UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

GENWORTH FINANCIAL WEALTH MANAGEMENT, INC.	:	
Plaintiff,	:	**Civil Action No.**
v.	:	**3:09-cv-1521 (VLB)**
TIMOTHY McMULLAN, JAMES COOK, TIMOTHY McFADDEN, KAREN BAZON, TAMARA RIVERA and TJT CAPITAL GROUP, LLC.	:	
Defendants.	:	
TIMOTHY McMULLAN, JAMES COOK, TIMOTHY McFADDEN, and TJT CAPITAL GROUP, LLC	:	
Third–Party Plaintiffs,	:	
v.	:	
GURINDER AHLUWALIA,	:	
Third-Party Defendant.	:	**June 1, 2010**

MEMORANDUM OF DECISION AND ORDER GRANTING THE PLAINTIFF'S MOTION TO COMPEL DATA PRESERVATION AND FORENSIC IMAGING BY A NEUTRAL COURT-APPOINTED EXPERT, AND FOR SANCTIONS [Doc. #34].

Before the Court is Plaintiff Genworth Financial Wealth Management, Inc. ("Genworth") and Third-Party Defendant Gurinder Ahluwalia's (hereinafter referred to collectively as the "Plaintiff") [Doc. #34] Motion for a court order to compel the Defendants Timothy McMullan, James Cook, Timothy McFadden, Karen Bazon, Tamara Rivera, and TJT Capital Group LLC. ("TJT Capital") to

submit their computers and electronic media devices to forensic mirror imaging and examination by a neutral court-appointed forensic expert. The Plaintiff also seeks a court order for the preservation and production of evidence pursuant to Federal Rule of Civil Procedure 37(a)(5)(A) and Local Rule of Civil Procedure 37(c), and sanctions in the form of reasonable attorneys fees and costs associated with the Plaintiff's motion. [Doc. #34]. For the reasons stated herein the Plaintiff's motion is granted.

I. Background

Genworth initiated this action against the Defendants, former employees who left Genworth between June 29, 2009 and August 4, 2009 to establish TJT Capital, a competing business entity. The Plaintiff alleges that the Defendants requested and received DVD copies of Genworth's Automated Contract Tracking (ACT) database, which contains client names, phone numbers, contact information, portfolio management history, and client notes prior to their staggered departures for the benefit of their company's formation. Genworth alleges that the Defendants used trade secret client information, including information from the ACT database, to solicit hundreds of Genworth's current and former clients in violation of the Computer Fraud and Abuse Act, the Connecticut Uniform Trade Secrets Act, the Stored Communications Act, and Connecticut common law's prohibition of tortious interference with business relationships. [Doc. #1].

The Defendants in turn assert that they identified client information for solicitation through permissible means including internet searches and memory. In August 2009, counsel for Genworth, submitted a letter instructing the Defendants to preserve all electronically stored information (ESI) and other potentially relevant information in anticipation of litigation. [Doc. #35, Exh. A-C]. Genworth subsequently filed suit [Doc. #1] on September 25, 2009, and propounded document requests on November 10, 2009 seeking the production of electronic data and accompanying meta data. The Plaintiff notes that the Defendants failed to produce any e-mail, TJT's Junxure client management database, or Portfolio Center client invoicing database. [Doc. #35, Exh. D]. The Plaintiff sought the Defendants' assurance that forensic imaging had been undertaken, noting concerns that relevant data was at risk of being erased through automatic deletion of temporary and inactive files. [Doc. #35, Exh. F]. The Plaintiff notes that Defendants' counsel conceded that the Defendants had no intention of imaging any of their computer devices. [Doc. #35]. The Plaintiff therefore filed the instant motion on February 5, 2010 [Doc. #34]. In response, the Defendants noted that on February 12, 2010, after the Plaintiff filed its motion, Onsite IT Consulting performed imaging of TJT Financial's computer devices and business laptops used by Defendants McMullen, Cook, and McFadden. [Doc. #42].

On April 8, 2010, and April 12, 2010, the parties participated in a motion and evidentiary hearing during which the Plaintiff presented documentary evidence in

support of its request and Defendant McMullen testified regarding his handling of Genworth client data. [Docs. ##85, 87]. The hearing reflected that the Charles Schwab Corporation ("Schwab"), a custodian of assets for TJT Financial, produced pursuant to subpoena, email correspondence from Defendant McMullen and Cook's personal email account and computer that was not produced as part of the Defendants' response to Genworth's discovery requests. The correspondence reflects the Defendants' submission of Genworth client data and information to Schwab, while still employed by Genworth, as part of efforts to establish TJT Capital and secure Genworth clients for the new entity. [Plaintiff's Demonstrative Exhs. 4-6, 9-10, 12-16]. During the proceeding, Defendant McMullen testified that, prior to the start of the instant litigation, he discarded the personal computer onto which he downloaded ACT client information and from which he conducted correspondence with Schwab in anticipation of his departure from Genworth and the formation of TJT Financial. Testimony further reflected however, that the disposal of the personal computer may have occurred after Genworth submitted letters to the Defendants to preserve all relevant documents in anticipation of litigation.

II. Analysis

In responding to the Plaintiff's motion, the Defendants' acknowledge that

> **Rule 34 and the Comments thereto, together with Rule 26(b)(2)(B), strongly suggest that a court's ruling on such requests is discretionary and should take into account substantive considerations of the burden**

> **and expense of the request. . . . [and that] such relief is entirely within the discretion of the Court to grant or deny.**

[Doc. #42, page 8-9].

The Defendants assert that the Plaintiffs have "not proffered a sufficient basis with which to justify its demands." Id. at Page 9. A party is entitled however, to discover any unprivileged matter that is relevant to a party' s claim or defense, where the discovery "appears reasonably calculated to lead to the discovery of admissible evidence." Fed. R. Civ. P. 26(b)(1). With regard to the discovery of electronically stored information, the Federal Rules of Civil Procedure require a party to "produce and permit the party making the request . . . to inspect, copy, test, or sample any . . . electronically stored information." Fed. R. Civ. P. 34(a). This right to information however, is counterbalanced by a responding party's confidentiality or privacy interests. Notes of Advisory Committee on 2006 Amendments. A party is therefore not entitled to "a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances." Id.

> **In defining the extent of discovery to afford to a party, a court should:**
>
> **consider the relationship between the plaintiff's claims and the defendants' computers and, in some cases, whether the defendant has fully complied with discovery requests, in determining how the requested electronic discovery should proceed. Even in cases where courts have nonetheless adopted procedures to protect privilege and privacy concerns.**

Calyon v. Mizuho Securities USA Inc., No. 07 CIV0224IRODF, 2007 WL 1468889, at *3 (S.D.N.Y., May 18, 2007).

Particularly instructive, is the analysis provided in Ameriwood Industries, Inc. V. Liberman, No. 4:06 CV 524-DJS, 2006 WL 3825291, at *3, *6 (E.D. Mo. Dec. 27, 2006), amended by 2006 WL 685623 (E.D. Mo. Feb. 23, 2007). Similar to the instant proceeding, Ameriwood involved an alleged violation of the Computer Fraud and Abuse Act by several former employees of Ameriwood and their newly formed company for using the plaintiff's computers to download proprietary information and trade secrets to damage the "plaintiff's business relationships and divert [the] business to themselves." Id. at *1, *3. The plaintiff contended that the defendants forwarded trade secret information from Ameriwood's computer server to their personal e-mail accounts while still employed by Ameriwood and noted concern that the defendants may have further transmitted the information to others or deleted the information to conceal unlawful behavior. Id. Accordingly, the plaintiff sought the court to compel the defendants to produce a mirror image of their personal computer hard drives. Noting evidence that the defendants had not produced all responsive documents from their computers, the court observed that "discrepancies or inconsistencies in the responding party's discovery responses may justify a party's request to allow an expert to create and examine a mirror image of a hard drive." Id. at *4. More fully, the district court explained:

> **Courts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature. For example, a party may not inspect the physical hard drives of a computer merely because the**

> **party wants to search for additional documents responsive to the party's document requests. [A court has previously] declined to allow the examination of any ESI other than the information that had been deleted because the requesting party had not demonstrated that the producing party was unwilling to produce relevant evidence. [Evidence] raises the question of whether defendants have in fact produced all documents responsive to plaintiff's discovery requests. Furthermore, in cases where a defendant allegedly used the computer itself to commit the wrong that is the subject of the lawsuit, certain items on the hard drive may be discoverable. Particularly, allegations that a defendant downloaded trade secrets onto a computer provide a sufficient nexus between the plaintiff's claims and the need to obtain a mirror image of the computer's hard drive.**

Id. at *4 (internal citations and quotation marks omitted). The court therefore concluded that because the defendants were accused of using "the computers, which [were] the subject of the discovery request, to secrete and distribute plaintiff's confidential information. How and whether defendants handled those documents and what defendants did with the documents [were] certainly at issue." Id. at *5. The court recognized the defendants' privacy interests but promulgated a three-step imaging, recovery, and disclosure process to provide "sufficient access to information that [was] not reasonably accessible and ensure[] the process d[id] not place an undue burden on the responding party." Id.

The three steps consisted of: 1) an "imagining step" during which the parties selected a computer forensic expert who, operated pursuant to a confidentiality agreement, to inspect, copy, and image the defendants' computer equipment at a mutually agreeable and non-disruptive time, and provided a detailed report of the equipment produced and inspected; 2) a "recovery step,"

during which the expert recovered, from the mirrored images, all available word-processing documents, incoming and outgoing email messages, presentations, and files, including "deleted" files and provided the recovered documents in a reasonably convenient and searchable form to the defendants' counsel, with notice to the plaintiff; and 3) a "disclosure step" during which defendants' counsel examined the records for privilege and responsiveness, to supplement their responses and provided counsel all responsive and non-privileged documents and information, in addition to a privilege log that claimed each privilege expressly and described the "nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, [would] enable other parties to assess the applicability of the privilege or protection." Id. at *5-7.

The facts of this case are analogous to and warrant the remedy fashioned in Ameriwood. The Plaintiff has exhaustively established that forensic imaging by a neutral expert is the only way that the Plaintiff will be able to secure the electronic data to which it is entitled. The Plaintiff presented evidence that Defendant Timothy McMullen, the principal of Defendant TJT, used his personal computer and personal e-mail address to download, access, and transmit the Plaintiff's proprietary information without a scintilla of a reasonable expectation to his entitlement thereto or other legitimate justification therefore. Defendant McMullen, while testifying before this Court, admitted that he spoliated evidence when he discarded a personal computer, on which he admittedly accessed and

transmitted Genworth's proprietary information, in a trash can, hard drive and all. He further testified that he discarded the computer after having been advised by counsel that he had no right to the Genworth data that he had downloaded whille employed by Genworth. The Plaintiff effectively impeached Defendant McMullen's testimony through exhibits and testimony evidencing that he sent emails to Schwab from his personal email account and the personal computer after the date that he testified as having discarded the computer. Defendant McMullen falsely testified before this Court about the handling of at least one of the electronic devices from which the Plaintiff sought ESI production. Even if Defendant McMullen in fact discarded the computer as he claims, the timing of the computer's disposal evidences a consciousness of wrongdoing as to his disclosure of Genworth information.

Furthermore, the Plaintiff has also introduced evidence of the voluminous and detailed nature of the client information at issue, undermining if not rendering utterly incredulous the Defendants' contention that they recalled by memory and discovered through internet searches and other research the detailed client data, including the information that they allegedly conveyed to Schwab in anticipation of their departures. Moreover, the unique and detailed quality of the lists, which include idiosyncratic characteristics of the data undermine any credibility that the Defendants' contentions might have had.

Accordingly, as Genworth has alleged and provided evidence supporting its contention that the Defendants used "the computers, which are the subject of

the discovery request, to secrete and distribute plaintiff's confidential information" there is a sufficient nexus between Genworth's claims and its need to obtain a mirror image of the computer's hard drive, warranting the imaging requested by the Plaintiff. Ameriwood, 2006 WL 3825291, at *4. The Defendant McMullen's admitted spoliation of incriminating evidence and Schwab's disclosure of documents impeaching McMullen's testimony that he discarded the computer lend further support.

The Defendants argue that they should not be required to pay a neutral consultant to image their computers, noting that they have already hired such an expert. The Defendants initially refused to image their computers and only retained a computer consultant to do so after the Plaintiffs' motion for a neutral court-appointed expert was pending before this Court. The Plaintiff filed its motion only after seeking the Defendants' agreement in ensuring forensic imaging of the devices in question. The testimony at the evidentiary hearing however reflects that the Defendants did not exercise diligence in imaging all relevant electronic devices, and instead selectively identified only certain TJT Capital business computers that were not used during the period of misappropriation activity that was alleged to have occurred while the Defendants were still employed by Genworth. The totality of the circumstances under which the Defendants retained a forensic computer expert suggests an end run in furtherance of efforts by the Defendants to deny the discovery to which the Plaintiff is entitled. Moreover, the Defendants' contention that they cannot afford

to pay an expert is belied by their retention of their own expert while the motion for the appointment of a neutral expert for both parties was pending.

In further objection to the appointment of a forensic expert, the Defendants cite expense and the relative financial ability of the parties to pay the cost of such an expert. [Doc. #42]. But yet it is the Defendants' apparent deceit, obstreperousness and destruction of relevant information, that the Defendants were required to maintain and preserve, that necessitates the retention of a neutral forensic computer expert to ascertain what, if any, data existed on any and all computer and electronic storage devices to which the Defendants had access during the relevant period. In light of the Defendants' culpability in necessitating the expense of a neutral expert, the cost for the appointment of a neutral forensic expert is to be borne 80% by the Defendants and 20% by the Plaintiff.

The Court further notes that the Plaintiff's motion for sanctions is warranted by the fact that it had to seek Court orders to obtain that to which it has been entitled but which the Defendants unreasonably and dubiously refused and possibly intentionally made unavailable. The Defendants were wholly unjustified in their position as they tacitly admitted by finally hiring a computer imaging expert. The Defendants have wasted the Plaintiff and the Court's resources in necessitating the judicial resolution of this discovery dispute.

Based on its review of the materials submitted, and testimony at the evidentiary and motion hearing held on April 8 and 12, 2010, and the foregoing

analysis, the Court grants the Plaintiff's motion as follows:

(1) The Court grants the Plaintiff's motion to compel forensic imaging to be performed by a neutral court-appointed expert. The parties are to agree upon a neutral computer forensic expert and confidentiality agreement to govern the expert's handling of the imaged information by June 11, 2010 and submit the identified expert to the Court for approval. If the parties fail to do so, the Court will appoint an expert independently.

(2) The Defendants shall make all responsive computer equipment available, including applicable personal devices to the expert for inspection, copying, and imaging at a mutually agreeable and non-disruptive time, but no later than June, 18, 2010. The Defendants are to provide a detailed report and notice of all equipment produced for inspection by the same date.

(3) The expert is to use the mirrored computer data to recover and organize the mirrored files and information in a reasonable searchable form. The expert shall then provide the recovered data to the Defendants' counsel and contemporaneous notice of this production to the Plaintiff by no later than July 9, 2010.

(4) Defendants' counsel will have until July 30, 2010 to examine the records for privilege and responsiveness, and provide supplementary production of responsive items and a comprehensive privilege log in accordance with Federal Rule of Civil Procedure 26(b)(5)(A).

(5) The cost of the computer forensic expert is to be distributed among the parties in the following proportion: 80% of the cost is to be paid by the Defendants, and 20% is to be paid by the Plaintiff.

(6) As the Court is awarding reasonable attorney's fees and costs, the Plaintiff shall provide a detailed accounting of hours and costs associated with seeking this motion by June 15, 2010.

(7) The Defendants shall meet their data preservation and production obligations and will face further sanction for failure to comply with such requirements.

IT IS SO ORDERED

Signed this 1st day of June, 2010.

_____/s/_____
Hon. Vanessa L. Bryant
United States District Judge