] discovery rules," direct access to a party's computer is unwarranted.[31] In the present case, there has been no non-compliance that would justify direct access to Mr. Marshall's devices. Moreover, Mr. Marshall does not have possession of the computers used for online gambling. Indeed, he sold his prior computer to a pawn shop in approximately 2013.[32] Mr. Marshall does not possess electronic or physical copies of documentation regarding the purchases and sales of this

[30] *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F.Supp.2d 1317, 1326-27 (S.D. Fla. Aug. 23, 2010) (citing *Southeastern Mech. Serv's., Inc. v. Brody*, 2009 WL 2242395, at *2 (M.D. Fla. July 24, 2009) (noting that "[o]nce a party files suit or reasonably anticipates doing so…it has an obligation to make a conscientious effort to preserve electronically stored information that would be relevant to the dispute.")).

[31] *In re Ford Motor Co*., 345 F.3d 1315, 1317 (11th Cir. 2003). *See also John B. v. Goetz*, 531 F.3d 446, 459–60 (6th Cir. 2008) (*citing McCurdy Group, LLC v. Am. Biomedical Group, Inc*., 9 Fed. Appx. 822, 831 (10th Cir. 2001))("[M]ere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures.).

[32] Mr. Marshall began taking Abilify in December 2007.

computer - nor does he recall the names of the pawn shops where the computer was purchased or sold.

More recently, Mr. Marshall accessed a work-issued computer that belongs to a third party. Mr. Marshall used this computer to access his iCloud e-mail account. Plaintiff does not have control over this computer nor does it belong to him. To the extent that responsive email exists on the iCloud, they have or will be produced. Plaintiff submits that the bank records he has provided, in addition to his voluntary search of his iCloud e-mail account, are an appropriate source of information and discovery regarding Plaintiff's online gambling. Indeed, a protocol that implicates a third-party raises additional privacy and data concerns that are neither appropriately addressed in Defendants' proposed protocol nor justified in the current case.[33]

With respect to cell phone data and/or imaging, Plaintiff Marshall is no longer in possession of his prior cell phones. One phone was destroyed during a psychotic episode and other phones were returned to the cellular device retailers when Mr. Marshall received upgrades for new cell phones. With respect to Plaintiff's current phone, Mr. Marshall has had this phone for over a year and

[33] *See, Med. Components, Inc. v. Classical Med., Inc*., 210 F.R.D. 175, 180 n. 9 (M.D.N.C. Sept. 27, 2002) ("The current generally prevailing view is that the Court may first consider whether information should be obtained by direct discovery from a party, as opposed to from a non-party, and that the court should give special weight to the unwanted burden thrust upon non-parties when evaluating the balance of competing needs.").

previously provided Defendants with his cell phone number and carrier, as well as his prior carrier and telephone numbers based on Defendants' representation that the carrier and telephone numbers would be used to identify online gambling activity. As such, any suggestion that the Mr. Marshall has failed to disclosed relevant information or that his cell phone was not properly preserved is misplaced.[34]

In sum, Plaintiff Marshall has endeavored to provide accurate information through his Fact Sheet and supplemental discovery responses that demonstrate his online gambling activities. Indeed, volumes of information have been produced through the bank and other documents that are in Defendants' possession. Defendants have not demonstrated a legitimate need to conduct a forensic examination of Plaintiff's device (or that of the Third Party). Mr. Marshall's bank and other records, which have been produced, provide the best and most complete source of documentary evidence of Plaintiff's online gambling. Defendants' request for a forensic examination of these devices should be denied.

CONCLUSION

[34] Plaintiff previously disclosed (on his Plaintiff Fact Sheet) that he accessed the "Bodog" gambling website. (Plaintiff accessed "Bodog" during his January 2016 treatment admission). Plaintiff has also access online games called the World Series of Poker and Zynga. Plaintiff will supplement his earlier discovery response to include these online sites.

For the forgoing reasons, Plaintiffs respectfully request that this Court deny Defendants' Motion to Compel.

Respectfully submitted on this 1st day of December, 2017.

By: ***/s/ B. Kristian W. Rasmussen***

B. Kristian W. Rasmussen
FL Bar #:0229430
Cory Watson Attorneys
2131 Magnolia Avenue, Suite 200
Birmingham, AL 35205
krasmussen@corywatson.com
(205) 328-2200

Marlene J. Goldenberg
Goldenberg Law, PLLC
800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
mjgoldenberg@goldenberglaw.com
(612) 333-4662

Gary L. Wilson
Robins Kaplan LLP
800 LaSalle Avenue, 2800 LaSalle Plaza
Minneapolis, MN 55402-2015
gwilson@robinskaplan.com
(612) 349-8500

Bryan F. Aylstock (FL Bar No. 78263)
Aylstock, Witkin, Kreis & Overholtz
17 E. Main Street, Suite 200
Pensacola, FL 32502
baylstock@awkolaw.com
(850) 202-1010
Attorneys for Plaintiff Lilly

Behram V. Parekh
Kirtland & Packard LLP
2041 Rosecrans Ave., Third Floor
El Segundo, CA 90245
bvp@kirtlandpackard.com
(310) 536-1000

George T. Williamson
Farr, Farr, Emerich, Hackett, Carr & Holmes
99 Nesbit Street
Punta Gorda, FL 33950
(941) 639-1158
gwilliamson@farr.com

Lexi Hazam
Leif Cabraser Heimann & Bernstein, LLP
250 Hudson Street, 8th Floor
New York, NY 10013
(415) 956-1000
lhazam@lchb.com

Yvonne M. Flaherty
Lockridge Grindal Nauen, P.L.L.P
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
(612) 339-6900
ymflaherty@locklaw.com
Attorneys for Plaintiff Marshall

Counsel for Plaintiffs

CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 7.1(F)

I HEREBY CERTIFY that this brief complies with the word limit of Local Rule 7.1(F) and contains 5810 words, excluding the parts exempted by that Rule.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY this 1st day of December, 2017, a true and correct copy of the foregoing was electronically filed via the Court's CM/ECF system, which will automatically serve notice of this filing via e-mail notification to all registered counsel of record.

/s/ B. Kristian Rasmussen
B. Kristian Rasmussen

EXHIBIT 1

FORENSIC PRESERVATION AND INSPECTION PROTOCOL

Party A ("Plaintiff(s)") and Party B ("Defendant(s)") (collectively, the "Parties") jointly agree to this forensic inspection protocol (the "Protocol"), which sets forth the agreement between the Parties for the search and inspection of the computers, smart phones, media, electronic storage devices, or online repositories (such as email accounts, social media accounts, or online gambling accounts) (collectively, "Devices") in the possession, custody, or control of Plaintiffs which could potentially contain evidence of gambling. These Devices include but are not limited to the following:

(a) Plaintiffs' computers, including any information storage device(s);

(b) Plaintiffs' smart phones;

(c) Plaintiffs' email accounts; and

(d) Plaintiffs' mobile electronic devices (*e.g.*, Kindle, iPad);

(e) Plaintiffs' active or inactive gambling accounts; and

(f) Plaintiffs' storage devices including portable (or external) hard drives, thumb drives, and other storage media.

A computer forensic examiner ("Forensic Examiner") shall be retained by the Defendants to investigate and search for evidence of gambling. Depending on the volume of data, the Forensic Examiner may apply methods to certain data (e.g., search terms, de-duplication) to limit the volume of materials for its review. After the 3 day first look period, the Forensic Examiner will produce a copy of its results to Defendants. The Forensic Examiner shall function as a neutral in terms of protecting data privacy and privilege.

1. Identification and Certification of Device(s) and Account(s):

Plaintiff, by and through counsel, shall make available for forensic inspection to the Forensic Examiner the Device(s) within five (5) business days of execution of this Protocol. In connection with the same, Plaintiff shall provide a certification under penalty of perjury to Defendant's counsel and the Forensic Examiner within five (5) days of execution of this Protocol that (1) the Devices identified above are the only devices and accounts within Plaintiffs' possession, custody, or control that contained or contain evidence of gambling activity; Plaintiff does not have any hard copies of information related to gambling in their possession, (2) that any and all backups of any such information on the cloud or through an internet or online data storage account has also been made available to the Forensic Examiner, (3) that the devices listed above are the only Devices owned or possessed or used by Plaintiff wherein any alleged gaming information existed or may exist or be stored, or were used to access gambling providers, and (4) Plaintiff shall identify individuals that he/she shared, disclosed,

emailed the alleged information to the extent such information was shared, disclosed or emailed.

Access to such Device(s) identified above shall be provided by Plaintiff to the Forensic Examiner with all accompanying chain of custody documentation (which documentation is required as set forth in Section 2 herein), access passwords, and/or other information needed to allow access. Plaintiff will execute and provide a Declaration of Completeness relating to the each specific step taken to search for Device(s) that may have contained or contain on line gaming activity, within five (5) days of execution of this Protocol.

Access to such online accounts(s) identified above shall be provided by Plaintiff to the Forensic Examiner with user ids, access passwords, and/or other information needed to allow access. Plaintiff will execute and provide a Declaration of Completeness relating to each specific step taken to identify accounts that contained or contain records of gambling accounts, records of gambling activity, or discussions of gambling activity, within five (5) days of execution of this Protocol.

2. Chain of Custody:

Plaintiff shall provide a chain of custody to Forensic Examiner upon delivery of any Device(s) to Forensic Examiner. The chain of custody documentation shall identify all persons who handled, inspected, analyzed/examined, performed maintenance, or transported the Device(s) and any component part thereof and identify the locations and conditions under which it was stored or moved. Upon receipt of the Device(s), Forensic Examiner shall prepare documentation identifying the chain of custody of the Device(s) and any component part thereof, from the date of the receipt forward.

3. Preparation for Inspection:

Prior to imaging any Device(s), Forensic Examiner shall take all necessary digital photographs and shall record the specifications, characteristics, and any physical serial number identifiers (volume serial numbers shall be documented during the forensic investigation of the Device(s) as described below) for the Device(s) to document their current physical condition and operability. If any Device(s) are received in an already-imaged format, Forensic Examiner shall deploy a write-protection device prior to inspecting the contents of the container or device to ensure the device or container is not modified. Forensic Examiner shall document the image format and verify the integrity of the imaged device or image files contained on the device by comparing the MD5 hash value of the imaged device or image files to the original Device(s) acquisition MD5 hash value if the original device has been provided to Forensic Examiner. Prior to imaging, Forensic Examiner shall properly prepare suitable forensic storage media ("Target Media") for receipt of any forensic images created through Forensic Examiner's execution of any directives under this protocol.

4. Imaging of Device(s):

Forensic Examiner shall make at least one full forensic bit stream copy of each Device(s) onto Target Media. The original source Device(s) shall, at all times, be preserved in an unaltered state. Forensic Examiner shall document and record on an acquisition form: (i) a general description of the process and tools utilized to conduct the imaging; (ii) the MD5 hash value of the original source Device; and (iii) the MD5 hash value of the copy.

If any Device(s) are computers, Forensic Examiner shall also obtain complementary metal oxide semiconductor (CMOS) date and time data within the computer basic input/output system (BIOS). The BIOS date and time should be compared with the actual date and time, and the two shall be recorded.

If any Device(s) are online repositories, Forensic Examiner shall create logical evidence files of the same, and include within the logical evidence file properties any and all information necessary to identify the original source of the virtual repositories.

Forensic Examiner shall be entitled to make additional copies of any forensic image created under this Protocol for purposes of redundancy, disaster recovery, working copies, or to provide copies to the parties.

5. Location and Timing of Imaging:

The imaging process shall take place at the law firm of Co-Lead Counsel of this litigation, and shall continue until all Device(s) identified have been imaged and verified.

Capture of information from online accounts will be conducted in the presence of a representative of the Plaintiff who controls such account(s).

6. Preparation for Review and Search of Images:

Prior to the Forensic Examiner conducting any forensic analysis/examination (a "Review") of any forensic image created from a Device, Forensic Examiner shall make a determination as to the date of its' most recent reformatting or reset. In instances where a device has been in service for a limited time prior to the imaging process or recently re-imaged or reset, the Forensic Examiner may report this to counsel and seek access to additional sources.

7. Handling of Privileged and Confidential Material:

At the outset of the investigation the Examiner will take the following measures to protect confidential and/or privileged information on the devices;

(a.) No information contained on the Devices may be communicated in any way, either publicly or to a Party, unless permitted by this agreement or at the request of the parties.

(b.) The Forensic Examiner shall sign the Protective Order in this action (DE 185) and agree to be bound by its terms.

(c.) All information obtained by or made available to the Forensic Examiner under this Protocol shall be deemed Confidential Information under the Protective Order, and handled accordingly

(d.) Data sources likely to contain privileged communications, such as e-mail, will be separated and filtered by known e-mail addresses and domains. Plaintiff counsel will provide a list of such addresses and domains, or other privilege related search terms, and may supplement it during the course of this protocol if new information becomes available. Information identified by the above filter will be excluded from any investigation.

(e.) Plaintiffs' counsel may also request further sources be segregated and searched as above by notifying opposing counsel and Examiner by letter or e-mail.

(f.) Either party may request a listing of basic information (sender/recipient name, date, subject) withheld for privilege.

(g.) The Forensic Examiner shall have access to all content on any device. Copies of artifacts or exports of relevant files may be made during the course of the investigation. Non-privileged information relevant to the investigation may be communicated with counsel.

(h.) All information produced to the Plaintiffs will be produced to the Defendants after the 3 day first look period.

(i.) Either party may "Clawback" information later deemed as privileged or subject to the Protective Order in this action (ECF 185)at any time during the course of the protocol by informing counsel by letter or e-mail.

8. <u>Access to Files:</u>

The Forensic Examiner shall provide access to any non-privileged files contained on the Device(s) to either counsel that is evidence of gambling. Any such request will include opposing counsel who will have the opportunity to object on privilege and or confidentiality grounds.

9. Device Image Disposition:

Upon completion of review and delivery of any reports, Forensic Examiner shall maintain and store the images for the duration of the current matter. At any time the Parties may jointly request return or destruction of the images by letter or e-mail.

10. Right to Supplement

Based on the results of this executed Protocol, and any new additional information obtained during the execution of this Protocol, the Parties reserve the right to supplement the requests contained within this Protocol.

IT IS HEREBY AGREED:

_____

Counsel for and on behalf of
Plaintiff,
(Duly Authorized)

_____

Counsel for and on behalf of
Defendant
(Duly Authorized)

_____

Forensic Examiner

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA

IN RE: ABILIFY (ARIPIPRAZOLE) PRODUCTS LIABILITY LITIGATION Plaintiffs, v. Bristol-Myers Squibb Company, Otsuka Pharmaceutical Co., Ltd., and Otsuka America Pharmaceutical, Inc., Defendants.	Case No. 3:16-md-2734 Chief Judge M. Casey Rodgers Magistrate Judge Gary Jones

DECLARATION OF JONATHAN K. JAFFE
RE: DEFENDANTS' PROPOSED FORENSIC PRESERVATION AND INSPECTION PROTOCOL

IN BRIEF

On November 28, 2017, Defendants circulated their proposed Forensic Preservation and Inspection Protocol.

As Plaintiffs' retained ESI Expert, I have had the opportunity to thoroughly review Defendants' proposed protocol.

The proposed protocol is disproportionate to addressing shortcomings in the Plaintiffs' production of gambling related documents, email, and data responsive to Defendants' interrogatories and requests for production.

The proposed protocol does not protect sensitive information on Plaintiffs' devices, would place undue burdens on Plaintiffs, and exposes data and communications from third parties not party to nor relevant to this case without adequate control, notification nor protection.

To the extent that the Court requires additional production I propose:

(1) Plaintiffs to search devices and produce relevant information.
Herein this is noted as STAGE I.
(2) Only for good cause shown a Forensic Examiner to search limited devices of a Plaintiff.
Herein this is noted as STAGE II.

BACKGROUND

I was retained in February 2017 as Plaintiffs' ESI Expert.

My CV is attached as Exhibit 1.

I have been assisting Plaintiffs' counsel in several aspects of ESI production in this litigation. Up to this point, my involvement has been limited to productions *received* from Defendants. I have **not** been previously involved in the productions of Plaintiff data to Defendants.

In other mass tort and pharmaceutical litigations, I have been involved in the substantial production of Plaintiff data to Defendants.

In multiple litigations, I have been consulted on the protection of sensitive personal data inclusive of the most sensitive personal data (SSNs, dates of birth, medical identifiers, etc.) and financial data (account numbers, passwords, etc.).

CRITIQUE OF DEFENDANTS' NOV 28 PROPOSED PROTOCOL

Proportionality

The Defendants' proposed protocol requires the production of all devices (physical or virtual) in the possession, control or custody of Plaintiffs which could potentially contain evidence of gambling. This definition includes not only Plaintiffs' own computers, laptops and cell phones, but also as written any spousal or dependent computers, cell phones, and online accounts. If a Plaintiff owns a business, this definition would include all devices part of that business. If a Plaintiff pays for a cell phone for his/her parent, then it would include that device as well. If a Plaintiff's acquaintance has lent them a computer or similar device, then as that device is in Plaintiff's custody, it would include that as well.

To illustrate the scope of devices envisioned by the Defendants, one of the devices specifically cited as an example by Defendants was a Kindle.

Indeed, the definition of a computer used by Defendants is so broad that Plaintiffs would have to turn over their childrens' game controllers (Xboxes, PlayStations), smart TVs with Internet capability, WiFi routers with history, even printers.

The Defendants have asked for Plaintiffs social media accounts indiscriminately which would include Facebook private messages, direct Twitter messages, Instagram posts, and even postings to self-help groups such as Gamblers Anonymous.

Defendants' Forensic Examiner is instructed not only to search these information stores, but to retain complete forensically valid images, electronic pictures containing ALL of the data in these devices and accounts irrespective if the device contains responsive material. Specifically, the protocol states under the section of Imaging of the Devices that the "Forensic Examiner shall make at least one full forensic bit stream copy of each Device(s) onto Target Media." The Forensic Examiner is allowed to make unlimited copies of these images. While Plaintiffs are required under the protocol to maintain a

chain of custody on their devices, the Forensic Examiner is not required to maintain logs of access, duplication, and destruction of images of these devices, just the Devices themselves.

The destruction of the imaged devices requires a joint request by both parties, and does not specifically trigger that the imaged devices will be destroyed after a specific amount of time nor that all copies of a device will be destroyed. There is no required certification of destruction and production of the chain of custody. There is no accommodation of the destruction of files exported from an imaged device.

This type of search, retention and unaccountable reproduction is extraordinarily intrusive and incredibly disproportionate to the discovery of admissible evidence.

Further to this, there has been no evidence or finding of spoliation to warrant such an invasive and unusual extreme remedy. There are less invasive and burdensome solutions.

Undue Burden

The process for gathering and imaging these devices will be lengthy. Devices will have to be packed, shipped to Plaintiffs' attorneys, made available to the Defendants' Forensic Examiner, imaged by the Examiner, returned to Plaintiffs' attorneys, packed and shipped back to Plaintiffs. Depriving Plaintiffs of their devices, especially devices under their custody or control but not directly their devices (ex: a parent, child's or a spouse's smart phone), for such a length of time as will be required to image all these devices imposes a terrible burden on Plaintiffs who cannot simply swap out one device for another.

The Defendants' proposed protocol imposes a very strict five-day deadline on Plaintiffs to produce the devices, but provides no assurance or deadlines by which Plaintiffs are assured of getting their devices returned in a timely manner.

Defendants further impose upon Plaintiffs the burden of documenting a complete chain of custody for each device going back an unspecified time including "all persons who handled, inspected, analyzed/examined, performed maintenance, or transported the Device(s) and any component part thereof and identify the locations and conditions under which it was stored or moved."

Carte Blanche

The Defendants' protocol imposes virtually no limits on the investigation of the Forensic Examiner. The only limit is emails from a list of domains/email addresses sent in advance by Plaintiffs.

Defendants automatically receive ALL data found by the Forensic Examiner

The Defendants' protocol specifically says "after the 3-day first look period, the Forensic Examiner will produce a copy of its results to Defendants." This is repeated twice in the protocol: "All information produced to the Plaintiffs will be produced to the Defendants after the 3-day first look period." The 3-day look period is assumed to be regular days, not business days. There is no accommodation for Plaintiffs' counsel to review for Privilege and Redaction. The only remedy offered to Plaintiffs is to claw-back documents later deemed as privileged, but this includes no opportunity to claw-back documents

produced in error, containing unredacted confidential information, or documents irrelevant to the request. There is no opportunity to exclude non-relevant, non-responsive information.

No Enforced Security Measures

The Defendants' protocol does not lay out security requirements for the storage and inspection of the device. Plaintiffs are giving native files, passwords, and general access to very sensitive information under the protocol. The Forensic Examiner should be required to store all access codes, devices and files encrypted at rest, to perform examinations disconnected from the Internet and other networks, to log all access, and to have physical restrictions and monitoring in place (secure room, locked cabinet, security cameras). The Forensic Examiner should be required to report any unauthorized access and other incidents.

No Protocol for Production Format

The Forensic Examiner is not obligated to follow production protocol when producing documents and data to Defendants. The Forensic Examiner is at liberty to produce documents without Bates numbers and in Native format.

Forensic Examiner is not a Neutral Party

The Forensic Examiner is only obligated to "function as a neutral in terms of protecting data privacy and privilege." Otherwise, the Forensic Examiner is hired by the Defendants, will run their examination under direction of the Defendants, is not obligated to share the direction of the Defendants, can produce documents and data beyond the scope of evidence limited to gambling, and even "shall provide access to any non-privileged files contained on the Device(s) to either counsel that is evidence of gambling." The Forensic Examiner is not precluded from being retained as an expert by the Defendants.

Gambling is NOT a Well-Defined Term

As Defendants noted in their prior motion, gambling sites are not uncommonly listed under obfuscated names. Ambiguity may lead the Forensic Examiner to produce confidential data that is not clear evidence of gambling, but will have that taint, especially if the Forensic Examiner is later retained as an expert by the Defendants.

The proposed protocol does not limit disclosures to confirmed gambling information. Willfully or not, the Forensic Examiner is likely to disclose documents and data that are unrelated.

Insufficient Protection of Confidential Information including Passwords and Indirect Access

It is one thing to produce a bank statement, but the coerced production of passwords and access to online email enables the ability to reset access to accounts that day or months later. There is no restriction on how passwords are stored or requirements a Plaintiff representative for access after the initial imaging of online services. The mere knowledge that the Forensic Examiner holds information to Plaintiffs' bank accounts and other confidential information will be undoubtedly intimidating.

There are no restrictions on what information will NOT be provided to Defendants. There is no accommodation for redaction of sensitive information nor even definition of what would be considered sensitive information.

Insufficient Protection of Privileged Conversations

There is no protection for third party privileged conversations. What if a Plaintiff emailed a criminal attorney? a bankruptcy attorney? a divorce attorney? or received emails from the proceeding? In New York, an email between spouses discussing a conversation with an attorney is protected. Will the Forensic Examiner understand all the potential implications in all of the jurisdictions? Plaintiffs' counsel may not have sufficient knowledge to be able to identify what is privilege in advance.

Insufficient Protection of the Rights of Third Parties

The Defendants' protocol includes a request for devices under the possession, control, or custody of the Plaintiffs. That broad definition includes devices that undoubtedly have the personal information of third parties not a party to this specific litigation including their passwords, accounts, SSNs, dates of birth, credit card numbers, etc. There is no protection of the rights of those third parties.

Insufficient Protection of Protected Health Information

The Forensic Examiner will have access to protected health information including medical records, medical bills and conversations with doctors not relevant to this litigation including records Plaintiffs might have regarding their spouse, children, relatives, and anyone else falling under their care. There is no avenue to prevent this information from appearing in a search or being produced.

Insufficient Protection of Employment Information

The Forensic Examiner will be able to see trade secrets and proprietary information stored on any of these devices even if the information has been deleted from the device through their forensic investigation. There is no adequate protection of this information from the Forensic Examiner nor from being produced to the Defendants.

To this end to the extent the Court required additional production I propose the following:

STAGE I

(a) The Plaintiffs' designated ESI Expert will meet and confer with each Plaintiff and where appropriate their spouses/children to list out devices currently or previously under the possession, control or custody where gambling activity reasonably could have taken place. The Plaintiffs' ESI Expert will also log all devices within the possession, control or custody of each Plaintiff.

(b) The Plaintiffs' designated ESI Expert will meet and confer as well on each online account and each email account currently or previously under the possession, control or custody of the Plaintiff.

(c) Relevant portions of each identified device and account will be searched for documents and data responsive to the Defendants' prior requests.

(d) These documents will be produced in accordance with the existing protocols. Plaintiffs will meet and confer with Defendants to agree on the production format of any data (such as online gambling data) that does not fall directly under the existing protocols.

(e) Plaintiffs will certify that they disclosed all devices and accounts to Plaintiffs' ESI Expert and made them available to be searched.

(f) Plaintiffs and Defendants will meet and confer to agree upon reasonable timelines for the search and production.

STAGE II (only in the case for a specific Plaintiff that Defendants can show good cause why documents and data produced through Proposal I is insufficiently responsive to Defendants' request)

(a) Defendants will retain a Forensic Examiner mutually agreed to by the Parties.

(b) The Forensic Examiner will be allowed in the presence of the Plaintiffs and their attorney to examine specific identified devices and online accounts. At any time during the examination, the Plaintiffs may object to any part of the inspection, the Forensic Examiner will halt the examination, and the Plaintiff attorneys will be able to defer examination of that particular device or area of the device. Until a decision is reached on that particular device, the device would be retained by the Plaintiff's attorney.

(c) The Forensic Examiner would collect relevant documents from that device or account. The Plaintiffs would enter all passwords and access codes to which the Forensic Examiner would not have access.

(d) The Forensic Examiner would create MD5 hashes of any documents collected. The Forensic Examiner would retain the hash values and turn over any documents to the Plaintiffs' attorneys.

(e) The Forensic Examiner would log all devices and accounts searched and the extent and nature of each search.

(f) Plaintiff attorneys would prepare responsive documents collected for production, converting to the appropriate format, redacting and reviewing for privilege.

(g) These responsive documents would be produced to the Defendants in the ordinary manner of production.

(h) If there were a challenge to the authenticity of a particular document, the Forensic Examiner could authenticate the document using the MD5 hash value.

(i) The Forensic Examiner would be precluded from being retained as an Expert witness for the Defendants.

CERTIFICATION

I hereby certify that the foregoing statements made by me are true. I am aware if any of the foregoing statements made by me are willfully false, I am subject to punishment.

Digitally signed by Jonathan Jaffe
DN: cn=Jonathan Jaffe, o=www.its-your-internet.com, ou, email=jjaffe@its-your-internet.com, c=US
Date: 2017.11.30 19:19:14 -05'00'

_____

Jonathan K. Jaffe

www.its-your-internet.com

Dated: November 30, 2017

JONATHAN JAFFE
www.its-your-internet.com (866) 526-1836
Forest Hills, New York 11375 jjaffe@its-your-internet.com
linkedin.com/in/jonathankjaffe

EXPERT TECHNOLOGY + LITIGATION CONSULTING

Technology Negotiator… Federal Expert Witness…Discovery Consulting
Database Analysis…Statistical Sampling…Gap Analysis…Forensics

Its-Your-Internet **2008-present**

Its-Your-Internet is a bespoke technology software and general litigation support consultancy. It was established in March 2008.

Founding Owner, *2008-present;*

- Plaintiffs' Technical Representative for Over 500 Firms on Multiple Mass Tort Litigations involving Product Liability with Medical Devices and Drugs (hundreds of thousands of individual plaintiffs collectively)
- Plaintiffs' Technical Representative in Multiple Class Action Suits (many involving Fair Credit Reporting Act violations in consumer reporting)
- Plaintiffs' Technical Representative in Attorney General Suits involving Product Liability
- Litigation Technical Consulting
    - $247MM jury verdict (Nov 2017)
    - $1.04B jury verdict (Dec 2016)
    - $502MM jury verdict (Mar 2016)
    - Expert Witness in Federal Cases on Technical Issues
    - Database Analysis (Adverse Event/Safety, Clinical Trial, Registry, Call Note, Sales and Marketing, Statistical Analysis)
    - Sample Size Analysis
    - Working with Extremely Large Document Productions (100MM+ pages)
    - Working with Extremely Large Database Productions and Extracts
    - Analysis of Statistical Results from Clinical Studies
    - Trial Support (exhibit list document selection and preparation, helping find documents used with adverse witnesses and in cross examination, translating finds into usable exhibits, demonstratives, jury charges)
    - Built Production Review Tools (software applications) and Processes
    - Discovery Format and Production Negotiation
    - Keyword Search Term Recommendations
    - Custodial Production Forensics
    - Custodial Production Storage Recommendations
    - Deduplication, Gap Analysis, Forensic Analysis, Discovery Issues Analysis
    - Assisting Attorneys on 30(b)(6) Depositions, Meet and Confers, Hearings, Motions, Draft Orders, Stipulations, Rule 34 issues
    - Supporting other Expert Witnesses
    - Creating Supporting Reports for Hearings
    - Deposition Workup

- Supervising and participating (design, coding, analysis) over a large variety of projects, most with significant teams, inclusive of:
    - Litigation Support Custom Applications / Software / Data Analysis
    - Subscription Site for M&A Information, Oauth2 Authentication, Graph Analysis, and Internal Application Development for Investment Bank
    - Real-time Chat Extension for Large VoIP Provider
    - Redesign of Class Action Support System for a Top 3 Legal Administrative Services Firm (Billions of Dollars of Administration)
    - LMS and Exam SaaS applications for West African Market
    - Mobile West Africa #1 App – FindAMed
    - Subscription Based Site for Theater and Performing Arts Companies
    - School Based Management Systems Development
    - Raffle Contest Site and Variations
    - Writing and Support for Core Remake of Multi-Million Page Web Site
    - SEO and SEM Management for Multiple Clients
    - Finalist in Multi-Billion $ RFP for NYC DOE
    - > 50 original web sites inclusive of e-Commerce
    - Countless consultations with Entrepreneurs
- Multiple Entrepreneurial Projects Using Bleeding Edge Technology
- Established a Dozen Key Reciprocal Partnerships
- > 30 Talks and Lectures on Technology and Social Media for Chambers of Commerce, SBA, Charities and Non-Profit, Business Groups and Organizations
- Day to Day Resource Management, Staffing, Administration
- Oversight of Remote and Offshore Resources
- Branding, Marketing, Materials (for Firm and Clients)

Technologies: NoSQL, SQL, C#, PHP, NodeJS, Python, Django, NPM, PaaS, Heroku, HTML5, BackboneJS, EmberJS, AngularJS, MongoDB, Cloudant, Redis, MSSQL, Oracle, MySQL, MariaDB, Postgres SQL, ExpressJS, Git/GitHub, GruntJS, E2E Testing, ASP.NET MVC, ASP.NET, Cordova PhoneGap, Amazon Web Services (S3, CloudFront, EC2), XML, XML Schema, LESS, CSS3, SocketJS, Bower, Joomla, Drupal, WordPress, Office Live, SharePoint, SalesForce, JIRA, Photoshop, Illustrator, GIMP, RESTful and Agile Methodologies.

Weitz & Luxenberg, P.C. **2002-2008**

Weitz & Luxenberg is one of the nation's original and foremost firms in mass tort asbestos litigation handling nearly one million simultaneous pending court actions, 250,000 bankruptcy claims, and over 50 other personal injury litigations.

Manager of Software Development, *2003-2008*
Sr. Project Manager, *2002-2003*

- Federal Expert Witness resulting in substantial eDiscovery Sanctions
- Collection of documents for litigation; Validation; Forensic Analysis
- Coordinated activities of 5 teams, comprising 20 resources

- Achievements included: establishing and overseeing the 4th largest personal injury law firm site, www.weitzlux.com, all internal development, sales/marketing efforts, public relations, and client services.
- Chief software architect.
- Increased site traffic 5,000% (to 12,000+ unique visitors/day) and original content by 2MM+ pages.
- Positioned web site as a new sales channel, netting $MM in new revenue, 45,000% increase in leads to 1,500 new case leads/week.
- Gained first page ranking for 750,000+ search terms used to find the site including some of the most competitive (ex. *asbestos lawyer*).
- Reduced annual Internet marketing costs by $3.6 million, or 96%, while increasing returns.
- Transformed internal development into a premier asset of the firm resulting in joint development efforts with Federal Express, 2 case studies on our use of Web Services by Microsoft, and the adoption of our proprietary document management technologies by other law firms across the country.
- Oversaw distribution of $300 million/year in settlements to tens of thousands of clients.
- Increased overall internal system performance 500% with a 75% reduction in system downtime.
- Mentored technical team, developers, analysts, SEO (search engine optimization)

Technologies: C#. VB.NET, ASP.NET, SQL2005, SQL2000, OLTP, OLAP, JavaScript, HTML, Exchange2003, Win2003, IPSec, CISCO VPN, Citrix Presentation Server, Win2000, WinNT4, Project, PowerPoint, WebSense, eSafe, Active Directory (LDAP) Interface, XML, xHTML, Web Services, Visual Studio Team Foundation Server, VSS, VB6, Access, Microsoft Office, Cisco PIX (Firewall), Tape Library Backup, Document Management, CRM, ERP, Great Plains 7.0, Great Plains 6.0, Goldmine, ASP3.0, IIS 6.0, Windows Services, Snap NAS, LeadTools (Imaging), SharePoint, AscentCapture, Concordance, Summation, iConnect, ComponentOne for .NET, Flash, Mac OSX, Photoshop, SEO

Case Studies (Business + Technology):

http://download.microsoft.com/documents/customerevidence/27250_Weitz_Lux_Final_BA.doc

http://download.microsoft.com/documents/customerevidence/27249_Weitz_Lux_Final_CS.doc

IMJ Group Inc. **2001-2002**

IMJ was a startup business/technology consulting think tank and solution implementation firm I started with two partners.

Vice President, Technology / Founding Partner

- Established corporate status for the firm and branding.
- Recruited and supervised staff.

Technologies: Linux, BSD, Java, Access, Microsoft Project, Microsoft PowerPoint, Microsoft Excel.

Winstar Communications, Inc., Web Development Group **2000-2001**

The Winstar Web Development Group was an Internet consultancy, part of Winstar (a dot-com telecommunications firm), specializing in large Intranets and Internet sites.

Acting Director of Technology, *2001;*
Senior Technology Architect, *2000-2001*

Technical Leadership

- Directed a team of 17 – project managers, developers, system engineers, and site designers.
- Managed full project lifecycle for six and seven digit budgets.
- Chief Software Architect.
- Designed Internet and Intranet sites, including Hosting Solutions.
- Established procedures and process, integrating what had been five company acquisitions into one team.
- Mentored development team.

Business Development

- Increased average project value 10,000% (from $50,000) to $5 million, including winning the team's first $1 million contract.
- Liaised successfully with other Winstar divisions (Hosting, Office.com, Professional Services, and Winstar for Buildings) resulting in improved sales and project coordination.
- Led Winstar team on a $50 million proposal for the NYC Board of Education with partners Sun, Oracle, Lucent, Microsoft and Compaq.

Technologies: ASP 3.0, SQL2000, SQL 7.0, JavaScript, HTML, Project, PowerPoint, VSS, Exchange2000, Win2000, WinNT4, WebSense, Active Directory, VB6, VB5, Visio, Microsoft Office, Flash, Photoshop, QuarkXpress.

Example web site: http://www.nationalmssociety.org still largely uses the same information architecture laid out over 14 years ago.

Valinor, Inc. **1995-2000**

Valinor Inc., a wholly owned subsidiary of IKON Office Solutions, was the original Microsoft Solutions Partner/Provider & Authorized Technical Education Center in New York City, consulting for Fortune 500 firms.

Technical Project Manager / Microsoft Certified Trainer, 1998-2000
(after graduating Columbia);

Technical Project Leader / Senior Technical Architect, 1996-1998
(while attending Columbia full time 20+ hrs/wk);

Senior Application Developer / Application Developer, 1995-1996
(while attending Columbia full time, 20+ hrs/wk)

General Achievements

- Increased average project value, formerly $100,000 average, 500% to $500,000
- Led teams of up to 10 developers

Valinor Key Consulting Projects

- **AIG/AIU NAD** — migration of AIG Europe's mainframe-based quotation and policy generation system to Microsoft Windows/Office workstation platforms, reducing the time to policy from days to minutes.
- **Berkery, Noyes & Co.** — a company-wide line of business application matching companies seeking to sell themselves with potential buyers.
- **The College Board** — Internet application to gather annual survey data for all United States accredited colleges and universities.
- **DLJ** — on site training.
- **Garban Intercapital** — a cash derivatives trading system utilized by 60 brokers.
- **IKON Office Solutions** — reconciled revenue reporting data from multiple disparate databases.
- **Matsushita** — workflow support ticketing system.
- **Maersk Shipping** — reconciled multiple shipping databases.
- **Merrill Lynch** — on site training on active trading floors.
- **NYC Department of Technology** — on site training.
- **Sumitomo Mitsui** — application to monitor, track and handle all transactions and interest calculations for a multi-billion per year transfer of high risk loans.
- **Sun Chemical** — on site training and follow up consulting.
- **Yankee Copyrights Management** — a large eCommerce application for a startup to create a marketplace for permissions to use and replicate copyrighted materials.

Technologies: ASP2.0. SQL7.0, SQL6.0, Sybase, Oracle, MTS, COM, JavaScript, HTML, Project, Powerpoint, VSS, Exchange5, WinNT4, WinNT3.51, Unix-Solaris, C++, MFC, VB6, VB5, VB4, VB3, Access, Visio, Goldmine, Microsoft Word, Excel

ADJUNCT PROFESSOR

Columbia University School of Continuing Education, evening classes **2003-2005**

- Taught Database Design/Advanced SQL, and .NET Programming courses — QC7304, QC7305, QC7403.
- Developed curriculum for courses, part of SASE track certificate program.

EDUCATION

Bachelor of Arts, Economics/Mathematics, Magna cum Laude 3.72 GPA, Columbia University, 1999

Stuyvesant High School, 1995

CERTIFICATIONS

Microsoft Certified Professional, 1998

Microsoft Certified Trainer, 1998

MAJOR LAW FIRMS

LANIER FIRM

BARON BUDD

SIMMONS HANLY CONROY

WEITZ & LUXENBERG

BERGER MONTAGUE

NICHOLS KASTER

BAILEY PEAVY BAILEY

KAISER GORNICK

SANDERS VIENER GROSSMAN

MAZIE SLATER KATZ & FREEMAN

SALIM BEASLEY

CRONIN FRIED

NEBLETT, BEARD & ARSENAULT

BLASINGAME BURCH GARRARD ASHLEY

PODHURST ORSECK

EXPERT TESTIMONY

Hearings

2015

IN RE BENICAR (OLMESARTAN) PRODUCTS LIABILITY LITIGATION.

No. 15-2606

2010

IN RE: GADOLINIUM BASED CONTRAST AGENTS LITIGATION.

No. 1:08-GD-50000, MDL NO. 1909

2007

In re SEROQUEL PRODUCTS LIABILITY LITIGATION.

No. 6:06-md-1769-Orl-22DAB.

Depositions

2015

Plaintiffs v. SmithKline Beecham Corporation d/b/a,

GlaxoSmithKline

PHILADELPHIA COUNTY

COURT OF COMMON PLEAS

Nos. 01144, 0402, 3694, 3678, 3672, 3758, 3686, 3727, 0489

2015

JOSEPH JAUHOLA VS. CANADIAN NATIONAL RAILWAY COMPANY,

AND WISCONSIN CENTRAL, LTD.

No. 14-cv-1433

2007

In re SEROQUEL PRODUCTS LIABILITY LITIGATION.

No. 6:06-md-1769-Orl-22DAB.

SPEAKING ENGAGEMENTS

Chambers of Commerce

- Greater NY Chamber of Commerce
- Forest Hills Chamber of Commerce
- Franklin Square Chamber of Commerce
- Medford Chamber of Commerce
- Rockville Centre Chamber of Commerce
- Oceanside Chamber of Commerce
- BRiSC - the Unofficial Silicon Alley Chamber of Commerce

Small Business Administration

- USSBA (March 2010)
- USSBA (April 2010)
- USSBA (May 2010)

Business Groups and Organizations

- Independent Business Women's Group
- Associated Builders & Contractors – Lower NY State
- Associated Builders & Contractors – Nassau/Suffolk
- East End Women's Network

Charities and Non-Profits

- Northport Rotary
- Kiwanis International

Continuing Education

- Columbia University – School of Continuing Education – adjunct professor
- Locust Valley Adult Education
- College of New Rochelle – Graduate Program
- Monroe College – Graduate Program

EXHIBIT 3

VERIFICATION

I declare under penalty of perjury that all of the factual information contained in the Jennifer Lilly section of the attached Response in Opposition to Defendants' Motion to Compel the Search and Forensic Inspection of Plaintiffs' Computers and Other Devices for Forensic Inspection is true and correct to the best of my knowledge, information and belief.

Signature Jennifer Lilly Date: November 30, 2017

Witness Signature Kari Nunes Date: November 30, 2017

EXHIBIT 4

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION

IN RE: ABILIFY (ARIPIPRAZOLE) PRODUCTS LIABILITY LITIGATION This Document Relates to the Following Case: *Marshall v. Bristol-Myers Squibb Company, et al.*, 3:17-cv-172	MDL No. 3:16-md-2734 Chief Judge M. Casey Rodgers Magistrate Judge Gary Jones

DECLARATION OF PLAINTIFF BRYAN MARSHALL REGARDING RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO COMPEL

I, Bryan Marshall, do hereby state as follows:

1. I did not gamble online on a third party computer. The third party computer was used to access my iCloud e-mail account.

2. I am not in possession of old laptops. I purchased them at pawn shops and sold them at pawn shops. I sold my last laptop in 2013. I do not have documentation related to these transactions. I do not recall the pawn shops where these transactions took place.

3. I am not in possession of old cell phones. I typically returned them to the carrier when I received upgrades. I smashed one of my old cell phones during a psychotic episode. I do not recall the date of this episode.

4. I have had my current phone since approximately December 2015. The carrier is Verizon. I used my current phone to access the following gambling websites/ games: World Series of Poker, Zynga Poker, and www.Bodogs.com.

VERIFICATION

I declare under penalty of perjury that all of the factual information contained in the above Declaration is true and correct to the best of my knowledge, information and belief.

Signature: B. Marshall Date: 12/01/2017