UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Stacey Buzay,

Plaintiff,

v.

Edward Jones Mortgage, LLC,
Wells Fargo Bank, N.A., and
Doherty Employment Group, Inc.,

Defendants.

Case Type: Employment

AFFIDAVIT OF MARK LANTERMAN

Court File No. 11-cv-01315 (DSD/JSM)

STATE OF MINNESOTA)
) ss.
COUNTY OF HENNEPIN)

MARK LANTERMAN, being first duly sworn, deposes and says on oath as follows:

1. My name is Mark Lanterman. I am the Chief Technology Officer for Computer Forensic Services, Inc. ("CFS") located in Minnetonka, Minnesota. I submit this affidavit in support of Plaintiff Stacey Buzay's Motion to Compel Electronically-Stored Information and Related Discovery.

QUALIFICATIONS

2. Our firm specializes in the forensic examination of computer data for law enforcement agencies and law firms. Prior to joining CFS, I was a criminal investigator with over eleven years of law enforcement experience. During my last three years in law enforcement I was assigned to the United States Secret Service Electronic Crimes Task Force as its senior computer forensic analyst.

3. In connection with my current and former employment, I have supervised or participated in dozens of search warrant executions for digitally stored (computerized) records and evidence and personally analyzed over 1,500 hard drives. I am certified by the United States Department of Homeland Security as a "Seized Computer Evidence Recovery Specialist," as well as certified in computer forensics by the National White Collar Crime Center. I have conducted seminars and training for the Minnesota State Bar Association, the International Association of Chiefs of Police, the Federal Bureau of Investigation, the United States Secret Service, the New York State Bar, the Minnesota Criminal Justice Institute and the Minnesota Institute for Legal Education. Attached hereto as Exhibit A is a true and correct copy of my current curriculum vitae.

COLLECTION OF ELECTRONICALLY-STORED INFORMATION (ESI)

4. A complete response to discovery requests may require production of ESI in its native form, since computer-generated information (metadata) relating to a relevant document will not be produced by producing a "hard copy" of that document.

5. A complete response to discovery requests may also require a thorough forensic examination of digital media, because not all relevant ESI is active (non-deleted) data.

6. A thorough forensic examination of digital media often requires multiple analysts and may take dozens of human hours. Because of this, computer forensic examinations are most practical if conducted at the expert's home office.

7. The first step generally taken by a trained computer forensic examiner is to create a duplicate copy of an entire drive (the "Forensic Image"). This creates an accurate representation of the device, regardless of file or operating system.

8. The creation of the Forensic Image is recognized by the computer forensic community as the proper way to preserve original electronic evidence. Creation of the Forensic Image does not cause any damage to the computer.

9. The creation of the Forensic Image allows a computer forensic analyst to recreate an entire storage disk and allows him or her to analyze and recover data as if the analyst were working from the original device.

10. Merely turning on a computer will change the state of the evidence by altering critical date stamps and will potentially write over and erase existing files. For this reason, a Forensic Image should be created as soon as any electronic evidence, including relevant computer hard drive(s) and other digital media, has been identified. If relevant digital media are identified and not imaged, and the systems remain in use, data pertinent to an investigation may be overwritten or otherwise destroyed.

11. It is also important to understand that when a user "deletes" files, the files are not necessarily unrecoverable. Until the file is "overwritten" by another file, the "deleted" file is still subject to being recovered. As such, it is essential to preserve all relevant computer hard drives as soon as possible; otherwise, deleted, but relevant, data may be overwritten and destroyed.

12. It is necessary to image and analyze hard drives from any computer which may have accessed relevant data as well as any server hard drives on which the relevant data might be stored to get a complete picture of the data.

13. Should any hard drive imaging be completed by someone not trained in digital evidence preservation, or not be completed in a timely manner, there is the risk of spoliation.

CURRENT DISPUTE

14. I have spoken with Attorney Nicholas May, counsel for Plaintiff Stacey Buzay, regarding his concerns about defendants' production of electronically-stored information in this case.

15. I have reviewed a number of documents, including the following:

a. The complaint, dated May 20, 2011;

b. A letter from Mr. Martin to Mr. May, dated April 30, 2012;

c. The Motion to Compel, dated June 4, 2012.

16. Based on the foregoing, I believe that defendants' production of ESI to date may have been inadequate and its continued adherence to a 30-day "retention" policy may have led to spoliation. However, I cannot draw firm conclusions without being able to conduct my own forensic examination.

17. It may be that certain data was permanently lost. However, it may still be possible to find relevant data, not yet produced. I have recommended to Plaintiff's counsel that the parties adopt the following protocol in order to resolve these questions about the adequacy of defendants' production and to preserve any remaining relevant data.

PROPOSED PROTOCOL

18. I understand that the electronic storage devices subject to analysis in this, or any, case may contain highly personal and confidential information, possibly including proprietary information, attorney-client privileged material, and non-responsive e-mail communications.

19. I am familiar with the practice in litigation of requiring and using protective orders to restrict the disclosure and use of information. I have agreed to be bound by the terms

of any Protective Order in force in this case. I further agree to be bound by any other instructions of the Court.

20. I have designed the following protocol to be used in the production of ESI:

a. We would first identify the relevant computers, servers, hard drives or other devices on which may exists discoverable ESI. A Forensic Image would be made of each relevant computer or server hard drive, or other identified device, either "on site" at the computer's location, or in my offices if the computers were to be sent to me. If conducted on site, I would make every reasonable effort to insure that the Forensic Image would be made at a time that would not be unduly disruptive to any of the participants in this matter.

b. I would prepare, from the Forensic Images and a list of search terms provided by Plaintiffs' counsel, two detailed logs to be provided to counsel for the Defendants and Plaintiffs. The first log would list each relevant document on each hard drive or other device that accessed potentially relevant information with the document's file name; file extension (e.g., whether the document is a word document or e-mail); whether the file has been deleted; the date and time when the file was created, last accessed, and last altered; the size of the file; and the location of the file on the hard drive. This log would capture all potentially relevant documents anywhere on the hard drive. The second log would provide identification of each potentially relevant email and would list who send and receive the email, the date and time, the subject line and the names of any attached files.

c. I would provide the Defendants' counsel with a copy of all relevant documents from the Forensic Images, from which counsel would conduct a privilege review

and determine responsive documents. I would be permitted to discuss with Plaintiff's counsel any technical findings (e.g., evidence of file deletions, altering of documents, etc.) without disclosing to Plaintiff's counsel the body of any communications or documents.

21. This is the same protocol that I developed for use in the 2007 Pioneer Press v. Star Tribune litigation (*Northwest Publications LLC d/b/a St. Paul Pioneer Press v. The Star Tribune Company*, File No. 62-C6-07-003489).

s/ Mark Lanterman
Mark Lanterman

Subscribed and sworn to before me
this 4th day of June, 2012.

_____
Notary Public – Minnesota
My Commission Expires: _____