



AMERICAN
BANKRUPTCY
INSTITUTE

42nd Annual Alexander L. Paskay Memorial Bankruptcy Seminar

E-Discovery: How to Avoid Being TARred and Feathered

Hon. Roberta A. Colton

U.S. Bankruptcy Court (M.D. Fla.); Orlando

James D. Gassenheimer

Berger Singerman LLP; Miami

Michael G. McCartney

Avalon Cyber; Buffalo, N.Y.

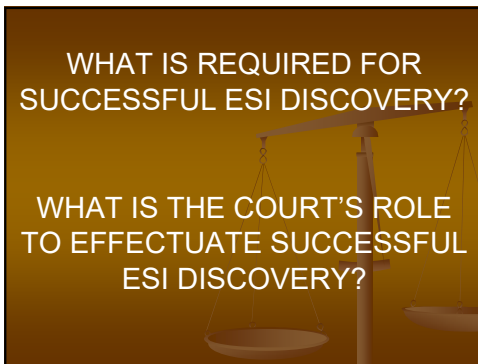
Hon. Anthony E. Porcelli

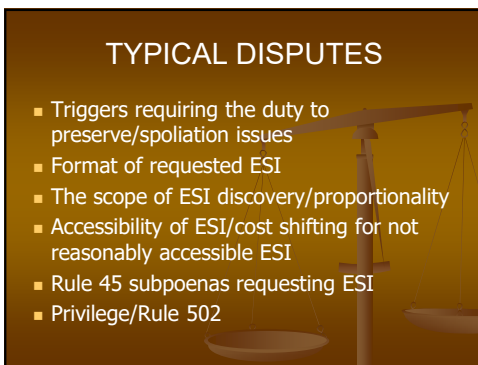
U.S. District Court (M.D. Fla.); Tampa

Hon. Julie S. Sneed

U.S. District Court (M.D. Fla.); Tampa







HYPOTHETICAL

- During the discovery process, Ms. Quinn requested a video copy of the March 18, 2016 TV segment. In response to the request, HSTV informed Ms. Quinn that they cannot produce a copy of the March 18th segment because due to their limited storage capacity all historical TV segments are only saved for 90 days and that the March 18th segment was deleted on June 16, 2016. Further, HSTV also informed Ms. Quinn that they have been advised by Mr. Joker that he deleted the video from his Facebook account on June 21, 2016. Ms. Quinn is now requesting sanctions be imposed for the spoliation of the March 18, 2016 TV segment. Specifically, Ms. Quinn is requesting that a default judgment be entered against HSTV, or in the alternative that an adverse jury instruction be given to the jury.

Revised Fed. R. Civ. P. 37(e)

(e) FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION:

If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

- (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
 - A. presume that the lost information was unfavorable to the party;
 - B. instruct the jury that it may or must presume the information was unfavorable to the party; or
 - C. dismiss the action or enter a default judgment.

PRESERVATION AND SPOILIATION

- WHEN DOES A PARTY'S PRESERVATION OBLIGATION BEGIN?
- WHAT CAN BE DELETED WITHOUT RISKING A CHARGE OF SPOILIATION?
- WHAT IS THE APPROPRIATE BALANCE BETWEEN PRESERVING POTENTIALLY RELEVANT INFORMATION WITHOUT IMPOSING UNDUE COST AND DISRUPTION?

LITIGATION HOLD

- A "litigation hold" must be disseminated and monitored.
 - In re Old Banc One Shareholders Security Litigation, 2005 WL 3372783 (N.D. Ill.)
 - Danis v. USN Communications, Inc., 2000 WL1694325 (N.D. Ill.)
 - E-mailing employees may be insufficient! In re Prudential Sales Practices Litigation, 169 F.R.D. 598, 615 (D.N.J. 1997)

"Identifying the boundaries of the duty to preserve involves two related inquiries: *when* does the duty to preserve attach and *what* evidence must be preserved?"

Zubulake v. UBS Warburg LLC,
220 F.R.D. 212 (S.D.N.Y. 2003)
(Zubulake IV)

HYPOTHETICAL

- During discovery HSTV only produced 12 of the alleged 25 e-mails sent by Mr. Joker to Ms. Quinn in January through February, 2016. Ms. Quinn is now requesting that the backup tapes be restored to search for the remaining emails. As for HSTV's backup system, the e-mail servers were backed up onto backup. According to HSTV's IT Director, each server was backed up as a unit; the e-mail of a particular employee could not be restored individually. Accordingly, if one individual's e-mail had to be recovered, the entire server would have to be restored. Such a restoration could take from two to five days. HSTV estimates that it would cost in excess of \$10,000 to restore one backup tape and that there are 4 backup tapes that would need to be restored. Ms. Quinn requests that HSTV be compelled to restore the 4 backup tapes.

RULE 26

Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the:

- (1) issues at stake in the action,
- (2) the amount in controversy,
- (3) the parties' relative access to relevant information,
- (4) the parties' resources,
- (5) the importance of the discovery in resolving the issues, and
- (6) whether the burden or expense of the proposed discovery outweighs its likely benefit.

NOT REASONABLY ACCESSIBLE DATA

- A party asserting that ESI is "not reasonably accessible," and thus not subject to discovery under Rule 26(b)(2)(B) absent a showing of good cause, has the burden of proving the undue burdens and costs of accessing it
- May likely require additional discovery
- Presumptive data (unallocated data, RAM, cache)

GOOD CAUSE TO OBTAIN NOT REASONABLY ACCESSIBLE ESI

- (1) the specificity of the discovery request;
- (2) the quantity of information available from other and more easily accessed sources;
- (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
- (5) predictions as to the importance and usefulness of the further information;
- (6) the importance of the issues at stake in the litigation; and
- (7) the parties' resources.

■ See Rule 26(b)(2)(B) advisory committee note

COST SHIFTING

- SEDONA SAYS THE COSTS OF RETRIEVING **AND REVIEWING** THE INFORMATION SHOULD BE SHIFTED. SEDONA PRINCIPLE 13 AND COMMENTARY 13(a)
- BUT CASES GENERALLY SHIFT ONLY THE COST OF RETRIEVAL, NOT COST OF REVIEW (see e.g., *ZUBULAKE, ROWE*).

7-FACTOR TEST FROM *ZUBULAKE v. UBS WARBURG LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) AND 216 F.R.D. 280 (S.D.N.Y. 2003) (J. SCHEINDLIN)

- "1. THE EXTENT TO WHICH THE REQUEST IS SPECIFICALLY TAILORED TO DISCOVER RELEVANT INFORMATION;
- 2. THE AVAILABILITY OF SUCH INFORMATION FROM OTHER SOURCES;
- 3. THE TOTAL COST OF PRODUCTION, COMPARED TO THE AMOUNT IN CONTROVERSY;
- 4. THE TOTAL COST OF PRODUCTION, COMPARED TO THE RESOURCES AVAILABLE TO EACH PARTY;
- 5. THE RELATIVE ABILITY OF EACH PARTY TO CONTROL COSTS AND ITS INCENTIVE TO DO SO;
- 6. THE IMPORTANCE OF THE ISSUES AT STAKE IN THE LITIGATION; AND
- 7. THE RELATIVE BENEFITS TO THE PARTIES OF OBTAINING THE INFORMATION."
- UNDER THIS TEST, AFTER REVIEWING A SAMPLE OF E-MAILS FOR 5 DATES, ASSESSED PLAINTIFF 25% OF COST OF RESTORING 77 BACKUP TAPES; BUT MADE DEFENDANT PAY FULL COST OF RESTORING OTHER BACKUPS ON SEARCHABLE OPTICAL MEDIA.

FORM OF PRODUCTION DISPUTES

- DOES THE E-INFORMATION HAVE TO BE PRODUCED IN A SEARCHABLE FORMAT?
- DOES THE E-INFORMATION HAVE TO BE PRODUCED IN MULTIPLE FORMATS?

RULE 34

- THE REQUEST MAY SPECIFY THE FORM IN WHICH ELECTRONICALLY STORED INFORMATION IS TO BE PRODUCED
- THE RESPONDING PARTY MAY OBJECT TO THE FORM REQUESTED
- IF THE REQUESTING PARTY DOES NOT SPECIFY THE FORM OF PRODUCTION, ABSENT AGREEMENT OR COURT ORDER THE RESPONDENT **MUST** PRODUCE E-INFORMATION IN A FORM IN WHICH IT IS ORDINARILY MAINTAINED, OR IN A REASONABLY USABLE FORM

AVOID THE PROBLEMS AND CONFRONT E-DISCOVERY ISSUES EARLY

- CONFRONTING E-DISCOVERY ISSUES EARLY SHOULD INCLUDE, FOR EXAMPLE, THE PARTIES EXCHANGING INFORMATION ABOUT THEIR COMPUTER SYSTEMS, IDENTIFYING E-DISCOVERY TECHNICAL POINT PERSONS, AND DISCUSSING THE TYPES OF E-DATA THAT WILL BE SEARCHED AND PRODUCED AND IN WHAT FORMAT

PARTIES DISCOVERY PLAN

- **RULE 26(f)(3):** THE PARTIES ARE TO DISCUSS ANY ISSUES RELATING TO DISCLOSURE, DISCOVERY, OR PRESERVATION OF ELECTRONICALLY STORED INFORMATION, INCLUDING THE FORM OR FORMS IN WHICH IT SHOULD BE PRODUCED, AND
- ANY ISSUES RELATING TO CLAIMS OF PRIVILEGE OR PROTECTION OF TRIAL-PREPARATION MATERIAL INCLUDING – IF THE PARTIES AGREE ON A PROCEDURE TO ASSERT SUCH CLAIMS AFTER PRODUCTION – WHETHER TO ASK THE COURT TO INCLUDE THEIR AGREEMENT IN A RULE 502 ORDER

26(f) CONSIDERATIONS

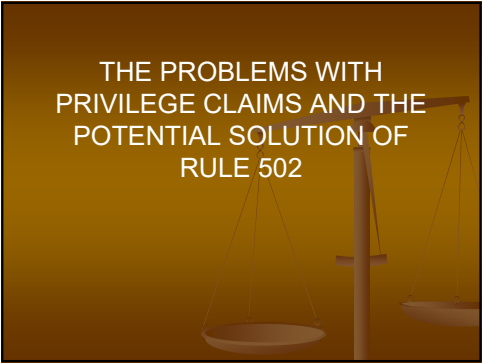
- whether there will be discovery of ESI at all;
- disclosures required under Federal Rule of Civil Procedure 26(a)(1), if any, and their timing;
- what types or categories of discoverable information each party has in electronic form, and where and on what type of media that information is likely to be found;
- the steps each party will take to preserve different types or categories of ESI;
- the number and identity of "key players" who are knowledgeable about potentially relevant ESI and on whose servers or devices ESI is likely to be found;
- what methods will be efficient in identifying discoverable ESI (e.g., sampling, key word searches);
- the anticipated schedule for production;
- the form in which such information is ordinarily maintained and whether it will be produced in that form—usually known as "native format"—or in another form;
- the scope of discovery of different categories of ESI, such as e-mail messages;
- whether relevant information has been deleted, and if so, whether one or more parties believe deleted information needs to be restored and who will bear the cost of restoring it;
- whether any information is not "reasonably accessible," the burdens and costs of retrieving that information, why it is needed, and any conditions that should be placed on its production, including who will bear the cost; and
- whether relevant information is in the possession of nonparties from whom discovery under Rule 45 will be required.

COURT EXPECTATIONS

- having a knowledgeable person describe the party's information systems, storage, and retention policies and practices to the opposing party and the court;
- interviewing key employees to determine sources of information;
- affirmatively and repeatedly communicating litigation holds to all affected employees and other persons and monitoring compliance on an ongoing basis;
- integrating discovery responsibilities with routine data retention policies and practices;
- actively managing and monitoring document collections; and
- documenting the steps taken to design, implement, and audit the litigation hold

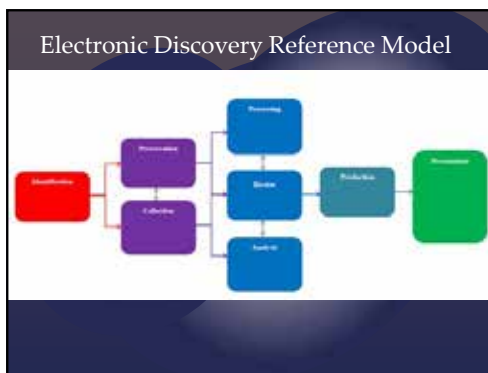
RULE 45 ISSUES

- Rule 45 of the Federal Rules of Civil Procedure conforms the rules on ESI discovery from third parties to those on ESI discovery from parties. Rule 45 introduces the concept of sources that are not reasonably accessible. It addresses the form or forms for the production of ESI, adds a post-production procedure for asserting claims of privilege or of protection as trial-preparation materials, and allows for the testing or sampling of ESI
- Although Rule 45 has no equivalent to the Rule 26(f) conference process, parties seeking discovery from nonparties under Rule 45 should be encouraged to meet informally with nonparty respondents and to discuss the scope of the subpoena, the form in which ESI will be produced, protection against waiver for privileged and protected information, and the allocation of discovery costs



12/16/2017





Scoping

How can you assist with the duty to preserve?

- Custodians: which individuals have relevant ESI?
- Devices
- Consider the type of information on each device
- Automatic purge policies
- Third-Party with Repositories

12/16/2017

Where is our data?

- Single on Premise Server
 - Email and files
- Desktops/Laptops
 - User files
- No remote access
- No BYOD
- No Cloud
- No outsources services

Entities & Types of ESI

- Banks
- Corporations
- Individuals

Preservation

- Litigation Hold Letter
- Purpose
- Proof of Delivery
- Acknowledgement
- Party vs. Non-Party Distinction

Spoliation

- Common issues
 - Collection Errors
 - Incomplete Collection

Collection & Preservation

- What is preservation? collection?
- Form request for production
- Security issues?
- Knowledge of the business and parties involved is required
 - Banks
 - Corporations
 - Individuals

Processing, Review & Analysis

- How to get the information down to a manageable amount of data for review?
- Cost
- What tools/analytics are available on a review platform?
- Search terms
- Hit reports
- Recovering deleted ESI

12/16/2017

Text Analytics

- Email Threading
- Near Duplicate Detection
- Categorization
- Domain Filter
- Prioritization
- Technology Assisted Review

Misc. Issues

- Security in collection/preservation/ review
- Forensic tools to assist in eDiscovery?
- Metadata vs. no metadata
- What should in-house counsel/outside counsel look for in an eDiscovery vendor?
- What are the typical pitfalls in dealing with an outside vendor?

The Federal Standard

- Fed. R. Civ. P. 37(e)
- *Zubulake v. UBS Warburg*




12/16/2017

The Florida Standard



- Fla. R. Civ. P. 1.380(e)
- *League of Women Voters of Florida v. Detzner*, 172 So. 2d 363, 391 (Fla. 2015)
- When are sanctions appropriate?



Procaps S.A. v. Patheon Inc., Case No. 12-24356-CIV-GOODMAN, 2015 WL 4430955 (S.D. Fla. July 20, 2015)



Brown v. Tellermate Holdings Ltd., No. 2:11-cv-1122, 2014 WL 2987051 (S.D. Ohio July 1, 2014)

12/16/2017



Moore v. Publicis Groupe, No. 11 Civ. 1279, 2012 WL 607412(ALC)(AJP)
(S.D.N.Y. Feb. 24, 2012)



Bridgestone Americas, Inc. v. Int'l Bus. Machs. Corp., No. 3:13-1196, 2014 wk 4923014 (M.D. Tenn. July 22, 2014)

Questions?

Michael McCartney
President Avalon Cyber
741 Main Street
Buffalo, NY 14203
Phone: 716-995-7777
Fax: 716-995-7778
Cell: 716-706-8403
Michael.McCartney@teamavalon.com
www.teamavalon.com



James D. Gassenheimer
Berger Singerman
1450 Brickell Ave, Suite 1900
Miami, FL 33131
Phone: 305-755-9500
Fax: 305-714-4340
Direct: 305-714-4383
Jgassenheimer@bergersingerman.com
www.bergersingerman.com



E-DISCOVERY PROBLEM

Home Shopping Television, Inc. (“HSTV” or “Debtor”) filed a chapter 11 bankruptcy on January 3, 2017. HSTV was a \$1.2 billion retailer that marketed products 24 hours a day directly to consumers through live television segments on cable television. The primary goal of HSTV’s chapter 11 was to restructure its secured debt.

Just before the bankruptcy, Harley Quinn filed a lawsuit against HSTV in federal court for one count of sexual harassment and one count of breach of contract. When she received notice of the chapter 11, Ms. Quinn promptly filed a proof of claim for \$1.0 million, and attached a copy of her federal court complaint. HSTV objected to her claim, and the creditor’s committee for HSTV has joined in the objection.

The bankruptcy court will be handling all pretrial and discovery matters on the objection to claim. Under Federal Rule of Bankruptcy Procedure (“Rule(s)”) 9014, the court has ruled that all of the Part VII rules will apply in this contested matter.

Ms. Quinn was an on-air personality/model for HSTV – under an employment contract – from February 1, 2010 to August 1, 2016. Her job was to market consumer products by describing, modeling, and demonstrating the products. HSTV employed 20 on-air personalities. All were paid a base salary with fluctuating bonuses, depending upon the sales resulting from their on-air TV segments. To maximize a bonus, certain time slots and certain products are more coveted than others. For example, selling jewelry at 8:00 pm is far better than selling mops at 3:00 am.

Jack Joker is the Managing Supervisor of TV at HSTV. He is responsible for the work schedules of all on-air personalities. Bruce Wayne is Vice President of TV. He is Mr. Joker’s direct supervisor, and determines what products to sell and when. Mr. Wayne also has the authority to change on-air schedules if he disagrees with Mr. Joker’s scheduling. As supervisors, Mr. Wayne and Mr. Joker are issued HSTV smart phones for both work and personal use.

From 2011 through 2015, Ms. Quinn was HSTV’s most successful and profitable on-air personality. However, in 2016, until her discharge on August 1, 2016, Ms. Quinn’s productivity declined substantially. Ms. Quinn alleges that her decline in sales performance and eventual discharge was due to the sexual harassment she endured from Mr. Joker.

Ms. Quinn alleges the following:

The Holiday Party – December 15, 2015

During an office holiday party on December 15, 2015, Mr. Joker was intoxicated and made unwelcomed sexual advances toward Ms. Quinn. Mr. Joker also used his cell phone to take multiple “selfie” pictures of himself attempting to kiss Ms. Quinn. The very next day, Ms. Quinn

complained in person to Mr. Wayne about Mr. Joker's conduct. She told Mr. Wayne that she was so angry that she was contemplating hiring a lawyer. Mr. Wayne advised Ms. Quinn that Mr. Joker had been having a difficult time since his recent divorce and that he would talk to Mr. Joker about his conduct.

E-mails at Work – January-February, 2016

Despite her conversation with Mr. Wayne, from January through February 2016, Mr. Joker sent Ms. Quinn sexually inappropriate e-mails at work. As she received these objectionable e-mails, she forwarded them to Mr. Wayne with comments, such as "he is at it again," "here is another one," or "he just won't stop." In total, Ms. Quinn received and forwarded 25 e-mails. By the end of February 2016, Mr. Joker stopped sending inappropriate e-mails.

The TV Segment – March 18, 2016

On March 18, 2016, Mr. Joker scheduled Ms. Quinn, along with Dick Grayson and Selina Kyle to appear in a segment to model a new line of bathing suits and bikinis. However, when she arrived at HSTV on March 18th, Mr. Joker told her that due to a scheduling problem, Mr. Grayson was unavailable, so instead he would be on-air with her and Ms. Kyle to model the male bathing suits. During the TV segment, while Ms. Quinn was modeling bikinis, both Ms. Kyle and Mr. Joker described the attributes of the bikinis. As both Ms. Kyle and Mr. Joker described the bikini attributes, Mr. Joker touched the bikini material, the straps, and often Ms. Quinn's skin. Ms. Quinn claims that Mr. Joker intentionally touched her inappropriately multiple times during the TV segment. During the live TV broadcast, numerous customers simultaneously posted their reaction on Twitter with such statements like "Did you see where he just touched her?" The customer reaction on Twitter resulted in "#JokerloveQuinnkini" ranking in the top ten trending tweets on Twitter that day.

When the broadcast ended, Ms. Quinn immediately confronted Mr. Joker. She told him that his conduct was unacceptable and that, in the future, he was not to speak to her unless it was work related. Despite this confrontation, Mr. Joker copied the March 18th TV segment, and, on March 19th, posted the video on his Facebook page stating "My big debut in front of the camera with the lovely Ms. Quinn...don't we make a great couple." Notably, to help expose their brand, HSTV encourages all employees to maintain personal social media accounts and post information about HSTV and its products.

Soon after the March 18th TV segment, Ms. Quinn began noticing that Mr. Joker scheduled her to work during the least desirable time slots. In mid-April, Ms. Quinn emailed Mr. Wayne to complain about her schedule, to which Mr. Wayne responded that if she had a concern about her schedule she should discuss it with Mr. Joker. Eventually, on May 10, 2016, Ms. Quinn emailed Mr. Joker to complain about her schedule, to which Mr. Joker replied "You know what needs to be done if you want your schedule to change." Ms. Quinn immediately forwarded Mr. Joker's

email to Mr. Wayne and stated “See below. I can’t take it anymore! We need to talk. Either your do something about Mr. Joker or I am suing.” Mr. Wayne responded the next day on May 11, 2016, and told Ms. Quinn that he would be out of the office until May 28, 2016, but would be happy to meet with her then to discuss the matter.

The Meeting – May 28, 2016

Ms. Quinn finally met with Mr. Wayne on May 28, 2016. She told Mr. Wayne that she retained a lawyer and handed him a letter from her lawyer. The letter stated that a sexual harassment complaint was being prepared on behalf of Ms. Quinn to be filed with the Equal Employment Opportunity Commission (“EEOC”) (Note: An EEOC complaint is a pre-requisite to filing a lawsuit). The letter further stated that Ms. Quinn intended to pursue all available legal recourses against HSTV, including breach of her employment agreement.

The Complaint – June 20, 2016

On June 20, 2016, Ms. Quinn’s EEOC complaint was served on HSTV. On June 21, 2016, HSTV disseminated a litigation hold to all key personal, specifically including Mr. Joker, to preserve all electronically stored information (“ESI”) pertaining to Ms. Quinn’s allegation of sexual harassment by Mr. Joker.

On August 1, 2016, Ms. Quinn was discharged from HSTV, and on December 15, 2016, Ms. Quinn filed suit against HSTV. HSTV filed its suggestion of bankruptcy with the district court on January 4, 2017.

Discovery in Claim Litigation

During discovery on the claim objection, Ms. Quinn requested a video copy of the March 18, 2016 TV segment. HSTV responded that the video was not available. Due to their limited storage capacity, all historical TV segments are only saved for 90 days. The March 18th segment, therefore, was automatically deleted on June 16, 2016. Further, HSTV informed Ms. Quinn that Mr. Joker deleted the video from his Facebook account on June 21, 2016.

Ms. Quinn now requests sanctions for the spoliation of the March 18, 2016 TV segment. Specifically, Ms. Quinn requests that a default be entered against HSTV and her claim allowed in the full amount of \$1.0 million.

The Joys of E-Discovery



WHAT IS REQUIRED FOR
SUCCESSFUL ESI DISCOVERY?

WHAT IS THE COURT'S ROLE
TO EFFECTUATE SUCCESSFUL
ESI DISCOVERY?



TYPICAL DISPUTES

- Triggers requiring the duty to preserve/spoliation issues
- Format of requested ESI
- The scope of ESI discovery/proportionality
- Accessibility of ESI/cost shifting for not reasonably accessible ESI
- Rule 45 subpoenas requesting ESI
- Privilege/Rule 502

HYPOTHETICAL

- During the discovery process, Ms. Quinn requested a video copy of the March 18, 2016 TV segment. In response to the request, HSTV informed Ms. Quinn that they cannot produce a copy of the March 18th segment because due to their limited storage capacity all historical TV segments are only saved for 90 days and that the March 18th segment was deleted on June 16, 2016. Further, HSTV also informed Ms. Quinn that they have been advised by Mr. Joker that he deleted the video from his Facebook account on June 21, 2016. Ms. Quinn is now requesting sanctions be imposed for the spoliation of the March 18, 2016 TV segment. Specifically, Ms. Quinn is requesting that a default judgment be entered against HSTV, or in the alternative that an adverse jury instruction be given to the jury.

Revised Fed. R. Civ. P. 37(e)

(e) FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION:

If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

- (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
 - A. presume that the lost information was unfavorable to the party;
 - B. instruct the jury that it may or must presume the information was unfavorable to the party; or
 - C. dismiss the action or enter a default judgment.

PRESERVATION AND SPOILIATION

- WHEN DOES A PARTY'S PRESERVATION OBLIGATION BEGIN?
- WHAT CAN BE DELETED WITHOUT RISKING A CHARGE OF SPOILIATION?
- WHAT IS THE APPROPRIATE BALANCE BETWEEN PRESERVING POTENTIALLY RELEVANT INFORMATION WITHOUT IMPOSING UNDUE COST AND DISRUPTION?

LITIGATION HOLD

- A “litigation hold” must be disseminated and monitored.
 - In re Old Banc One Shareholders Security Litigation, 2005 WL 3372783 (N.D. Ill.)
 - Danis v. USN Communications, Inc., 2000 WL1694325 (N.D. Ill.)
 - E-mailing employees may be insufficient! In re Prudential Sales Practices Litigation, 169 F.R.D. 598, 615 (D.N.J. 1997)

“Identifying the boundaries of the duty to preserve involves two related inquiries: *when* does the duty to preserve attach and *what* evidence must be preserved?”

Zubulake v. UBS Warburg LLC,
220 F.R.D 212 (S.D.N.Y. 2003)
(Zubulake IV)

HYPOTHETICAL

- During discovery HSTV only produced 12 of the alleged 25 e-mails sent by Mr. Joker to Ms. Quinn in January through February, 2016. Ms. Quinn is now requesting that the backup tapes be restored to search for the remaining emails. As for HSTV's backup system, the e-mail servers were backed up onto backup. According to HSTV's IT Director, each server was backed up as a unit; the e-mail of a particular employee could not be restored individually. Accordingly, if one individual's e-mail had to be recovered, the entire server would have to be restored. Such a restoration could take from two to five days. HSTV estimates that it would cost in excess of \$10,000 to restore one backup tape and that there are 4 backup tapes that would need to be restored. Ms. Quinn requests that HSTV be compelled to restore the 4 backup tapes.

RULE 26

Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding **any nonprivileged matter** that is **relevant to any party's claim or defense** and **proportional to the needs of the case**, considering the importance of the:

- (1) issues at stake in the action,
- (2) the amount in controversy,
- (3) the parties' relative access to relevant information,
- (4) the parties' resources,
- (5) the importance of the discovery in resolving the issues, and
- (6) whether the burden or expense of the proposed discovery outweighs its likely benefit.

NOT REASONABLY ACCESSIBLE DATA

- A party asserting that ESI is “not reasonably accessible,” and thus not subject to discovery under Rule 26(b)(2)(B) absent a showing of good cause, has the burden of proving the undue burdens and costs of accessing it
- May likely require additional discovery
- Presumptive data (unallocated data, RAM, cache)

GOOD CAUSE TO OBTAIN NOT REASONABLY ACCESSIBLE ESI

- (1) the specificity of the discovery request;
- (2) the quantity of information available from other and more easily accessed sources;
- (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
- (5) predictions as to the importance and usefulness of the further information;
- (6) the importance of the issues at stake in the litigation; and
- (7) the parties’ resources.

- See Rule 26(b)(2)(B) advisory committee note

COST SHIFTING

- SEDONA SAYS THE COSTS OF RETRIEVING ***AND REVIEWING*** THE INFORMATION SHOULD BE SHIFTED. SEDONA PRINCIPLE 13 AND COMMENTARY 13(a)
- BUT CASES GENERALLY SHIFT ONLY THE COST OF RETRIEVAL, NOT COST OF REVIEW (*see e.g., ZUBULAKE, ROWE*).

7-FACTOR TEST FROM *ZUBULAKE v. UBS WARBURG LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) AND 216 F.R.D. 280 (S.D.N.Y. 2003) (J. SCHEINDLIN)

- "1. THE EXTENT TO WHICH THE REQUEST IS SPECIFICALLY TAILORED TO DISCOVER RELEVANT INFORMATION;
- 2. THE AVAILABILITY OF SUCH INFORMATION FROM OTHER SOURCES;
- 3. THE TOTAL COST OF PRODUCTION, COMPARED TO THE AMOUNT IN CONTROVERSY;
- 4. THE TOTAL COST OF PRODUCTION, COMPARED TO THE RESOURCES AVAILABLE TO EACH PARTY;
- 5. THE RELATIVE ABILITY OF EACH PARTY TO CONTROL COSTS AND ITS INCENTIVE TO DO SO;
- 6. THE IMPORTANCE OF THE ISSUES AT STAKE IN THE LITIGATION; AND
- 7. THE RELATIVE BENEFITS TO THE PARTIES OF OBTAINING THE INFORMATION."
- UNDER THIS TEST, AFTER REVIEWING A SAMPLE OF E-MAILS FOR 5 DATES, ASSESSED PLAINTIFF 25% OF COST OF RESTORING 77 BACKUP TAPES; BUT MADE DEFENDANT PAY FULL COST OF RESTORING OTHER BACKUPS ON SEARCHABLE OPTICAL MEDIA.

FORM OF PRODUCTION DISPUTES

- DOES THE E-INFORMATION HAVE TO BE PRODUCED IN A SEARCHABLE FORMAT?
- DOES THE E-INFORMATION HAVE TO BE PRODUCED IN MULTIPLE FORMATS?

RULE 34

- THE REQUEST MAY SPECIFY THE FORM IN WHICH ELECTRONICALLY STORED INFORMATION IS TO BE PRODUCED
- THE RESPONDING PARTY MAY OBJECT TO THE FORM REQUESTED
- IF THE REQUESTING PARTY DOES NOT SPECIFY THE FORM OF PRODUCTION, ABSENT AGREEMENT OR COURT ORDER THE RESPONDENT **MUST** PRODUCE E-INFORMATION IN A FORM IN WHICH IT IS ORDINARILY MAINTAINED, OR IN A REASONABLY USABLE FORM

AVOID THE PROBLEMS AND CONFRONT E-DISCOVERY ISSUES EARLY



- CONFRONTING E-DISCOVERY ISSUES EARLY SHOULD INCLUDE, FOR EXAMPLE, THE PARTIES EXCHANGING INFORMATION ABOUT THEIR COMPUTER SYSTEMS, IDENTIFYING E-DISCOVERY TECHNICAL POINT PERSONS, AND DISCUSSING THE TYPES OF E-DATA THAT WILL BE SEARCHED AND PRODUCED AND IN WHAT FORMAT

PARTIES DISCOVERY PLAN



- **RULE 26(f)(3):** THE PARTIES ARE TO DISCUSS ANY ISSUES RELATING TO DISCLOSURE, DISCOVERY, OR PRESERVATION OF ELECTRONICALLY STORED INFORMATION, INCLUDING THE FORM OR FORMS IN WHICH IT SHOULD BE PRODUCED, AND
- ANY ISSUES RELATING TO CLAIMS OF PRIVILEGE OR PROTECTION OF TRIAL-PREPARATION MATERIAL INCLUDING – IF THE PARTIES AGREE ON A PROCEDURE TO ASSERT SUCH CLAIMS AFTER PRODUCTION – WHETHER TO ASK THE COURT TO INCLUDE THEIR AGREEMENT IN A RULE 502 ORDER

26(f) CONSIDERATIONS

- whether there will be discovery of ESI at all;
- disclosures required under Federal Rule of Civil Procedure 26(a)(1), if any, and their timing;
- what types or categories of discoverable information each party has in electronic form, and where and on what type of media that information is likely to be found;
- the steps each party will take to preserve different types or categories of ESI;
- the number and identity of “key players” who are knowledgeable about potentially relevant ESI and on whose servers or devices ESI is likely to be found;
- what methods will be efficient in identifying discoverable ESI (e.g., sampling, key word searches);
- the anticipated schedule for production;
- the form in which such information is ordinarily maintained and whether it will be produced in that form—usually known as “native format”—or in another form;
- the scope of discovery of different categories of ESI, such as e-mail messages;
- whether relevant information has been deleted, and if so, whether one or more parties believe deleted information needs to be restored and who will bear the cost of restoring it;
- whether any information is not “reasonably accessible,” the burdens and costs of retrieving that information, why it is needed, and any conditions that should be placed on its production, including who will bear the cost; and
- whether relevant information is in the possession of nonparties from whom discovery under Rule 45 will be required.

COURT EXPECTATIONS

- having a knowledgeable person describe the party’s information systems, storage, and retention policies and practices to the opposing party and the court;
- interviewing key employees to determine sources of information;
- affirmatively and repeatedly communicating litigation holds to all affected employees and other persons and monitoring compliance on an ongoing basis;
- integrating discovery responsibilities with routine data retention policies and practices;
- actively managing and monitoring document collections; and
- documenting the steps taken to design, implement, and audit the litigation hold

RULE 45 ISSUES

- Rule 45 of the Federal Rules of Civil Procedure conforms the rules on ESI discovery from third parties to those on ESI discovery from parties. Rule 45 introduces the concept of sources that are not reasonably accessible. It addresses the form or forms for the production of ESI, adds a post-production procedure for asserting claims of privilege or of protection as trial-preparation materials, and allows for the testing or sampling of ESI
- Although Rule 45 has no equivalent to the Rule 26(f) conference process, parties seeking discovery from nonparties under Rule 45 should be encouraged to meet informally with nonparty respondents and to discuss the scope of the subpoena, the form in which ESI will be produced, protection against waiver for privileged and protected information, and the allocation of discovery costs

THE PROBLEMS WITH PRIVILEGE CLAIMS AND THE POTENTIAL SOLUTION OF RULE 502

2016 WL 3917513

Only the Westlaw citation is currently available.
United States District Court,
M.D. Florida,
Tampa Division.

Thomas Bingham, Plaintiff,

v.

Baycare Health System, Defendant.

Case No: 8:14-cv-73-T-23JSS

Signed 07/20/2016

Attorneys and Law Firms

Anna Christina Weidner-Tafs, Phillip Paul Weidner, Weidner & Associates, APC, Anchorage, AK, Jonathan Kroner, Jonathan Kroner Law Office, Miami Beach, FL, Phillip E. Benson, Warren | Benson Law Group, Minnetonka, MN, for Plaintiff.

J. Logan Murphy, Scott A. McLaren, Hill Ward Henderson, PA, Todd A. Jennings, Galloway, Johnson, Tompkins, Burr & Smith, PLC, Tampa, FL, Kelly J. Davidson, S. Craig Holden, Stewart W. Kameen, Ober, Kaler, Grimes & Shriver, Baltimore, MD, Brian J. Aungst, Jr., MacFarlane, Ferguson & McMullen, PA, Clearwater, FL, for Defendant.

ORDER ON MOTION FOR DETERMINATION OF PRIVILEGE

JULIE S. SNEED, UNITED STATES MAGISTRATE JUDGE

*1 THIS MATTER is before the Court on Defendant's Motion for a Determination That Certain E-Mail Communications Are Not Privileged or Otherwise Protected from Discovery ("Motion"). (Dkt. 94.) Defendant seeks a determination that certain e-mails exchanged between Plaintiff and his attorneys and thereafter forwarded by Plaintiff to his work e-mail account are not protected from discovery by the attorney-client privilege. The Court held a hearing on this matter on June 30, 2016. For the reasons that follow, Defendant's Motion is granted.

BACKGROUND

On January 29, 2016, Defendant served a subpoena on Plaintiff's employer, Holladay Properties Services Midwest, Inc. ("Holladay"), seeking documents related to the allegations in this lawsuit. In response, Holladay produced the responsive documents, which included e-mails and attachments between Plaintiff and his attorneys that Plaintiff forwarded from his personal e-mail account to his work e-mail account at Holladay. (Dkt. 96 at 2.) Upon receiving Holladay's production, Defendant notified Plaintiff of its receipt of the e-mails, and Plaintiff asserted a claim of privilege as to the e-mails. (Dkt. 94.) Defendant now seeks a determination that the e-mails from Plaintiff's work e-mail account are not confidential and thus not privileged or otherwise protected from discovery.

APPLICABLE STANDARDS

When the court's jurisdiction is premised on a federal question in a civil case, federal law of privilege applies. *Hancock v. Hobbs*, 967 F.2d 462, 467 (11th Cir. 1992); see *Fed. R. Evid. 501* (providing that federal common law governs a claim of privilege unless the United States Constitution, federal statute, or rules prescribed by the Supreme Court provide otherwise). This lawsuit was brought in federal court based on federal question jurisdiction as an action under the False Claims Act, 31 U.S.C. §§ 3729–3733. (Dkt. 32.) Therefore, federal common law applies in analyzing the attorney-client privilege. The attorney-client privilege protects the disclosures that a client makes to his attorney, in confidence, for the purpose of securing legal advice or assistance. *Cox v. Adm'r U.S. Steel & Carnegie*, 17 F.3d 1386, 1414 (11th Cir. 1994).

To determine if a particular communication is confidential and protected by the attorney-client privilege, the privilege holder must prove that the communication was intended to remain confidential and, under the circumstances, was reasonably expected and understood to be confidential. *Bogle v. McClure*, 332 F.3d 1347, 1358 (11th Cir. 2003); see also *United States v. Schaltenbrand*, 930 F.2d 1554, 1562 (11th Cir. 1991) ("The party invoking the attorney-client privilege has the burden of proving that an attorney-client relationship existed and that the particular communications were confidential.").

Thus, the relevant inquiry is not whether the individual expected his or her communications to remain confidential but rather whether that expectation was reasonable. *United States v. Bell*, 776 F.2d 965, 971 (11th Cir. 1985).

ANALYSIS

*2 In this case, the e-mails at issue represent communications between Plaintiff and his attorneys that were exchanged on Plaintiff's personal e-mail account.¹ The e-mails contained a link to a cloud storage account where Plaintiff's attorneys had uploaded documents for Plaintiff's review. Plaintiff then forwarded certain e-mails from his personal e-mail account to his work e-mail account so that he could access the links from work. (Dkt. 94 at 2; Dkt. 96 at 2.) The forwarded e-mails contain discussions between Plaintiff and his attorneys, as well as links to documents. (Dkt. 96 at 2.)

Based on the written submissions of the parties and the arguments advanced at the hearing, the parties agree that the e-mails consist of communications between Plaintiff and his attorneys regarding this lawsuit. The parties dispute only whether the e-mails in question are protected by the attorney-client privilege when they were accessed by Plaintiff on his work e-mail account on Holladay's "communications system," which is described in Holladay's policy as "including e-mail and voice mail systems and Intranet/Internet connections." (Dkt. 94-1.) As such, the Court must determine the confidential nature of the e-mails transmitted over Holladay's communications systems.

A. Application of Attorney-Client Privilege to Workplace E-Mails

Courts addressing this issue have focused primarily on whether the employer maintains a policy regarding the use of its computer or e-mail systems. Specifically, courts consider the specificity of the policy and the extent to which the policy diminishes an employee's reasonable expectation of privacy in communications transmitted over the employer's systems. However, because the overarching consideration in determining whether a communication is privileged is whether the individual had an objectively reasonable expectation that his or her communications were confidential, privilege determinations of this nature are extremely fact-specific and often depend on the particular policy language, if any, adopted by the employer.

Notably, courts have adopted a four-factor test to determine whether a reasonable expectation of privacy exists in the context of e-mail transmitted over and maintained on a company server. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005); see *In re Reserve Fund Sec. & Derivative Litig.*, 275 F.R.D. 154, 159–60 (S.D.N.Y. 2011) (listing cases adopting the four-factor test); *Leor Expl. & Prod. LLC v. Aguiar*, No. 09-60136-CIV, 2009 WL 3097207, at *4 (S.D. Fla. Sept. 23, 2009) (applying the four-factor test). In determining this issue, courts have considered the following four factors: (1) whether the corporation maintains a policy banning personal or other objectionable use; (2) whether the company monitors the use of the employee's computer or e-mail; (3) whether third parties have a right of access to the computer or e-mails; and (4) whether the corporation notifies the employee, or whether the employee was aware, of the use and monitoring policies. See *Asia Global*, 322 B.R. at 257. The four-factor test provides persuasive guidance in evaluating whether an individual's expectation of confidentiality is reasonable in light of the existence of other factors that tend to cast doubt on the reasonableness of that expectation, namely the scope of an employer's policy. See *id.* at 258 ("[T]he question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.").

*3 The determination of whether a communication is confidential is somewhat similar to the search-and-seizure determination under the Fourth Amendment. See *id.* at 256 (comparing the Fourth Amendment analysis to the attorney-client privilege analysis); see also cases cited *infra* note 2. Under the Fourth Amendment analysis, the court considers whether an individual's expectation of privacy is objectively reasonable. See *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (providing that an individual's Fourth Amendment rights are implicated only if the conduct at issue infringes an expectation of privacy "that society is prepared to accept as reasonable"). Similarly, under the attorney-client privilege analysis, the court must consider whether a communication was reasonably expected and understood to be confidential. *Bell*, 776 F.2d at 971. As such, courts addressing the issue of attorney-client privilege refer to Fourth Amendment cases addressing an individual's reasonable expectation of privacy in the context of electronic communications, as the analysis under both standards requires consideration of whether one's expectation of privacy was objectively reasonable.² Courts also seek guidance from cases addressing invasion of privacy claims in the context of the workplace, as those cases also consider an individual's reasonable expectation of privacy.³

*4 In applying the four factors discussed above, courts diverge on the issue of whether there must be evidence of actual monitoring or whether a policy reserving the right to monitor employee communications is sufficient to meet the second factor. For example, some courts weigh the act of enforcement more heavily than the existence of a limiting policy. As such, these courts have required some evidence that the employer in fact monitored the employee's communications. *E.g.*, *Flatworld Interactives v. Apple Inc.*, No. C1201956JSWEDL, 2013 WL 11319071, at *1 (N.D. Cal. Dec. 24, 2013); *In re High-Tech Employee Antitrust Litig.*, No. 11-CV-2509-LHK-PSG, 2013 WL 772668, at *7 (N.D. Cal. Feb. 28, 2013); *United States v. Hatfield*, No. 06-CR-0550 (JS), 2009 WL 3806300, at *9 (E.D.N.Y. Nov. 13, 2009); *Brown-Crisuolo v. Wolfe*, 601 F. Supp. 2d 441, 450 (D. Conn. 2009).

Other courts, however, have been satisfied with the finding that the employer's policy provided a right to access and monitor the employee's use, regardless of whether the policy was consistently enforced. These courts have found it sufficient that the employer's policy reserved the right—or permitted the employer—to monitor the employee's communications, without requiring evidence or a showing of actual monitoring. *E.g.*, *L-3 Commc'ns Corp. v. Jaxon Eng'g & Maint., Inc.*, No. 10-CV-02868-MSK-KMT, 2014 WL 183303, at *6 (D. Colo. Jan. 12, 2014); *United States v. Finazzo*, No. 10-CR-457 RRM RML, 2013 WL 619572, at *9 (E.D.N.Y. Feb. 19, 2013); *Chechele v. Ward*, No. CIV-10-1286-M, 2012 WL 4481439, at *2 (W.D. Okla. Sept. 28, 2012); *Dombrowski v. Governor Mifflin Sch. Dist.*, No. CIV.A. 11-1278, 2012 WL 2501017, at *6 (E.D. Pa. June 29, 2012); *Aventa Learning, Inc. v. K12, Inc.*, 830 F. Supp. 2d 1083, 1109 (W.D. Wash. 2011); *Hanson v. First Nat'l Bank*, No. 5:10-0906, 2011 WL 5201430, at *6 (S.D. W. Va. Oct. 31, 2011); *In re Reserve Fund*, 275 F.R.D. at 164; *In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, on Apr. 20, 2010*, No. MDL 2179, 2011 WL 1193030, at *3 (E.D. La. Mar. 28, 2011); *Alamar Ranch, LLC v. Cty. of Boise*, No. CV-09-004-S-BLW, 2009 WL 3669741, at *4 (D. Idaho Nov. 2, 2009); *Leor Expl.*, 2009 WL 3097207, at *4; *Smith v. United Salt Corp.*, No. 1:08CV00053, 2009 WL 2929343, at *9 (W.D. Va. Sept. 9, 2009); *United States v. Etkin*, No. 07-CR-913(KMK), 2008 WL 482281, at *4 (S.D.N.Y. Feb. 20, 2008); *Sims v. Lakeside Sch.*, No. C06-1412RSM, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007); *Long v. Marubeni Am. Corp.*, No. 05CIV.639 (GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006); *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236 (JLL), 2006 WL 1307882, at *4 (D. N.J.

May 10, 2006); *see also United States v. Hamilton*, 778 F. Supp. 2d 651, 655 (E.D. Va. 2011) (focusing on an employer's policy reserving the right to inspect and monitor employee accounts).

Upon review of the applicable caselaw, it appears that the majority of courts have found that an employee has no reasonable expectation of privacy in workplace e-mails when the employer's policy limits personal use or otherwise restricts employees' use of its system and notifies employees of its policy.⁴ *See Pure Power*, 587 F. Supp. 2d at 559–60 (“Courts have routinely found that employees have no reasonable expectation of privacy in their workplace computers, where the employer has a policy which clearly informs employees that company computers cannot be used for personal e-mail activity, and that they will be monitored.”). Further, the majority of courts have relied on the existence of a workplace policy reserving the right to access and monitor employee communications rather than a showing that employee accounts were routinely monitored. Upon consideration, the Court is persuaded by these authorities and agrees under the circumstances presented in this case, that a policy reserving the right to access and monitor employee accounts is sufficient to support a finding that an employee has no reasonable expectation of confidentiality in e-mails transmitted over an employer's e-mail system.

B. Holladay's Policy on Electronic Access

*5 Under Holladay's Personnel Handbook, employees have access to the company's communications systems, including the e-mail system, to conduct “legitimate company business.” (Dkt. 94-1.) Holladay's policy also allows “de minimus (very limited) personal use,” but it provides that Holladay's communications systems may not be used for the operation of personal business or for personal gain. (Dkt. 94-2.) The policy further provides that the “communications systems, including all correspondence, is company property.” (Dkt. 94-1.) Specifically, the policy states that “all communications composed, sent, received, or stored on Holladay's communications system are, and remain, the property of Holladay” and “are not the private property of any employee, even if the employee has used his or her own personal computer, tablet, cell phone or other personal device.” (Dkt. 94-2.)

In regard to the monitoring of electronic communications, Holladay's policy provides that Holladay “reserves and intends to exercise the right to monitor, review, audit, intercept, access and disclose all electronic and telephone communications created, received or sent over the company's communication system for any purpose.”

(Dkt. 94-1.) The policy explicitly warns that it “creates no expectation of privacy concerning such messages” and that the “confidentiality of any message should not be assumed,” regardless of password protection. (Dkt. 94-1, 94-2.) Indeed, the policy notes that “the use of passwords for security does not guarantee confidentiality,” and “[a]ll e-mail and voicemail passwords for access to information on Holladay’s communications system must be disclosed to Holladay.” (Dkt. 94-2.)

C. Application of Attorney-Client Privilege to Plaintiff’s E-Mails

Upon consideration of the applicable facts and caselaw, the Court finds that the factors weigh in favor of a finding that Plaintiff did not have a reasonable expectation of confidentiality in his workplace e-mails. First, it is clear that Holladay maintained a policy that allowed employees to have “very limited personal use” of Holladay’s communications systems and explicitly banned certain personal use. Second, Holladay reserved the right to monitor employees’ computer and e-mail. Third, Holladay reserved the right to access, read, and disclose any electronic communication sent or received over its communications systems. And fourth, Holladay made its employees, including Plaintiff, aware of its policy. Indeed, Plaintiff admits awareness of the policy, and Plaintiff certified his acknowledgment of and compliance with the policy. (Dkt. 94-3.) This sufficiently establishes his awareness of the policy, including the provision requiring that all e-mail passwords be disclosed to Holladay.

With regard to Holladay’s practice of monitoring employee e-mails, neither party specified whether Holladay regularly monitored its employee’s e-mails or electronically stored information. According to Plaintiff, he was “not aware that anyone at Holladay ever actually accessed [his] Holladay account emails, other than for IT Department operational support and/or maintenance,” and his understanding was that Holladay rarely monitored employee e-mails. (Dkt. 96, Ex. 1 ¶¶ 7–8.) Likewise, Plaintiff argues that although he was aware of Holladay’s policy regarding the potential for monitoring and accessing employees’ emails, “[t]he ‘operational reality’ was that [he] was not aware of Holladay accessing or auditing employee e-mail accounts for purposes unrelated to Holladay’s business needs.” (Dkt. 96 at 9–10.) Plaintiff therefore admits that he was aware that Holladay did in fact monitor and access employee accounts but only for *certain* purposes. This distinction, however, is insufficient to establish that Plaintiff was unaware of Holladay’s policy or that Holladay did not enforce its policy.

*6 The explicit language in Holladay’s policy further undermines Plaintiff’s argument, as the policy expressly reserves the right to monitor, access, and disclose all electronic communications received or sent over Holladay’s communications systems for *any purpose*. (Dkt. 94-1.) Under the circumstances, it is clear that Plaintiff was aware that Holladay could access and monitor employee e-mails and that Holladay did in fact access and monitor employee accounts for at least one purpose. See *Goldstein v. Colborne Acquisition Co., LLC*, 873 F. Supp. 2d 932, 938 (N.D. Ill. 2012) (finding that the employees’ “subjective belief that their communications were confidential was not a reasonable one in light of the company policy in place, and in light of their failure to assert that they were unaware of it”).

It is well-settled that the party invoking the attorney-client privilege bears the burden of proving that the particular communications are confidential. See *In re Grand Jury Proceedings in Matter of Freeman*, 708 F.2d 1571, 1575 (11th Cir. 1983) (stating that the party invoking the privilege has the burden of establishing the confidential nature of the communication). In this case, Plaintiff has asserted that the e-mails are privileged, and therefore he bears the burden of proving the confidentiality of the communications. Plaintiff’s subjective belief that Holladay rarely monitored employee e-mails, standing alone, is insufficient to meet his burden. See *Alamar Ranch*, 2009 WL 3669741, at *4 (rejecting the employee’s assertion that she was not aware of any company monitoring and finding the assertion unreasonable).

In support of his assertion that his communications were confidential, Plaintiff refers to a provision in Holladay’s policy that communications should be treated as confidential and accessed only by the intended recipient. (Dkt. 94-1.) This provision, however, only indicates that employees are to regard e-mail communications of other employees as confidential, specifying that “[e]mployees are not authorized to retrieve or read any communications that are not sent to them.” (Dkt. 94-1.) It does not qualify or restrict Holladay’s reservation of the right to access and monitor e-mail communications. See *Hanson*, 2011 WL 5201430, at *6 (analyzing a similar provision and finding that it applied to the receipt of communications by other employees, not the employer).

Plaintiff’s argument relies primarily on his subjective belief that e-mails he accessed on his workplace account were confidential. However, as noted above, the question is not whether he thought or believed his communications were confidential but rather whether his expectation was reasonable under the circumstances. See *Pensacola*

Firefighters' Relief Pension Fund Bd. of Trustees v. Merrill Lynch Pierce Fenner & Smith, Inc., No. 3:09CV53/MCR/MD, 2011 WL 3512180, at *8 (N.D. Fla. July 7, 2011) (emphasizing that the dispositive question is whether, under the circumstances, the individual reasonably believed that his or her communications were confidential despite the existence of a workplace policy and despite the individual's subjective belief that the communications were exchanged in confidence).

In light of the explicit provisions in Holladay's policy and Plaintiff's awareness of these provisions, the Court finds that Plaintiff did not have a reasonable expectation that the handful of e-mails he sent or received over Holladay's communications systems were confidential. Specifically, as noted above, the policy expressly limited personal use of Holladay's communications systems, banned the use of the system for the operation of personal business or personal gain, reserved the right to access and monitor employee use for any purpose, warned employees that they had no expectation of privacy in e-mails transmitted over the company system, and required that employees—including Plaintiff—certify compliance with

its provisions by signing an acknowledgment form. Plaintiff was well aware of Holladay's policy, including the unequivocal notice that his communications were not to be regarded as confidential, and the risk that his e-mail account would be monitored and accessed. As such, Plaintiff has not met his burden of showing that his communications were reasonably expected and understood to be confidential. Accordingly, it is

***7 ORDERED** that Defendant's Motion for a Determination That Certain E-Mail Communications Are Not Privileged or Otherwise Protected from Discovery (Dkt. 94) is **GRANTED**.

DONE and ORDERED in Tampa, Florida, on July 20, 2016. Copies furnished to:

All Citations

Not Reported in F.Supp.3d, 2016 WL 3917513

Footnotes

- 1 At the hearing, Plaintiff stated that there were only a few e-mails produced by Holladay over which the instant dispute arises.
- 2 For a discussion of an employee's reasonable expectation of privacy in the workplace under the Fourth Amendment, see *O'Connor*, 480 U.S. at 714; *United States v. Ziegler*, 456 F.3d 1138, 1146 (9th Cir. 2006); *Biby v. Bd. of Regents, of Univ. of Neb. at Lincoln*, 419 F.3d 845, 850 (8th Cir. 2005); *United States v. Angevine*, 281 F.3d 1130, 1135 (10th Cir. 2002); *United States v. Slanina*, 283 F.3d 670, 676 (5th Cir. 2002); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002); *Leventhal v. Knapke*, 266 F.3d 64, 73 (2d Cir. 2001); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000); *United States v. DiTomasso*, 56 F. Supp. 3d 584, 591 (S.D.N.Y. 2014); *United States v. Yudong Zhu*, 23 F. Supp. 3d 234, 238 (S.D.N.Y. 2014); *United States v. Linder*, No. 12 CR 22-1, 2012 WL 3264924, at *8 (N.D. Ill. Aug. 9, 2012); *United States v. Busby*, No. CR 11-00188 SBA, 2011 WL 6303367, at *4 (N.D. Cal. Dec. 16, 2011); *Keck v. Virginia*, No. 3:10-CV-555, 2011 WL 4589997, at *12 (E.D. Va. Sept. 9, 2011); *United States v. Elmquist*, No. 07-00245-01-CR-W-ODS, 2008 WL 3895971, at *10 (W.D. Mo. Aug. 18, 2008) (following the reasoning of *United States v. Thorn*, 375 F.3d 679 (8th Cir. 2004)); *United States v. Mosby*, No. CRIM. A. 3:08-CR-127, 2008 WL 2961316, at *5 (E.D. Va. July 25, 2008); *United States v. Hassoun*, No. 04 60001 CR BROWN, 2007 WL 141151, at *1 (S.D. Fla. Jan. 17, 2007); *Haynes v. Attorney Gen. of Kan.*, No. 03-4209-RDR, 2005 WL 2704956, at *4 (D. Kan. Aug. 26, 2005); *United States v. Scrushy*, No. CR-03-BE-0530-S, 2005 WL 4149004, at *5 (N.D. Ala. Jan. 21, 2005); *United States v. Bailey*, 272 F. Supp. 2d 822, 835 (D. Neb. 2003); *United States v. Sims*, No. CR 00-193 MV, 2001 WL 36498440, at *7 (D. N.M. Apr. 19, 2001); *Wasson v. Sonoma Cty. Jr. Coll. Dist.*, 4 F. Supp. 2d 893, 905 (N.D. Cal. 1997); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1234 (D. Nev. 1996). In this context, the majority of courts have found that employees do not have a reasonable expectation of privacy in their work computers or in e-mails exchanged using a work account, especially when the employer retains a policy or otherwise notifies employees that their equipment or accounts are subject to monitoring.
- 3 For a discussion of an employee's reasonable expectation of privacy in materials transmitted over an employer's computer system under a claim for invasion of privacy, see *Metzler v. XPO Logistics, Inc.*, No. 4:13-CV-278, 2014 WL 4792984, at *6 (E.D. Tex. Sept. 25, 2014); *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 761 (N.D. Ohio 2013); *Mintz v. Mark Bartelstein & Assocs., Inc.*, 885 F. Supp. 2d 987, 997 (C.D. Cal. 2012); *Gauntlett v. Ill. Union Ins. Co.*, No. 5:CV 11-00455-EJD, 2011 WL 5191808, at *9 (N.D. Cal. Nov. 1, 2011); *Yarborough v. King*, No. CA 2:11-2602-MBS-BHH, 2011 WL 5238920, at *5 n.5 (D. S.C. Oct. 3, 2011); *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 633 (C.D. Ill. 2010); *Miller v. Blattner*, 676 F. Supp. 2d 485, 497 (E.D. La. 2009); *Sporer v. UAL Corp.*, No. C 08-02835 JSW, 2009 WL 2761329, at *5 (N.D. Cal. Aug. 27, 2009); *Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746, at *18 (D. Or. Sept.

15, 2004); *Kelleher v. City of Reading*, No. CIV.A.01-3386, 2002 WL 1067442, at *7 (E.D. Pa. May 29, 2002); *Garrity v. John Hancock Mut. Life Ins. Co.*, No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1 (D. Mass. May 7, 2002); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100 (E.D. Pa. 1996). The majority of these cases have concluded that an employee has no reasonable expectation of privacy in computer files, e-mails, or electronic data maintained at his or her workplace.

- 4 The specific facts of this case establish that Holladay maintained a formal policy that limited personal use. As such, in considering the applicable caselaw, cases in which the employer did not maintain a policy regarding electronic communications or did not otherwise ban or limit personal use are distinguishable from the present case. *E.g.*, *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 897, 904 (9th Cir. 2008); *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007); *United States v. Hudson*, No. CRIM.A. 13-20063-01, 2013 WL 4768084, at *9 (D. Kan. Sept. 5, 2013); *Maxtena, Inc. v. Marks*, No. CIV.A. DKC 11-0945, 2013 WL 1316386, at *5 (D. Md. Mar. 26, 2013); *United States v. Nagle*, No. 1:09-CR-384, 2010 WL 3896200, at *4 (M.D. Pa. Sept. 30, 2010); *Convertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97, 110 (D. D.C. 2009); *Sprenger v. Rector & Bd. of Visitors of Virginia Tech*, No. CIV.A. 7:07CV502, 2008 WL 2465236, at *4 (W.D. Va. June 17, 2008); *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1203 (S.D. Cal. 2008); *see also Orbit One Commc'ns, Inc. v. Numerex Corp.*, 255 F.R.D. 98, 108 n.11 (S.D.N.Y. 2008) (noting the limited right of disclosure in company policy); *Mason v. ILS Techs., LLC*, No. CIVA304CV-139RJC-DCK, 2008 WL 731557, at *4 (W.D.N.C. Feb. 29, 2008) (declining to find waiver of privilege when no evidence established that the employee was aware of the employer's policy and no one alleged that he agreed to abide by it). Similarly, because this case involves the use of a work computer and e-mails sent and retrieved on a work e-mail account, cases addressing an employee's use of a personal computer or use of personal or web-based e-mail accounts are distinguishable. *E.g.*, *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007) (commercial Internet service provider); *Hoofnagle v. Smyth-Wythe Airport Comm'n*, No. 1:15CV00008, 2016 WL 3014702, at *8 (W.D. Va. May 24, 2016) (personal e-mail account and no policy limiting personal use); *Billups v. Penn State Milton S. Hershey Med. Ctr.*, No. 1-11-CV-01784, 2015 WL 7871029, at *3 n.2 (M.D. Pa. Dec. 3, 2015) (no ban on personal use and limited right to access); *Wellin v. Wellin*, No. 2:13-CV-1831-DCN, 2015 WL 5785709, at *26 (D. S.C. July 31, 2015) (personal e-mail account); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 559 (S.D.N.Y. 2008) (personal e-mail from a third party e-mail provider); *Sims*, 2007 WL 2745367, at *2 (web-based e-mail); *Geer v. Gilman Corp.*, No. 306 CV 889 JBA, 2007 WL 1423752, at *3 (D. Conn. Feb. 12, 2007) (employee's use of e-mail and computer of her fiancé); *Curto v. Med. World Commc'ns, Inc.*, No. 03CV6327 DRH MLO, 2006 WL 1318387, at *5 (E.D.N.Y. May 15, 2006) (home office); *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 927 (W.D. Wis. 2002) (web-based e-mail account).

2016 WL 3574587

Only the Westlaw citation is currently available.
 United States District Court,
 M.D. Florida,
 Tampa Division.

Centennial Bank, Plaintiff,
 v.
 Servisfirst Bank Inc. and Gregory W. Bryant,
 Defendants.

Case No: 8:16-cv-88-T-36JSS

Signed 07/01/2016

Attorneys and Law Firms

Andrew James Ghekas, John A. Anthony, Stephenie Biernacki Anthony, Anthony & Partners, LLC, Eduardo A. Suarez, The Suarez Law Firm, P.A., Tampa, FL, for Plaintiff.

Michael Sansbury, William Thomas Paulk, Spotswood Sansom & Sansbury, LLC, Birmingham, AL, Sean P. Keefe, James, Hoyer, Newcomer & Smiljanich, PA, Burton Webb Wiand, Gianluca Morello, Jared J. Perez, Wiand Guerra King, PL, Tampa, FL, for Defendants.

ORDER

JULIE S. SNEED, UNITED STATES MAGISTRATE JUDGE

*1 THIS MATTER is before the Court on Plaintiff Centennial Bank's Motion to Compel Complete Responses to Subpoenas to Produce Documents Served on ServisFirst Employees ("Non-Party Motion") (Dkt. 88) and Plaintiff Centennial Bank's Motion to Compel Bryant to Provide Better Responses to Centennial Bank's First Request for Production ("Bryant Motion") (Dkt. 124). On June 28, 2016, a hearing was held on the Non-Party Motion and the Bryant Motion. Upon consideration of the parties' oral arguments on the Non-Party Motion and the Bryant Motion at the hearing and for the reasons stated on the record at the hearing, the Non-Party Motion is granted and the Bryant Motion is denied.

BACKGROUND**A. Overview**

This case concerns alleged violations of the non-compete provisions in the employment contracts of several of Plaintiff Centennial Bank's ("Centennial") former employees. Centennial acquired Bay Cities Bank ("Bay Cities") in October 2015. (Dkt. 53 at ¶ 7(b).) In connection with the acquisition, Centennial retained several former Bay Cities employees to aid in the integration of its Tampa Bay area branches, specifically Defendant Gregory W. Bryant, the former CEO of Bay Cities, Patrick Murrin, former Chief Risk Manager and Executive Vice President of Bay Cities, and Gwynn Davey, Bay Cities' former Market President of Hillsborough County. (*Id.* at ¶¶ 13, 26–27.) Mr. Bryant, Mr. Murrin, and Ms. Davey signed employment contracts with Centennial that included provisions governing the maintenance of Centennial's confidential information; noncompetition; non-solicitation of Centennial's customers; and non-solicitation of Centennial's employees. (*Id.* at ¶¶ 24–25; Ex. 6–8.)

On December 31, 2015, after Centennial's acquisition of Bay Cities, Mr. Bryant, Mr. Murrin, and Ms. Davey simultaneously resigned from Centennial and, in January 2016, began working for Defendant ServisFirst Bank ("ServisFirst"). (*Id.* at ¶¶ 42–44, 49, 53.) Shortly thereafter, on January 14, 2016, Centennial filed suit against ServisFirst and Mr. Bryant (collectively, "Defendants"). (Dkt. 1.)

B. Non-Party Motion

In the Non-Party Motion, Centennial seeks to compel Ms. Davey and Mr. Murrin (together, "Non-Parties") to produce documents responsive to its subpoenas. (Dkt. 88 at ¶ 7.) The information Centennial seeks from the Non-Parties are: (1) Centennial's confidential information that the Non-Parties allegedly forwarded to their personal email accounts while still employed by Centennial, which Centennial contends is contained in the Non-Parties' personal email accounts, and (2) indemnification agreements between the Non-Parties and ServisFirst, executed on December 31, 2015.

With regard to the confidential information Centennial contends is in the Non-Parties' personal email accounts, Centennial seeks an order compelling the Non-Parties to produce the hard drives of their personal devices for

inspection and mirror imaging. (*Id.* at 18–21.) This measure is warranted, Centennial argued, because there is a question of whether the Non-Parties deleted their personal emails at the end of 2015 and, therefore, the information it seeks from the Non-Parties may not be otherwise obtainable. (*Id.* at 13, 20–21) (“[Counsel for the Non-Parties] communicated that Davey had committed ‘e-mail bankruptcy’ and deleted all of her personal e-mails at the end of 2015 and that Murrin followed a similar procedure.”).

*2 As further articulated at the June 28, 2016 hearing, Centennial requests that a data specialist be permitted to access the devices the Non-Parties used to access their personal email accounts and mirror image the hard drives, which would remain in the specialist’s custody pending resolution of the Non-Party Motion. Also, Centennial requests that the specialist be permitted to access the Non-Parties’ personal email accounts in order to determine which devices accessed the email accounts and whether emails were deleted or captured in the accounts’ archives. At the hearing, the parties conferred as to the procedure for mirror imaging the Non-Parties’ hard drives and reached a tentative agreement in that regard.

As to the indemnification agreements, at the hearing, Centennial argued that the agreements do not constitute work product because they were not created in anticipation of litigation, as demonstrated by the timeline of events leading up to the execution of the agreements. Specifically, on December 11, 2015, ServisFirst offered Mr. Bryant and the Non-Parties positions with ServisFirst. On December 31, 2015, the Non-Parties and Mr. Bryant gave their notice to Centennial and executed the indemnification agreements on the same day. Finally, on January 11, 2016, Centennial sent cease and desist letters to Defendants and the Non-Parties, and on January 14, 2016, Centennial filed suit. Thus, Centennial argues, the Non-Parties could not have anticipated litigation when the indemnification agreements were executed because no demand had been made or suit filed.

At the hearing, the Non-Parties contended that they have produced all responsive documents, with the exception of the indemnification agreements, but that, to the extent emails were deleted and are recoverable, those emails have not been produced. They also objected to Centennial’s request to mirror image the hard drives of their devices because the request is overly broad and unduly burdensome. (Dkt. 121 at 3–8.) The Non-Parties argued that the indemnification agreements are protected from production by the work product doctrine because the language of the agreements themselves show that they were prepared in anticipation of litigation such as the

present case. (*Id.* at 8.)

C. Bryant Motion

Centennial moves to compel responses to requests for production it served on Mr. Bryant. As narrowed at the hearing, Centennial seeks (1) the indemnity agreement between ServisFirst and Mr. Bryant and (2) emails from Mr. Bryant’s personal email account that he has yet to produce, should such emails exist. Generally, Centennial argued, Mr. Bryant’s objections to the requests for production are insufficiently specific and should be overruled. (Dkt. 124 at 6–8.) Further, Mr. Bryant waived any assertions of attorney-client privilege or work product, Centennial argued, because he served his privilege log about a week after he produced responsive documents. (*Id.* at 11.)

In response, Mr. Bryant argued that the indemnification agreements are protected from discovery by the work product doctrine because the agreements themselves state that they were created in anticipation of the present litigation. (Dkt. 139 at 9–10.) Further, he did not waive this protection, Mr. Bryant argued, because no federal rule requires service of a privilege log simultaneously with the responses to production requests and, here, his log was served only six business days after his production of responsive documents. (Dkt. 139 at 4–6.) Finally, at the hearing, counsel for Mr. Bryant stated that Mr. Bryant has produced his emails to Centennial, and, to the extent he withholds responsive documents on the basis of his objections, he identified such documents on his privilege log and specifically stated so in his objections.

*3 Finally, at the hearing, counsel for Mr. Bryant offered to submit his indemnification agreement with ServisFirst for the Court’s *in camera* review. Counsel for the Non-Parties likewise agreed to submit the Non-Parties’ indemnification agreements with ServisFirst. Following the hearing, the indemnification agreements were submitted for *in camera* review.

APPLICABLE STANDARDS

A party, “[o]n notice to other parties and all affected persons,” may move to compel discovery. *Fed. R. Civ. P.* 37(a)(1). “[A]n evasive or incomplete disclosure, answer, or response must be treated as a failure to disclose, answer, or respond.” *Id.* at 37(a)(4). Courts maintain great discretion to regulate discovery. *Patterson v. U.S. Postal Serv.*, 901 F.2d 927, 929 (11th Cir. 1990). The court has

broad discretion to compel or deny discovery. *Josendis v. Wall to Wall Residence Repairs, Inc.*, 662 F.3d 1292, 1306 (11th Cir. 2011).

Through discovery, parties may obtain materials that are within the scope of discovery, meaning they are nonprivileged, relevant to any party's claim or defense, and "proportional to the needs of the case." *Fed. R. Civ. P. 26(b)(1)*. The term "relevant" is "construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978). Courts consider the following factors when evaluating whether requested discovery is proportional to the needs of the case: (1) "the importance of the issues at stake in the action," (2) "the amount in controversy," (3) "the parties' relative access to relevant information," (4) "the parties' resources," (5) "the importance of the discovery in resolving the issues," and (6) "whether the burden or expense of the proposed discovery outweighs its likely benefit." *Fed. R. Civ. P. 26(b)(1)*.

Parties responsible for issuing subpoenas "must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena," and the Court must enforce this duty. *Id.* at 45(d)(1). An order compelling production "must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance." *Id.* at 45(d)(2)(B)(ii). In response to a subpoena, a subpoenaed person may serve objections to the subpoena and, if a person withholds information under a claim of privilege or work product protection, the person must "expressly make the claim" and "describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim." *Id.* at 45(d)(2)(B) and (e)(2).

Under the work product doctrine, documents and other "tangible things" are not discoverable by a party when they were "prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)." *Id.* at 26(b)(3)(A). These protected materials may be discovered, however, if "they are otherwise discoverable under *Rule 26(b)(1)*" and the party seeking production "shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means." *Id.*

*4 As to the production of electronically-stored

information, "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." *Id.* at 26(b)(2)(B). When a motion to compel has been filed, the resisting party "must show that the information is not reasonably accessible because of undue burden or cost," and, if such showing is made, "the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of *Rule 26(b)(2)(C)*." *Id.*

ANALYSIS

A. Non-Party Motion

As stated on the record at the hearing, the Non-Party Motion is granted and the Non-Parties shall produce e-discovery responsive to Centennial's requests because the requests are relevant to Centennial's claims in this case. *See Fed. R. Civ. P. 26(b)(1)*. Specifically, Centennial's information that the Non-Parties forwarded to their personal email accounts while they were still employed by Centennial is relevant to Centennial's allegations of Defendants' wrongdoing. (Dkt. 53 at ¶ 73.)

As to the indemnification agreements between the Non-Parties and ServisFirst, the indemnification agreements are relevant and therefore discoverable because ServisFirst's agreement to indemnify the Non-Parties and Mr. Bryant in the event of litigation such as the present litigation is relevant to Centennial's claims regarding ServisFirst's interference with the Non-Parties' and Mr. Bryant's employment agreements. *See Fed. R. Civ. P. 26(b)(1)*. Because the Non-Parties oppose production, it is their burden to establish that the work product doctrine protects the indemnification agreements from discovery. *Republic of Ecuador v. Hincsee*, 741 F.3d 1185, 1189 (11th Cir. 2013).

The work product doctrine protects from production documents and other "tangible things" that were "prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)." *Fed. R. Civ. P. 26(b)(3)(A)*. The Eleventh Circuit, in *Tambourine Comercio Internacional SA v. Solowsky*, held that "[b]y its plain text, *Rule 26(b)(3)* applies to documents or things prepared by or for another party or its representative" and held that the work product protection does not apply to documents prepared for those who are not parties to the case "even though the person may be a party to a closely related lawsuit in which he

will be disadvantaged if he must disclose in the present suit.” 312 Fed.Appx. 263, 284 (11th Cir. 2009) (internal citations omitted). The Eleventh Circuit’s holding in *Tambourine* has been interpreted to mean that “[a] non-party is not entitled to claim work product protection.” *Bozeman v. Chartis Cas. Co.*, No. 2:10-CV-102-FTM-36, 2010 WL 4386826, at *2 (M.D. Fla. Oct. 29, 2010) (citing *Tambourine*, 312 Fed.Appx. 263).

Here, the Non-Parties are not parties to the present litigation. As such, they cannot claim the protections of the work product doctrine and therefore must produce the indemnification agreements. However, the Court notes that, since the hearing, ServisFirst has filed a motion to quash Centennial’s subpoenas to the Non-Parties to the extent they seek the indemnification agreements. (See Dkts. 160–161.) At the time of entry of this Order, ServisFirst’s motion to quash remains pending. Accordingly, the Court finds it appropriate to stay the Non-Parties’ production of the indemnification agreements pending the disposition of ServisFirst’s motion to quash.

B. Bryant Motion

*5 The Court rejects Centennial’s contention that Mr. Bryant’s objections to Centennial’s request for production are not sufficiently specific because, after review of his objections (Dkt. 124 at Ex. B), the Court finds that Mr. Bryant adequately stated the basis for his objections and the objections are well taken. The Court further rejects Centennial’s argument that Mr. Bryant has waived any attorney-client privilege or work product protections because Centennial cites no binding authority that a privilege log must be produced simultaneously with a party’s responses and, in any event, Mr. Bryant served his privilege log shortly after providing responsive documents. *Universal City Dev. Partners, Ltd. v. Ride & Show Eng’g, Inc.*, 230 F.R.D. 688, 696 (M.D. Fla. 2005) (“The Eleventh Circuit has never determined what constitutes a timely production of a privilege log in response to a request for production of documents.”). Further, Centennial suffered no prejudice due to the short delay.

Footnotes

- ¹ The indemnification agreement between ServisFirst and non-parties Mr. Murrin and Ms. Davey were virtually identical to the indemnification agreement between ServisFirst and Mr. Bryant. Having conducted an *in camera* review of the three agreements, they all appear to have been prepared in anticipation of litigation such as the present litigation.

As to Centennial’s request to compel production of the indemnification between ServisFirst and Mr. Bryant, the Court denies the request because it is protected from discovery under the work product doctrine. Specifically, Mr. Bryant, as a party, may assert the work product protection and, after the Court’s *in camera* inspection of the indemnification agreement, the agreement, on its face, states that it was prepared in anticipation of litigation such as the present litigation.¹ See Fed. R. Civ. P. 26(b)(3)(A). Further, Centennial has not shown that the agreement is “otherwise discoverable under Rule 26(b)(1)” or that it has a “substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.” See Fed. R. Civ. P. 26(b)(3).

Accordingly, it is

1. Plaintiff Centennial Bank’s Motion to Compel Complete Responses to Subpoenas to Produce Documents Served on ServisFirst Employees (“Non-Party Motion”) (Dkt. 88) is **GRANTED**; however, the Non-Parties’ obligation to produce the indemnification agreements is stayed pending the disposition of ServisFirst’s motion to quash. (See Dkts. 160–161.)

2. The Non-Parties shall serve e-discovery responsive to Centennial’s subpoenas within sixty (60) days of entry of this Order.

3. Plaintiff Centennial Bank’s Motion to Compel Bryant to Provide Better Responses to Centennial Bank’s First Request for Production (“Bryant Motion”) (Dkt. 124) is **DENIED**.

DONE and ORDERED in Tampa, Florida on July 1, 2016.

All Citations

Not Reported in F.Supp.3d, 2016 WL 3574587

Sample Orders Related to ESI Discovery

1. Order (Agreed) Regarding Appointment of Neutral Forensic Expert and ESI Protocols

- a. *Centennial Bank v. Servisfirst Bank Inc.*, 8:16-cv-88-T-36JSS (M.D. Fla. Sept. 26, 2016)
- b. Order delineates procedures for an designated computer forensics consultant to produce mirror images of mobile devices, computers and portable hard drives and provide the results for review for privilege and responsiveness.

2. Document Production Protocol and Cost of Production Order

- a. *In re: Darvocet, Darvon and Propoxyphene Products Liability Litigation*, 2:11-md-02226-DCR, MDL No. 2226,, Doc. 2290 (E.D. Ky. Oct. 11, 2012)
- b. Order provides for procedures regarding the production of documents, including ESI; timing, format and cost of production; and matters related to privilege.

3. Order Regarding the Preservation of Documents, Electronically Stored Information, and Tangible Things Within the United States

- a. *In re: Darvocet, Darvon and Propoxyphene Products Liability Litigation*, 2:11-md-02226-DCR, MDL No. 2226,, Doc. 387 (E.D. Ky. Nov. 16, 2011)
- b. Order provides for procedures and protocols regarding preservation of documents, ESI, and tangible things, including describing acceptable methods of preservation.

4. Stipulated Order Regarding Discovery Procedure

- a. *Advanced Telecomm. Network, Inc. v. Flaster Greenburg , P.C. (In re Advanced Telecomm. Network, Inc.)*, Adv. Proc. 6:05-ap-00006-KSJ, 6:05-ap-00008-KSJ, No. 6:03-bk-00299-KSJ, Doc. 152 (Bankr. M.D. Fla. Aug. 18, 2015).
- b. Order provides for procedures regarding claims of privilege in produced ESI.

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

CENTENNIAL BANK,

Plaintiff,

v.

Case No: 8:16-cv-88-T-36JSS

SERVISFIRST BANK INC., and
GREGORY W. BRYANT,

Defendants.

ORDER

THIS MATTER is before the Court on the Motion for Appointment of Neutral Forensic Expert and Confirmation of Proposed ESI Protocol (the “Appointment Motion”) (Dkt. 171), filed by Plaintiff Centennial Bank (“Centennial”), and the response in opposition to the Appointment Motion filed by non-parties Gwynn Davey and Patrick Murrin (Dkt. 174) (together, the “ServisFirst Employees,” and, collectively with Centennial, the “Parties”), and the Joint Motion and Stipulation for Entry of Agreed Order (the “Joint Motion”) (Dkt. 190), filed jointly by the Parties.

On July 26, 2016, Centennial filed the Appointment Motion (Dkt. 171), requesting that the Court enter an order appointing a neutral computer forensic expert to conduct mirror imaging, preservation, and retrieval of electronic evidence within the mobile and computer devices of the ServisFirst Employees. On August 12, 2016, the ServisFirst Employees filed a response in opposition to the Appointment Motion (the “Appointment Response”). (Dkt. 174.)

On September 15, 2016, the Court held a hearing on the Appointment Motion. (Dkts. 186, 188.) At the hearing, the Parties disagreed regarding what data and information is necessarily recoverable from mobile devices and other computer equipment.

The Court then noticed the Appointment Motion for evidentiary hearing to occur on September 26, 2016. (Dkt. 187.) The Court instructed the parties to “meet and confer prior to the evidentiary hearing regarding the issues of electronic discovery raised in the motion and at the hearing held before the Court on September 15, 2016.” (Dkt. 187.)

On September 23, 2016, the Court was contacted by counsel for the Parties and informed that the Parties had reached an agreement regarding the issues of electronic discovery raised in the Appointment Motion, which agreement the Parties memorialized in the Joint Motion and the agreed order attached thereto. (Dkts. 190, 190-1.)

Upon consideration of the Appointment Motion, the Appointment Response, the Joint Motion, and the Parties’ proposed agreed order resolving the Appointment Motion, it is

ORDERED:

1. The Joint Motion and Stipulation for Entry of Agreed Order (Dkt. 190) is **GRANTED**.

2. In light of the Parties’ agreement regarding the resolution of Centennial’s Motion for Appointment of Neutral Forensic Expert and Confirmation of Proposed ESI Protocol (Dkt. 171), as set forth in the Joint Motion and the agreed proposed order attached thereto (Dkts. 190, 190-1), Centennial’s Motion for Appointment of Neutral Forensic Expert and Confirmation of Proposed ESI Protocol (Dkt. 171) is **GRANTED** to the extent set forth hereinafter:

A. Dwayne Denny, a computer forensics consultant chosen by Centennial, will produce mirror images of all mobile devices, computers and portable or detachable hard drives in the ServisFirst Employees’ personal possession, custody, or control and used by the ServisFirst Employees since January 1, 2015, as well as the ServisFirst Employees’

respective Gmail and iCloud accounts. Mr. Denny will execute a confidentiality agreement agreed to by the Parties.

B. Within ten (10) days of entry of this Order, the ServisFirst Employees will make available to Mr. Denny, at a place of their choosing, and at mutually agreeable times, all of the computer equipment described in the preceding paragraph. Mr. Denny will use his best efforts to avoid unnecessarily disrupting the normal activities or business operations of the ServisFirst Employees while inspecting, copying, and imaging the ServisFirst Employees' mobile devices, computers and other portable or detachable hard drives. The ServisFirst Employees, in the presence of Mr. Denny, will log into their respective Gmail and iCloud accounts, without Mr. Denny observing their passwords, and subsequently provide Mr. Denny with access to the same in their presence. Mr. Denny may not remove the ServisFirst Employees' mobile devices and computer equipment from the ServisFirst Employees' premises, and only Mr. Denny and his employees assigned to this project are authorized to inspect the equipment produced. The ServisFirst Employees may also have their own electronic data recovery expert, Adam Sharp, present to observe the inspection and imaging of their mobile devices, computer equipment, and respective Gmail and iCloud accounts. After the inspection and imaging is complete, Mr. Denny and Mr. Sharp will videotape the packaging of the forensic images in sealed evidence bags. Mr. Sharp will then take custody of the forensic images and is ordered not to open the evidence bags or otherwise interfere with the forensic images contained therein unless in the presence of Mr. Denny or ordered otherwise by the Court.

C. Within ten (10) days of inspection and imaging of the ServisFirst Employees' mobile devices, computer equipment and respective Gmail and iCloud

accounts, Mr. Sharp shall deliver the sealed evidence bags containing the forensic images to Mr. Denny's principal office. Mr. Denny, utilizing the tools and methodology deemed appropriate by him, shall then proceed to recover from the forensic images all available Relevant Records,¹ including but not limited to word-processing documents, incoming and outgoing email messages, PowerPoint or similar presentations, spreadsheets, and other files, including files that were "deleted." Mr. Sharp is permitted to be present and observe the recovery and extraction of Relevant Records from the forensic images but may not otherwise interfere in the data recovery and extraction process. Once the recovery and extraction process is completed, Mr. Denny is to repackage the forensic images and return them to Mr. Sharp.

D. Following the recovery and extraction process, Mr. Denny shall provide the Relevant Records in a reasonably convenient and searchable form to the ServisFirst Employees' counsel, along with, to the extent possible, the information showing when any files were created, accessed, copied, or deleted, and the information about the deletion and the contents of deleted files that could not be recovered. Mr. Denny is not to maintain a copy of any data or documents recovered from the ServisFirst Employees and is not to disclose any of his findings to Centennial or any other third-party. Mr. Denny shall submit an affidavit certifying that he has not retained any copies of any data or documents recovered from the ServisFirst Employees and that he has not disclosed any of his findings

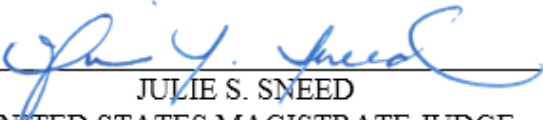
¹ "Relevant Records" are records responsive to search terms established by the Parties or this Court and metadata associated with those records. The Parties are instructed to meet and confer regarding establishing a set of agreed-to search terms to be utilized by Mr. Denny. The Parties shall use best efforts to agree to an initial preliminary set of search terms fourteen (14) days after the date of this Order. If the Parties are unable to agree on an initial set of search terms, after conferring in good faith, any Party may raise the issue with the Court by motion.

to Centennial or any other third-party. Mr. Denny shall also provide Centennial notice of when the Relevant Records were provided to the ServisFirst Employees' counsel.

E. Within twenty (20) days of the receipt of the Relevant Records, the ServisFirst Employees' counsel shall review the records for privilege and responsiveness, supplement the ServisFirst Employees' responses to Centennial's subpoenas, if necessary, and send to Centennial's counsel all previously-unproduced non-privileged responsive documents and information, as well as a privilege log, which claims each privilege expressly and describes "the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection." Fed. R. Civ. P. 26(b)(5)(A). Nothing in this Order shall prevent Centennial from filing a motion to compel if it is unable to resolve a claim of privilege or relevance with the ServisFirst Employees, but the Parties are strongly encouraged to resolve these issues without Court intervention.

F. The Parties are to bear their own costs associated with their respective electronic data recovery experts, and Centennial shall not be allowed such costs pursuant to Rule 54 of the Federal Rules of Civil Procedure.

DONE and ORDERED, in Tampa, Florida, on September 26, 2016.



JULIE S. SNEED
UNITED STATES MAGISTRATE JUDGE

Copies furnished to:
Counsel of Record

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
NORTHERN DIVISION
(at Covington)

IN RE: DARVOCET, DARVON AND
PROPOXYPHENE PRODUCTS
LIABILITY LITIGATION

MDL No. 2226
ALL CASES

**DOCUMENT PRODUCTION
PROTOCOL AND COST
OF PRODUCTION ORDER**

This Document Production Protocol and Cost of Production Order (the “Document Production Protocol”) shall apply to all cases transferred to this Court by the Judicial Panel on Multidistrict Litigation pursuant to its Order of August 16, 2011, any tag-along actions transferred to this Court by the Panel, and any related actions that have been or will be originally filed in, transferred to, or removed to this Court and assigned thereto as part of *In re: Darvocet, Darvon, and Propoxyphene Products Liability Litigation*, MDL No. 2226. This Document Production Protocol is intended to address issues as contemplated in Sections IV(E), (J) and (K) of the May 25, 2012 Order (as defined below), between Plaintiffs and Brand Defendants.

1. **Definitions:**

- a. “March 20, 2012 Protective Order” shall refer to the Stipulation and Protective Order of Confidentiality, entered by this Court on March 20, 2012, as Docket No. 1513.

- b. “May 25, 2012 Order” shall refer to the Procedures Governing Discovery Order entered by this Court on May 25, 2012, as Docket No. 1886.
- c. “Brand Defendants” shall have the same meaning as that term is used in the May 25, 2012 Order.
- d. “Documents” and “Electronically Stored Information (ESI)” shall be defined as they are in Federal Rule of Civil Procedure 34. The definitions of these terms do not include voicemail; instant messages; information on hand-held devices synchronized to other electronic media that store such data; or temporary, transient, residual, or fragmented data.

2. **Requests for Production of Documents.** Plaintiffs may propound one Master Set of Requests for Production, as described in the May 25, 2012 Order, which shall include no more than 50 requests for production of documents, to each Brand Defendant on or before December 1, 2012 (or later as the parties may separately agree). Nothing included herein shall preclude Plaintiffs from seeking leave to file additional Requests for Production as described in the May 25, 2012 Order.

3. **Schedule of Production of Brand Defendants’ Documents.**

- a. Brand Defendants shall produce the documents specifically described in the May 25, 2012 Order, pursuant to the deadlines set forth therein.
- b. Thereafter, Brand Defendants shall produce documents responsive to the Master Set of Requests for Production and in the Defendant Fact Sheets (“DFS”) on a rolling basis.

- c. The parties shall work in good faith to agree on a schedule for the rolling production.
4. **Schedule for Production of Plaintiffs' Documents.** Each Plaintiff shall produce documents requested in the Plaintiff Fact Sheet ("PFS") when the Plaintiff serves responses to the PFS.
5. **Method For Initial Collection of Potentially Responsive ESI.** In light of any forthcoming requests for production to the Brand Defendants, Plaintiffs and the Brand Defendants will cooperate in good faith to discuss and agree upon the method for collecting potentially responsive ESI (for example, a discussion of specific search terms to be used) at the appropriate time.
6. **Format of Production for Plaintiffs' Documents.**
 - a. Each Plaintiff shall produce documents in either hard-copy format or electronically on a disk or equivalent media.
 - b. The documents produced by Plaintiffs shall be Bates-stamped and, where appropriate, endorsed with a stamp identifying the document as confidential, in accordance with the March 20, 2012 Protective Order.
 - c. Every Plaintiff shall affix a prefix to the Bates stamp on every document produced. The prefix shall be the Plaintiff's first initial and last name (and, if needed, additional plaintiff-specific identification).

- d. This section shall not apply to require Plaintiffs who already have produced documents prior to the entry of this Order to produce their documents a second time in the format described above.

7. Format of Production for Defendants' Documents.

- a. Format of Production for ESI:
 - i. The Brand Defendants shall produce documents electronically ("Produced Documents") by providing them on disks or hard drives, or publishing them on a secure website, at the Brand Defendant's election.
 - ii. All Produced Documents will be in the form of Group IV .tif images at 300 dpi or greater.
 - iii. Each .tif file shall be Bates-stamped in accordance with the May 25, 2012 Order, and where appropriate, redacted and endorsed with a stamp identifying the document as confidential, in accordance with the March 20, 2012 Protective Order. After such production in .tif format is complete, a party must demonstrate a particularized need for production of electronic documents in any other format.
 - iv. Each Brand Defendant is assigned a prefix, as set forth below. The appropriate prefix shall be stamped on every .tif file produced.
 - A. The prefix assigned to Xanodyne Pharmaceuticals, Inc. is "XANO."
 - B. The prefix assigned to Eli Lilly is "LILLY."

- v. Any secure website, if elected for use by a producing party, will include a coding screen, such that Plaintiffs can designate any document for physical production to Plaintiffs. Brand Defendants will provide Plaintiffs a copy of any such document that is designated per paragraph 7.a.2 on a hard drive or disk (“Copied Documents”).
 - A. All Copied Documents shall be produced with a load file that is compatible with Concordance.
 - B. The Bates stamps and confidentiality endorsements that appear on the documents produced through any secure website also shall appear on the Copied Documents.
 - C. All Copied Documents will be produced with multi-page OCR text. Page breaks shall be preserved within the OCR text. OCR text files shall match the respective Bates number of its document, with a file extension of .txt.
 - D. Plaintiffs shall not produce or share Copied Documents except as already negotiated and agreed upon by the parties, and outlined in Section VII of the Stipulation and Protective Order of Confidentiality entered by the Court on March 20, 2012.
- b. Format of Production for Hard-Copy Documents:
 - i. Unless the producing party elects to scan, review, and produce selected hard copy material consistent with paragraph 7.a and its subparagraphs,

hard-copy documents will be made available for inspection and copying at the requesting party's expense.

- ii. Lilly IND/NDA and "Regulatory File" Documents. The obligation of Lilly to produce "regulatory file" documents pursuant to Section IV(B)(1) of the Court's May 25, 2012 *Procedures Governing Discovery* shall be stayed pending Plaintiffs' receipt and review of "regulatory file" documents from Xanodyne, as outlined in paragraph 7.b.iii, below, without any waiver of rights. After such review, Plaintiffs and Lilly will confer concerning the extent to which Plaintiffs still seek Lilly "regulatory file" documents and the procedures for such a production.
- iii. Xanodyne IND/NDA and "Regulatory File" Documents. Pursuant to Section IV(B)(1) of the Court's May 25, 2012 *Procedures Governing Discovery*, Xanodyne will produce its regulatory files for Darvon, Darvocet and/or any other propoxyphene-containing pain product that it actually marketed in the United States, or any part thereof, in its possession. Xanodyne will produce such documents on disks or hard drives in .tif format as Copied Documents. The parties acknowledge that the produced documents will contain personally identifiable information that will be redacted.
- iv. If the requesting party, upon inspection, wants copies of hard-copy documents, then unless the parties agree to a different format, such

documents shall be produced as image files in *.tif format at the requesting party's expense. The parties may also agree to share the cost of any requested enhancements to such *.tif images such as optical character recognition (OCR). No party is required to incur the cost of OCR without express agreement as to cost sharing.

v. All hard-copy documents shall be Bates numbered pursuant to paragraph 7.a.iv and produced with a load file that is compatible with Concordance.

c. Encryption: To maximize the security of information in transit, any media on which documents are produced may be encrypted by the producing party. In such cases, the producing party shall transmit the encryption key or password to the requesting party, under separate cover, contemporaneously with sending the encrypted media.

8. **Cost.**

a. The cost of production of any Copied Documents pursuant to this Document Production Protocol shall be \$0.10 per page. The cost shall be allocated/paid as follows:

- i. One-half the cost (*i.e.*, \$0.05 per page) shall be paid by the requesting party at the time of production.
- ii. One-half of the cost shall be deemed a taxable cost available for recovery by the producing party, subject to the producing party's application for the

award of such costs pursuant to law depending on the ultimate disposition of the litigation.

- b. Brand Defendants shall reimburse each Plaintiff for every document produced directly by the Plaintiffs consistent with paragraph 8.a, above.
- c. Brand Defendants will provide copies of every document obtained from third parties through the use of any authorization described in the May 25, 2012 Order if the Plaintiff has paid to the Brand Defendants:
 - i. One-half the cost charged by the provider, employer, or other entity that provided such documents pursuant to a release, plus
 - ii. \$0.10 per page for hard copies of produced documents.
 - iii. No costs in addition to those set forth in paragraph 8(c)(i) will be applicable if third parties produce documents in electronic format and Plaintiffs request electronic copies in lieu of hard copies.
- d. Notwithstanding the foregoing, the parties reserve the right to revisit issues regarding cost sharing and the costs of production as additional discovery requests are served or exchanged or as circumstances change.

9. **Organization of Production.** The documents produced shall be either:

- a. Organized and labeled to correspond with the number of the specific request to which the documents are responsive; or,
- b. Produced in the order in which they are kept in the usual course of business.

10. **Avoidance of Duplicate Production.** Each party will take all reasonable steps to reduce duplication of documents within production sets. De-duplication will be performed globally across data sets. The parties may also use e-mail thread suppression to reduce duplicative production of e-mail threads by producing the most recent e-mail containing the thread of e-mails, as well as all attachments within the thread.

11. **Privilege Log.** Any document withheld on the basis that the producing party believes production of the document is protected by the work product doctrine or an applicable privilege (“Privileged Material”) shall describe that document in a privilege log, as set forth in the May 25, 2012 Order.

- a. No party need list on a privilege log:
 - i. Documents generated after December 3, 2010. Documents produced and redacted for privilege, so long as:
 - A. For e-mails, the bibliographic information (*i.e.*, to, from, cc, bcc, date/time) is not redacted; and
 - B. For non-email documents, the redaction is noted on the face of the document in the redaction field.
 - ii. An e-mail thread may be logged in a single entry provided that such entry identifies all senders and recipients appearing at any point in the thread.
 - iii. Documents that are presumptively privileged need not be logged. These are:

- A. Internal communications within (a) a law firm, (b) a legal assistance organization, (c) a governmental law office or (d) a legal department of a corporation or of another organization.
 - B. Communications solely between outside counsel and in-house counsel.
- b. After the receipt of a privilege log, any party may dispute a claim of privilege; however, prior to any submission to the Court for an *in camera* review, the party disputing a claim of privilege shall provide in writing the identification of the documents for which it questions the claim of privilege and the reasons (including legal support) for its assertion that the documents are not privileged. Within thirty days, the party seeking to support the claim of privilege shall provide a written response supporting the claim of privilege (including legal support). The parties will then meet and confer in good faith as to the claims of privilege. If agreement cannot be met after thirty days, any party may thereafter submit the Discovery Material under seal to the Court for a determination as to privilege.
12. **Inadvertent Disclosure of Privileged Material.** The inadvertent production of Privileged Material shall be governed by Section X of the March 20, 2012 Stipulation and Protective Order of Confidentiality.
13. **Authenticity and Admissibility.** Nothing in this protocol shall be construed to affect the authenticity or admissibility of any document or data. All objections to the authenticity or admissibility of any document or data are preserved and may be asserted at any time.

14. **Confidential or Highly-Confidential-Attorneys' Eyes Only Information.** For the avoidance of doubt, nothing herein shall contradict the parties' rights and obligations with respect to any designated Confidential Information, as governed by the March 20, 2012 Protective Order regarding the protection of such information.

This 11th day of October, 2012.



Signed By:

Danny C. Reeves DCR

United States District Judge

II. Definitions

A. Documents and Electronically Stored Information

As used herein, “*Documents*” and “*Electronically Stored Information*” shall be defined as they are in Rule 34 of the Federal Rules of Civil Procedure. Information that serves to identify or locate such documents and ESI, such as file inventories, file folders, indices and metadata, if any, are also included in this definition. No party is under an obligation to preserve voice mail, instant messages, or information on hand held devices synchronized to other electronic media that store such data. No party is under an obligation to preserve temporary, transient, residual or fragmented data. Except as otherwise described in this Order, the corporate parties may continue the routine, good-faith operation of their electronic information systems.

B. Preservation

As used herein, “*Preservation*” shall be interpreted to accomplish the goal of maintaining the integrity of potentially relevant *Documents*, *ESI* and *Tangible Things* and shall include taking reasonable steps to prevent the partial or full destruction, alteration, shredding or deletion of such materials related to plaintiffs’ claims. Provided that reasonable steps have otherwise been taken to preserve potentially relevant *Documents*, *ESI* and *Tangible Things* related to plaintiffs’ claims, the defendants may continue the practice of rewriting and/or reusing backup tapes and media. Electronic documents and data shall be maintained and preserved in their native format, except as authorized by §V below.

C. Product(s)

As used herein, the term “*Product(s)*” means any and all propoxyphene-containing pain medicine(s), including “Darvocet” and “Darvon” and/or generic prescription propoxyphene-containing pain medicines. Defendants are not obligated by this Litigation to preserve materials relating to any other products.

D. Healthcare Provider

As used herein, the term “*Healthcare Provider*” means any surgeon, physician (whether homeopathic, osteopathic or chiropractic), physician assistant, physical, occupational or rehabilitative therapist, pharmacist, nurse, psychologist, dentist, psychiatrist, social worker, alternative healthcare practitioner, counselor or other practitioner of the healing arts.

E. Medical Facility

As used herein, the term “*Medical Facility*” means any location where the healing arts are practiced including but not limited to hospitals, doctor’s offices, clinics, urgent care centers, emergency rooms, trauma centers and nursing and long-term care facilities. For purposes of this Order, “Medical Facility” also refers to any location where prescription pharmaceutical products are dispensed, including but not limited to, pharmacies.

III. Preservation Obligations — Defendants

Defendants shall take reasonable steps, including the dissemination of Legal Hold Notices to employees and manufacturers of the product(s) to preserve *Documents*, *ESI* and *Tangible Things* believed to be reasonably related to plaintiffs’ claims in this litigation. Such material may include regulatory documents, purported adverse event reports, INDs/NDAs/ANDAs as

applicable, product literature, lot samples, and promotional materials, if any, for the Product(s). This obligation requires defendants and their employees to preserve all relevant e-mails, websites, ESI on removable media, postings or statements made on social media, chat rooms, blogs, etc.

IV. Preservation Obligations — Plaintiffs

The individual plaintiffs in the Litigation shall take all reasonable steps to ensure the preservation of *Documents*, *ESI* and *Tangible Things* that are reasonably related to plaintiffs' claims in the Litigation. This includes, but is not limited to, the following *Documents*, *ESI* and *Tangible Things*:

- A. Product labels, bottles, packaging, containers and remaining Product.
- B. ESI stored on the hard drive of a computer owned by plaintiff or plaintiff's decedent. This obligation does not require a plaintiff to copy or create a duplicate image of the hard drive. Plaintiff's obligation is fulfilled if the relevant ESI and documents are retained on the hard drive. However, if the computer is replaced, the plaintiff will retain the old computer hard drive in order to satisfy his or her preservation obligation.
- C. ESI stored on any removable media owned by plaintiff or plaintiff's decedent. This obligation does not require a plaintiff to copy or create a duplicate image of the media. Plaintiff's obligation is fulfilled if the relevant documents are retained on the media or plaintiff creates and maintains complete hard copies of any documents on the media.
- D. To the extent discovered or otherwise known or found, postings or statements made by plaintiff or plaintiff's decedent on social media, chat rooms, blogs, etc.

E. All diaries and calendars from January 1, 1991 to the present, or for a period of five years pre-dating the date of the first alleged ingestion of the Product to the present, whichever period is longer.

F. E-mails (whether on plaintiff's or plaintiff's decedent's hard drive or stored on ISP servers or services such as g-mail, Hot-mail, and the like) and written communications.

G. Records of and printed results from Internet searches reasonably related to plaintiff's claims.

H. Medical and pharmacy records and records of medical or pharmacy expenses. For cases currently pending in this Litigation, each plaintiff shall notify the individuals or entities listed below in subparagraphs 1. through 6. within sixty (60) days of this Order, or within forty-five (45) days of discovering an additional individual or entity, that they have records relevant to the plaintiff's claims and that those records must be preserved, pending collection by a party to the Litigation or appropriate party designee. For future cases transferred or reassigned to this Litigation, each plaintiff must comply with this notice requirement within sixty (60) days of a case being docketed to this Court. The following individuals or entities must be notified pursuant to paragraph H:

1. All pharmacies that dispensed any medications to the plaintiff or plaintiff's decedent from January 1, 1991 to the present, or for a period of five years pre-dating the date of the first alleged ingestion of the Product to the present, whichever period is longer];

2. All Medical Facilities, Healthcare Providers and/or others persons who plaintiff claims provided any samples of the Products to the plaintiff or plaintiff's decedent;

3. All Medical Facilities and/or other Healthcare Providers who prescribed the Products for the plaintiff or plaintiff's decedent;

4. All Medical Facilities and/or Healthcare Providers who treated plaintiff or plaintiff's decedent from January 1, 1991 to the present, or from the five year period pre-dating the date of the first alleged ingestion of the Product to the present, whichever period is longer];

5. All medical examiners, coroners, or toxicology laboratories involved in the examination or investigation of a plaintiff's decedent's death; and

6. If plaintiff is seeking lost wages, all of his/her/plaintiff's decedent's employers for the period from five years prior to the date for which he or she is seeking lost wages through the last day for which plaintiff is seeking lost wages.

7. Plaintiff shall provide the names and addresses of all individuals or entities to which notices were sent, in due course, if requested by defendants through discovery.

V. Acceptable Methods of Preservation

The following methods of preserving *Documents*, *ESI* and *Tangible Things* shall satisfy a Party's duty to preserve in the Litigation. Defendants may select any of the non-exclusive methods set forth under each sub-section A through C as the means to preserve *Documents*, *ESI* or *Tangible Things*, and the decision as to which method to use is at the judgment of the party. The methods below shall be deemed sufficient, but do not rule out other methods.

A. E-mail

The defendants shall preserve e-mail communications and associated attachments (of employees located in the United States) reasonably related to plaintiffs' claims, by either:

1. Maintaining one set of back-up tapes for implicated servers; or
2. Creating an electronic snapshot of implicated servers; or
3. Maintaining e-mail files on a server or within an electronic archive.

B. Databases

Defendants utilize a variety of databases to operate their business. Defendants will issue a preservation notice to employees located in the United States believed to have information reasonably related to plaintiffs' claims; the scope of this notice will include information stored in databases housed on servers located in the United States. The defendants shall preserve data held in such databases, believed to contain information reasonably related to plaintiffs' claims, by:

1. Maintaining such data in accessible electronic systems; or
2. Creating an electronic snapshot of relevant database servers; or
3. Maintaining one set of back-up tapes for relevant database servers.

C. Electronic documents contained in Shared or Home Directories

Where electronic documents in shared or home directories (e.g., word processing documents, spreadsheets, and PowerPoint presentations) are subject to a deletion schedule, the defendants shall preserve documents believed to be reasonably related to plaintiffs' claims contained in shared and home directories housed on servers located in the United States by:

1. Maintaining such directories and files contained therein in accessible electronic systems; or
2. Creating an electronic snapshot of relevant shared drive or home directory servers; or
3. Maintaining one set of back-up tapes for relevant servers.

D. Tangible Documents

For Documents not in electronic form the party shall maintain the original form of the document, a copy, or scanned image.

VI. Reservation of Rights

The Parties do not concede that any of the information subject to this Order is discoverable, relevant or admissible, and the Parties expressly reserve the right to challenge any specific discovery request concerning any such information. The Parties also reserve the right to challenge the competency, relevance, materiality, privilege and/or admissibility into evidence of such documents, information or material in these or any subsequent proceedings or at the trial of these or any other actions, in this or any other jurisdiction.

This 16th day of November, 2011.

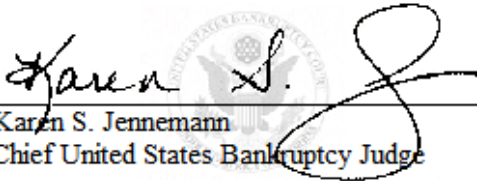


Signed By:

Danny C. Reeves DCR
United States District Judge

ORDERED.

Dated: August 18, 2015


Karen S. Jennemann
Chief United States Bankruptcy Judge

UNITED STATES BANKRUPTCY COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION
www.flmb.uscourts.gov

In re:

ADVANCED TELECOMMUNICATION
NETWORK, INC.,

Debtor.

Case No. 6:03-bk-00299-KSJ

Chapter 11

ADVANCED TELECOMMUNICATION
NETWORK, INC., a New Jersey corporation,

Plaintiff,

Adv. Proc. No. 6:05-ap-00006-KSJ

Adv. Proc. No. 6:05-ap-00008-KSJ

v.

FLASTER GREENBERG, P.C. and
PETER R. SPIRGEL,

Defendants.

STIPULATION AND ORDER REGARDING DISCOVERY PROCEDURE

WHEREAS, the various claims and defenses in this action may require each Party to produce voluminous information and documents through the discovery process and a page-by-page preproduction privilege review may impose an undue burden on the Parties and a waste of resources; and

WHEREAS, the Parties have stipulated to the entry of a claw back order pursuant to Rule 502(d).

NOW THEREFORE, pursuant to Rules 16(b) and 26(c) of the Federal Rules of Civil Procedure, and pursuant to Rule 502 of the Federal Rules of Evidence, it is hereby ORDERED:

1. This Order invokes the protections afforded by Rule 502(d) of the Federal Rules of Evidence.
2. Each Party is entitled to decide the appropriate degree of care to exercise in reviewing materials for privilege, taking into account the volume and sensitivity of the materials, the demands of the litigation, and the resources that the Party can make available. Irrespective of the care that is actually exercised in reviewing materials for privilege, the Court hereby orders pursuant to Rule 502(d) of the Federal Rules of Evidence that disclosure of privileged or protected information or documents in discovery conducted in this litigation will not constitute or be deemed a waiver or forfeiture—in this or any other federal or state proceeding—of any claims of attorney-client privilege or work product protection that the disclosing Party would otherwise be entitled to assert with respect to the information or documents and their subject matter.
3. Either Party may seek to claw back any privileged document within 7 days of determining that the Party has produced such materials.
4. If a Party identifies a document, produced by the opposing Party in discovery, that appears on its face to be subject to a claim of privilege without an applicable written voluntary waiver, and further provided that the Party receiving such document wishes to use such document in such a manner that would reveal the contents of such document to any other person, then the Party receiving such document shall provide 7 days written notice to the opposing Party so that such opposing Party may file any applicable claim seeking to claw back such document pursuant to this Order. If the opposing Party does not seek to claw back such document within this 7 day time frame, any claim of privilege with respect to that document shall be deemed waived.
5. To the extent a document that has not previously been identified, as set forth in paragraphs 3 or 4 above, is listed on a Party's Exhibit List for trial, any request to claw back such document must be made no later than 14 days after the Party has filed its Exhibit List for trial, or such claim shall be deemed waived. Any Party that complies with the foregoing will be deemed to have taken reasonable steps to rectify disclosures of privileged or protected information or materials.
6. Upon receiving notice of any claim seeking to claw back any document, the receiving Party must, in accordance with Fed. R. Civ. P. 26(b)(5)(B), promptly sequester the specified information and any copies it has and may not use or disclose the information, except as provided by Fed. R. Civ. P. 26(b)(5)(B), until such claim is resolved.
7. The Party wishing to assert any claim of privilege retains the burden of establishing the applicability of the claimed privilege. This Order does not preclude a written voluntary waiver of any claims of privilege.

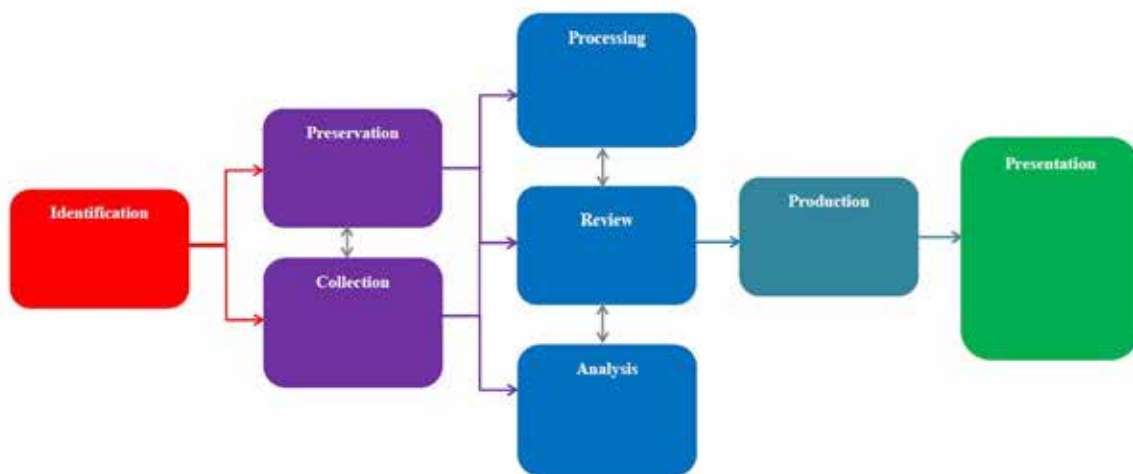
8. Before or concurrently with the production of documents, the producing Party shall provide the receiving Party with a list of individuals between whom privileged or protected materials would have been exchanged (List of Privileged Players). The List of Privileged Players shall include all attorneys, clients, and clients representatives. If, after the production of documents, a producing Party discovers additional individuals who need to be added to the List of Privileged Players, the producing Party should supplement its List of Privileged Players and provide a copy to the other party within 14 days of making the discovery.
9. To the extent either Party withholds a document on the basis of privilege, such Party shall produce a privilege log that complies with the requirements of Fed. R. Civ. P. 26 either before or concurrently with the production of the producing Party's documents.
10. Nothing in this Order supersedes or replaces any provisions of Federal Rule of Evidence 502 or Federal Rule 26, except 502(b). Any terms not defined in this document should be interpreted consistently with Rule 502 and Rule 26.

Roberta A. Colton is directed to serve a copy of this order on interested parties who are non-CM/ECF users and file a proof of service within 3 days of entry of the order.

eDiscovery & ESI: Practical Applications



Electronic Discovery Reference Model



Scoping

How can you assist with the duty to preserve?

- Custodians: which individuals have relevant ESI?
- Devices
- Consider the type of information on each device
- Automatic purge policies
- Third-Party with Repositories

Where is our data?

- Single on Premise Server
 - Email and files
- Desktops/Laptops
 - User files
- No remote access
- No BYOD
- No Cloud
- No outsources services

Entities & Types of ESI

- Banks
- Corporations
- Individuals

Preservation

- Litigation Hold Letter
- Purpose
- Proof of Delivery
- Acknowledgement
- Party vs. Non-Party Distinction

Spoliation

- Common issues
 - Collection Errors
 - Incomplete Collection

Collection & Preservation

- What is preservation? collection?
- Form request for production
- Security issues?
- Knowledge of the business and parties involved is required
 - Banks
 - Corporations
 - Individuals

Processing, Review & Analysis

- How to get the information down to a manageable amount of data for review?
- Cost
- What tools/analytics are available on a review platform?
- Search terms
- Hit reports
- Recovering deleted ESI

Text Analytics

- Email Threading
- Near Duplicate Detection
- Categorization
- Domain Filter
- Prioritization
- Technology Assisted Review

Misc. Issues

- Security in collection/preservation/ review
- Forensic tools to assist in eDiscovery?
- Metadata vs. no metadata
- What should in-house counsel/outside counsel look for in an eDiscovery vendor?
- What are the typical pitfalls in dealing with an outside vendor?

The Federal Standard



- Fed. R. Civ. P. 37(e)
- *Zubulake v. UBS Warburg*

The Florida Standard

FLORIDA RULES
OF CIVIL
PROCEDURE

- Fla. R. Civ. P. 1.380(e)
- *League of Women Voters of Florida v. Detzner*, 172 So. 2d 363, 391 (Fla. 2015)
- When are sanctions appropriate?



Procaps S.A. v. Patheon Inc., Case No. 12-24356-CIV-GOODMAN, 2015 WL 4430955 (S.D. Fla. July 20, 2015)



Brown v. Tellerate Holdings Ltd., No. 2:11-cv-1122, 2014 WL 2987051 (S.D. Ohio July 1, 2014)



Moore v. Publicis Groupe, No. 11 Civ. 1279, 2012 WL 607412(ALC)(AJP) (S.D.N.Y. Feb. 24, 2012)



Bridgestone Americas, Inc. v. Int'l Bus. Machs. Corp., No. 3:13-1196, 2014 wk 4923014 (M.D. Tenn. July 22, 2014)

Questions?

Michael McCartney
President Avalon Cyber
741 Main Street
Buffalo, NY 14203
Phone: 716-995-7777
Fax: 716-995-7778
Cell: 716-706-8403
Michael.McCartney@teamavalon.com
www.teamavalon.com



James D. Gassenheimer
Berger Singerman
1450 Brickell Ave, Suite 1900
Miami, FL 33131
Phone: 305-755-9500
Fax: 305-714-4340
Direct: 305-714-4383
Jgassenheimer@bergersingerman.com
www.bergersingerman.com



**PRIVILEGED AND CONFIDENTIAL
ATTORNEY/CLIENT COMMUNICATION**

**INFORMATION NEEDED BY _____, 201____
YOUR RESPONSE TO THIS MEMORANDUM IS REQUIRED**

_____, 201____

Demand for Preservation of Electronically Stored Information

[PLAINTIFFS / COUNSEL] demand that you preserve all documents, tangible things and electronically stored information potentially relevant to the issues in this case. As used in this document, “you” and “your” refers to [NAME OF DEFENDANT], and its predecessors, successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

You should anticipate that much of the information subject to disclosure or responsive to discovery in this matter is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)

- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO)
- Back Up tape media

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obligated to preserve potentially relevant evidence from both these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/06), you must identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably accessible. For good cause shown, the court may then order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the [PLAINTIFFS / COUNSEL] of their right to secure the evidence or the Court of its right to adjudicate the issue.

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information with the earlier of a Created or Last Modified date on or after [DATE] through the date of this demand and concerning:

1. The events and causes of action described in [Plaintiffs' Complaint];
2. ESI you may use to support claims or defenses in this case;
3. Back ups of all Epic System applications used for the administration of electronic records management of patient data.
4. Any and all associated log files, audit files, user authentication logs, data change logs, transaction logs, or overall system logs.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve document, tangible things and other potentially relevant evidence.

Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion

You should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees and officers. It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

Preservation by Imaging

You should take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive, including use of commercially available backup

software such as Ghost, is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file.

With respect to the hard drives and storage devices of each of the persons named below and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by that person during the period from ____ to ____, as well as recording and preserving the system time and date of each such computer.

[Insert names, job descriptions and titles here].

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration. The use of outside, qualified forensic experts should be contemplated.

Preservation in Native Form

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained (Native File Format). Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

You should further anticipate the need to disclose and produce system and application metadata and take proactive steps to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data, file path or data location information and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded

attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields. The use of outside, qualified forensic experts should be contemplated.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that we will accept as sufficient, please call to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home, portable systems and cloud based repositories that may contain potentially relevant data. To the extent that officers, board members or employees have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's PDA, smart phone (BlackBerry, iPhone, etc), voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based email accounts or cloud services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved. Any data stored within Cloud Storage locations (such as Dropbox, Apple iCloud, Microsoft OneDrive, Amazon Cloud Storage or the like) should also be preserved.

Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like.

You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys and Third Parties

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control.

Accordingly, you must notify any current or former agent, attorney, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System Sequestration or Forensically Sound Imaging

We suggest that, with respect to [NAME KEY PLAYERS] removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step.

In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss. A forensically certified professional with the appropriate certifications should be used to perform this function.

By “forensically sound,” we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called “unallocated clusters,” holding deleted files. The use of outside, qualified forensic experts should be contemplated.

Preservation Protocols

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I'm available to discuss reasonable preservation steps; however, you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Confirmation of Compliance

Please confirm by [DATE], that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Respectfully,

[Paul Steven Singerman](#)
[\(305\) 714-4343](#)
Singerman@bergersingerman.com

[ABC](#)

Re: [ABC](#) (“Matter”)

Identification, Preservation and Collection of Information and Records
(Including Electronically Stored Information)

Dear [ABC](#):

In connection with our engagement as counsel to [ABC](#) (“You” or “Your”), we advise You of Your duty and our duty, as outside counsel, to identify and preserve information and records that may be relevant to the Matter, including electronically stored information, and set forth the steps that You and we should follow to fulfill our respective duties to identify and preserve information and records that may be relevant to the Matter.

**A. Your Duty To Preserve All Potentially Relevant Information, Including
“Electronically Stored Information”**

One of Your (and our) primary obligations is to identify and preserve all information potentially relevant to the Matter, including for example, physical documents, records and tangible items that may be relevant to the Matter. This obligation also includes the preservation of information stored electronically in Your computers and electronic information systems, mobile devices and removable electronic media. Electronically Stored Information (“ESI”) includes (i) email and other electronic communications; (ii) word processing documents, spreadsheets, and other user-created files; (iii) electronic data files (such as those created by programs that process financial, accounting, billing, marketing or sales information); (iv) databases; (v) electronic calendars and scheduling programs; (vi) telephone logs; (vii) contact manager and/or sales force automation (“SFA”) tools and files; (viii) Internet usage histories and files; (ix) social media content (for instance, LinkedIn, Facebook, Twitter and YouTube accounts and content); (x) instant messaging (“IM”) files and logs; (xi) network access information; and (xii) voicemail.

ESI may exist on multiple storage devices and in multiple locations, including (i) “online” data storage devices such as mainframes, servers, personal computers, laptop computers, PDAs, mobile devices such as “BlackBerrys”, “iPhones” and “Androids”, tablets, “flash drives” or “thumb drives”; and (ii) “backup,” archival or “offline” storage such as backup tapes, floppy disks, CD-ROMS, and optical disks. We have enclosed a checklist of various types of physical documents and records, electronically stored information and electronic storage devices with which You and Your employees should be familiar (*see Attachment A* to this letter). This checklist is intended to be over-inclusive; not all of the documents, records and devices identified in the checklist may be relevant to this Matter or to You; however, we have found this checklist helpful in ensuring that You consider all potentially relevant documents, records and data, and all potential locations and devices where relevant information might be stored.

We as Your outside counsel also have duties concerning the identification, preservation and collection of relevant information and documents, particularly in the context of electronically stored information. These duties include providing advice to You of Your obligation to preserve relevant information, including electronically stored information, identifying steps that You should take to preserve relevant information, becoming familiar with Your document retention methods, electronic information storage systems and data retention architecture, and monitoring Your compliance with the obligation to preserve relevant information.

Depending upon the nature, location and quantity of electronically stored information, Your compliance with this obligation may require substantial time and effort. We appreciate the burden this obligation imposes on You, and we will do our best to assist You.

***Please note:** Your failure to comply with these duties could result in severe adverse consequences for You if loss or destruction of relevant evidence occurs. These severe adverse consequences could include, for example, adverse inference instructions to the jury, court-imposed monetary sanctions against You, and/or the entry of a default judgment against You on liability and/or damages.*

B. Preliminary Assessment of What May Be Relevant

Based upon our initial discussions and preliminary investigation, the Matter concerns [describe parameters of factual and legal issues perceived]. We further expect that discovery of facts will cover the following period of time: [insert timeframe]. However, both the scope and time period relevant to the Matter may change as we receive further information. For this reason, You should view Your obligations to identify and preserve relevant information broadly.

C. Steps You Should Take to Identify, Preserve and Collect Relevant Information and Records

Under applicable law, You are required to immediately suspend any destruction of documents and put in place a “litigation hold.” The purpose of a “litigation hold” is to prevent the inadvertent deletion, alteration or corruption of relevant information. The “litigation hold” must apply to all potentially relevant sources of electronically stored information as well as to physical records and tangible items.

Among other things, You must halt all routine deletion, archiving, recycling or destruction practices for information and records relevant to the Matter (whether in tangible form or electronically stored), including “re-write” programs, system upgrades, operating system re-installations, data compressions, disk de-fragmentation or optimization routines that could destroy, corrupt or alter electronically stored information potentially relevant to the Matter. You should suspend any automatic deletion or purging rules for Microsoft Outlook or any other program that includes an automatic deletion function.

You should halt all overwriting, recycling or erasing of online or offline data storage (such as back-up tapes or other storage media) that may contain information relevant to the Matter. All existing back-up tapes that may contain information and records relevant to the Matter must be held aside and not recycled.

You should not remove, repair or otherwise alter any computers, handheld devices (such as PDAs) or any other electronic devices that may contain information and records relevant to the Matter without consultation with counsel.

You should immediately provide a copy of this letter to Your IT personnel and ensure their compliance with these obligations. In addition, You should immediately provide a copy of this letter to all persons who possess, control or have regular access to information and records relevant to the Matter (“Key Personnel”) and direct them to take all reasonable steps to preserve those information and records. Key Personnel also includes any outside contractors, accountants, attorneys or other professional consultants that are subject to Your control.

You also remain obligated to identify, preserve and collect information and records relevant to the Matter that come into existence in the future.

D. Further Consultation

We will contact You shortly to confirm Your receipt of this letter, to discuss any questions You may have regarding Your obligations, and to discuss Your efforts to identify, preserve and collect records and information relevant to the Matter. If You have any questions in the meantime, please contact us immediately.

Sincerely,

BERGER SINGERMANN LLP

Paul Steven Singerman

PSS

ee:

ATTACHMENT A

**CHECKLIST OF PHYSICAL DOCUMENTS AND RECORDS,
ELECTRONICALLY STORED INFORMATION AND ELECTRONIC
STORAGE DEVICES**

a. Physical Records, and Other Tangible Items

The following are examples of the types of physical documents, records and tangible items that may be relevant to the Matter (whether maintained as active records or in storage): abstracts; acceptance test procedures; address books; advertisements; agreements; analyses of any kind; appointment books; bid packages; bids; books of account; brochures; bulletins; calendars; catalogues and catalog sheets; charts; check books; checks; check stubs; circulars, compilations; consultants' reports or studies; contracts; correspondence; data sheets and reports; defective material reports and deficiency lists and memoranda; diagrams; directories; discs; drafts; drawings; estimates; experts' reports or studies; financial statements or calculations; graphs; data sheets and reports; interoffice and intra-office communications; invoices; laboratory notebooks; layouts; ledgers; letters; licenses; lists; log books; manuals; maps; memoranda of any type; microfilm; minutes or records of any sort of directors' and/or board meetings; minutes or records of any other sort of meetings; movies; notebooks; notes; operating, maintenance, and instruction manuals; opinions; organization charts, directories, tables, and lists; pamphlets; parts lists; photographs; pictures; plans; presentations; press clippings or releases; procedures; pro forma invoices or pro forma purchase orders; projections; promotional materials; proposals; publications; publicity materials or releases; purchase orders or invoices; quality control procedures; radiograms; records and recordings of any kind; rejection reports; renderings; reports of any kind; rework instructions/orders; sales orders and sales records; salvage instructions and reports; schedules; scrap reports; service reports; sketches; specifications; statistical analyses; stress analyses; studies of any kind; style books; subcontracts; summaries; tabulations; tallies; tapes; technical specifications; telegrams; teletype, telefax, and telex messages; telephone logs and messages; test procedures; test records, reports, and specifications; time logs; vouchers; working drawings, papers and files; and drafts of such documents.

b. Electronically Stored Information

The following are examples of the types of electronically stored information that may be relevant to the Matter: (i) "active data" (data immediately and easily accessible on Your computer systems), (ii) "archived data" (data residing on backup tapes or other storage media), (iii) "deleted data" (data that has been deleted from a system's drive but is recoverable through computer forensic techniques), and/or (iv) "legacy data" (data created on old or obsolete hardware or software).

The following are common types of electronically stored information:

E-Mail: All internal and external e-mail (including metadata, message contents, header information and logs of e-mail system usage). E-mail must be preserved in electronic format, regardless of whether hard copies of the information exist. This includes any web-based e-mail systems used by relevant persons (such as Gmail, AOL, and Yahoo!).

User Created Electronic Documents and Files: Active and deleted copies of word processing files, spreadsheets, PowerPoint or other user created electronic documents and files. The obligation to preserve these records includes all drafts and revisions; and, includes the software application programs used to create such electronic documents and files.

Databases: All databases (including all fields and structural information of such databases) containing information that may be relevant to the subject matter of the Matter.

Activity Logs: All paper and/or electronic logs of Your computer system and network activity pertaining to data storage that (i) reflect use of Your computer system or network activity by relevant persons, and/or (ii) contain information relevant to the Matter.

Calendars/Electronic Task Management Information: Active and deleted copies of electronic calendars or scheduling programs, as well as all data generated by calendaring, task management and personal information management software (such as Microsoft Outlook) (i) of any of the relevant persons during the relevant time period, and/or (ii) concerning any issues relevant to the Matter.

Contact Manager/ Sales Force Automation (“SFA”) Information: Active and deleted copies of files and records created and/or maintained by any contact manager, SFA, or similar sales or marketing programs or tools.

PDA Created Information: Data created with personal data assistants (PDAs) (such as PalmPilot or BlackBerry) (i) by any of the relevant persons during the relevant time period, and/or (ii) concerning any issues relevant to the Matter.

Voicemail: Voicemail (i) received by any of the relevant persons during the relevant time period, and/or (ii) concerning any issues relevant to the Matter.

Internet and Web Browser Related Files: Records of Internet and web-browser generated files (i) reflecting activities by the relevant persons during the relevant time period, and/or (ii) concerning any issues relevant to the Matter. This would include webpages, as well as files, logs and records relating to text and instant messaging (“IM”) usage, chat rooms, newsgroups, user groups, “cookies,” “listserves,” cache files, Internet history logs, firewalls and web logs.

Audio, Photographic, Video and Multimedia Files: Electronic files that store audio, photographic, video and multimedia content that is relevant to the Matter.

Other Electronically Stored Information: You may well have other types of electronically stored information which may relate to the Matter. It is important that it also be preserved. These other types of electronically stored information should be immediately identified and preserved.

c. Electronic Data Storage Devices and Media

Potentially relevant data identified above may be stored in or on multiple electronic data storage devices¹ and/or media, including the following:

Online Data Storage Devices and Media: Online storage and/or direct access storage devices include mainframe computers, mini-computers, servers, personal computers (desktop, workstation, laptop or otherwise), mobile devices, tablets, voice mail and answering machines, paging devices, printers, copiers, CD duplicators, digital cameras and camcorders, and electronic game devices.

Offline Data Storage Devices and Media: Offline data storage devices and media include backup and archival devices and media such as “cloud storage”, backup computers, servers, backup or removable hard drives, floppy diskettes, backup/archival tapes and media (such as magnetic, magneto-optical, and/or optical tapes and cartridges), DVDs, CDROMs, Jaz and Zip disks, “SuperDisks,” PC Cards, removable drives and memory (such as “pen” or “thumb” drives, micro drives, Bernoulli drives and memory sticks) and memory cards (such as compact flash cards and smart cards). You must immediately suspend all activity that might result in destruction or modification of all of the data stored on any such offline devices or media, including overwriting, recycling or erasing all or part of the media.

Data Storage Device Replacement: If You replace any electronic data storage devices or media that may contain relevant information, You should not dispose of such storage device or medium.

¹In order to preserve information stored on the hard drives of computers and servers, You should consider securing a “mirror image” copy (a bit-by-bit copy of a hard drive that ensures that the computer system is not altered during the imaging process) of all electronic data contained on the personal computers and/or laptops of the relevant persons. The “mirror image” must include active files, deleted files, deleted file fragments, hidden files, directories, and any other data contained on the computer.

FIRST REQUEST FOR PRODUCTION OF DOCUMENTS

Pursuant to Rule 1.350 of the Florida Rules of Civil Procedure, «Client», requests that «Recipient», produce the following described documents and tangible things in accordance with Rule 1.350 and the definitions and instructions stated below, at the offices of Berger Singerman, 1450 Brickell Avenue, Suite 1900, Miami, FL 33131-3453, within 30 days of service of this Request.

I. DEFINITIONS AND INSTRUCTIONS:

The following definitions shall apply to this Request:

A. “You”, “Your”, or “[Recipient]” as used herein means [Recipient] and includes any and all agents, employees, servants, officers, directors, attorneys and any other person or entity acting or purporting to act on its behalf.

B. “Person” as used herein means any natural person or any entity, including without limitation any individual, firm, corporation, company, joint venture, trust, tenancy, association, partnership, business, agency, department, bureau, board, commission, or any other form of public, private or legal entity. Any reference herein to any public or private company, partnership, association, or other entity include such entity’s subsidiaries and affiliates, as well as the present and former directors, officers, employees, attorneys, agents and anyone acting on behalf of, at the direction of, or under the control of the entity, its subsidiaries or its affiliates.

C. “Documents” shall mean the original or copies of any tangible written, typed, printed or other form of recorded or graphic matter of every kind or description, however produced or reproduced, whether mechanically or electronically recorded, draft, final original, reproduction, signed or unsigned, regardless of whether approved, signed, sent, received, redrafted, or executed, and whether handwritten, typed, printed, photostated, duplicated, carbon or otherwise copied or produced in any other manner whatsoever. Without limiting the generality of the foregoing, “documents” shall include correspondence, letters, telegrams, telexes, mailgrams, memoranda, including inter-office and intra-office memoranda, memoranda for files, memoranda of telephone or other conversations, including meetings, invoices, reports, receipts and statements of account, ledgers, notes or notations, notes or memorandum attached to or to be read with any document, booklets, books, drawings, graphs, charts, photographs, phone records, electronic tapes, discs or other recordings, computer programs, printouts, data cards, studies, analysis and other data compilations from which information can be obtained. Copies of documents, which are not identical duplications of the originals or which contain additions to or deletions from the originals or copies of the originals if the originals are not available, shall be considered to be separate documents.

“Documents” shall also include all electronic data storage documents or electronically stored information (ESI) including but not limited to e-mails and any related

attachments, electronic files or other data compilations which relate to the categories of documents as requested below. Your search for these electronically stored documents shall include all of your computer hard drives, floppy discs, compact discs, backup and archival tapes, removable media such as zip drives, password protected and encrypted files, databases, electronic calendars, personal digital assistants, proprietary software and inactive or unused computer disc storage areas.

ESI shall be produced in the format described in Exhibit "B" hereto.

D. "Communications" shall mean any oral or written statement, dialogue, colloquy, discussion or conversation and, also, means any transfer of thoughts or ideas between persons by means of documents and includes a transfer of data from one location to another by electronic or similar means.

E. "Related to" shall mean, directly or indirectly, refer to, reflect, mention, describe, pertain to, arise out of or in connection with or in any way legally, logically, or factually be connected with the matter discussed.

F. As used herein, the conjunctions "and" and "or" shall be interpreted in each instance as meaning "and/or" so as to encompass the broader of the two possible constructions, and shall not be interpreted disjunctively so as to exclude any information or documents otherwise within the scope of any request.

G. Any pronouns used herein shall include and be read and applied as to encompass the alternative forms of the pronoun, whether masculine, feminine, neuter, singular or plural, and shall not be interpreted so as to exclude any information or documents otherwise within the scope of any request.

H. Unless otherwise specified herein, the time frame for each request is from and including _____ to the present.

I. If you contend that you are entitled to withhold any responsive document(s) on the basis of privilege or other grounds, for each and every such document specify:

- i. The type or nature of the document;
- ii. The general subject matter of the document;
- iii. The date of the document;
- iv. The author, addressee, and any other recipient(s) of the document; and
- v. The basis on which you contend you are entitled to withhold the document.

J. If you assert that any document sought by any request is protected against disclosure as the attorney's work product doctrine or by the attorney-client privilege, you shall provide the following information with respect to such document:

- a. the name and capacity of the person or persons who prepared the documents;
- b. the name and capacity of all addresses or recipients of the original or copies thereof;
- c. the date, if any, borne by the document;
- d. a brief description of its subject matter and physical size;
- e. the source of the factual information from which such document was prepared; and
- f. the nature of the privilege claimed.

K. You must produce all documents within your case, custody or control that are responsive to any of these requests. A document is within your care, custody or control if you have the right or ability to secure the document or a copy thereof from any other person having physical possession thereof.

L. If you at any time had possession, custody or control of a document called for under this request and if such document has been lost, destroyed, purged, or is not presently in your possession, custody or control, you shall describe the document, the date of its loss, destruction, purge, or separation from possession, custody or control and the circumstances surrounding its loss, destruction, purge, or separation from possession, custody or control.

M. All documents produced pursuant hereto are to be produced as they are kept in the usual course of business and shall be organized and labeled (without permanently marking the item produced) so as to correspond with the categories of each numbered request hereof.

N. When appropriate, the singular form of a word should be interpreted in the plural as may be necessary to bring within the scope hereof any documents which might otherwise be construed to be outside the scope hereof.

O. "«Specific Target»" refers to _____, and includes any corporation owned or controlled by _____, directly or indirectly, or any of their parent, subsidiary and affiliated companies, partnerships, predecessors in interest and all officers, directors, employees, agents, servants and other persons acting or purporting to act on _____'s behalf.

II. **DOCUMENTS REQUESTED:**

Subject to and in accordance with the foregoing, you are directed to produce the following:

1. All documents obtained by you in this litigation through use of subpoenas duces tecum directed at third parties.

2. All documents related to, identified in, or which served as a basis for providing Answers to Interrogatories served upon you concurrent herewith.
3. All documents related to any examination or use by an expert related to the subject in your Complaint.
4. All documents prepared by or for the use of any expert employed by you, for the purpose of testifying in this cause.

EXHIBIT

**Production of Electronically Stored Information (ESI)
FORM OF PRODUCTION**

_____ requests that all ESI (electronically stored information) be produced as single- page Tagged Image File Format (“TIFF “ or “.tiff”) images with accompanying load files as reflected below:

ESI will be produced (printed and loaded) in 300DPI resolution or greater, Group IV Monochrome Tagged Image File Format (.TIFF or .tiff) files in single-page format, with native files and word searchable OCR/extracted text (Optical Character Recognized – i.e. searchable text). Load files will be provided in Summation (.DII) format including an “@Fulltext PAGE or Doc” token for loading of OCR/Extracted text files. The text file containing the OCR/Extracted Text shall be produced in single page format with the name corresponding to its associated image. It should also be in the same folder as the tiff images. Color pages should be produced as color JPEG images.

By agreement, native documents will not be produced for Redacted Documents, which will be produced in 300DPI Group IV Monochrome Tagged Image File Format (.TIFF or .tiff) files without native files or redacted information. Metadata for redacted files shall be produced. Metadata which discloses the content of redacted information may be withheld.

The specs are:

Single page tiff images

Single page text files (preferred), MultiPage text files, also known as “Document level”

Summation load file (.dii)

Metadata text file with the ^ | delimiters, do not use the , ‘ delimiters.

The files should be delivered with the following folder structure:

Images – contains the tiff and txt files, up to 50,000 items.

Data – contains the dii file and the metadata text file

Natives – contains the native files.

In general, Summation accepts images with the following set protocols:

Load requirements for images only:

- Single page Group 4 Tiff files, resolution 300 dpi
- Must use Bates numbers to identify Tiff files names
- Summation Load File requirements:
 - @C ENDDOC# GT000003
 - @T GT000001
 - @D @I\Images\001\GT000001.tif
 - GT000001.txt
 - GT000002.tif
 - GT000003.tif

Load requirements for images with OCR:

- Single page level OCR Text files corresponding to the Tiff file names
- Summation Load File requirements:
 - @FullTEXT Page
@C ENDDOC# GT000003
@T GT000001
@D @I\Images\001\
GT000001.tif
 - GT000001.txt
GT000002.tif
 - GT000001.txt
GT000003.tif
 - GT000001.txt

The following metadata fields will be produced: (Metadata is defined as “unaltered metadata that exists at the time of collection”).

- a. Beg Doc;
- b. End Doc;
- c. Attachment Beg;
- d. Attachment End;
- e. Attachment Range;
- f. Attachment Count;
- g. Author E-mail;
- h. Author Name;
- i. Recipients;
- j. CC;
- k. BCC;
- l. Subject;
- m. Sent Time and Date;
- n. Parent;
- o. File Type (e.g. .xls, .doc., .ppt)
- p. File Name
- q. Custodian
- r. Hidden Cells,
- s. Hidden Text
- t. Create Date,
- u. Last Modification,
- v. Last Access,
- w. Last Save (date and username)
- x. Formulas

For .xls (Excel) file the following additional metadata fields should be included

Number of lines
Number of paragraphs
Number of slides

Number of notes
Number of hidden Slides
Number of multimedia clips
Hyperlink base
Security