

Acton Law Partners LLP 101 Centerpoint Drive Suite 105 Middletown, CT 06457

T 860,724,2160 F 860,724,2161 actoriaw.com



VIA HAND DELIVERY

May 30, 2013

Danny Seigle FindTheBest.com, Inc. 101 Innovation Place, # A Santa Barbara, California 93108

c/o Thomas N. Harding Seed Mackall LLP 1332 Anacapa St., Suite 200 Santa Barbara, CA 93101

RE: Lumen View Technology LLC v. FindTheBest.com, Inc., S.D.N.Y.

Dear Mr. Seigle:

This firm represents Lumen View Technology LLC ("Plaintiff") in connection with U.S. Patent Number 8,069,073, entitled "System and Method for Facilitating Bilateral and Multilateral Decision- Making" ("the '073 Patent"). We write to you as Director of Operations for FindTheBest.com, Inc. ("Company") regarding Company's unlicensed use of subject matter covered by the claims of the '073 Patent.

Based on our examination, Company's AssistMc feature meets one or more claims of the '073 Patent, as more fully described in the Complaint attached hereto which already has been filed against Company in the United States District Court for the Southern District of New York (the "Suit"), and that Company has directed this infringing activity to residents in the State of New York.

A service copy of the Complaint is attached. The Complaint has been filed and served on the Company's New York registered agent listed above. Please note that a response to the Complaint ("Response") must be filed within twenty-one (21) days from the date of service or a default judgment may be entered against the Company.

If Company is interested in avoiding the need for filing responsive pleadings, you must contact us (prior to the due date of Company's Response) to discuss license terms. To facilitate such discussions, please be prepared to discuss the extent of the

Company's use of and revenues generated from the features described in the Complaint.

While it is Plaintiff's desire that the parties amicably resolve this matter, please be advised that Plaintiff is prepared for full-scale litigation to enforce its rights. This includes all motion practice as well as protracted discovery.

Should Company engage in early motion practice, however, we must advise that it will force us to reevaluate and likely increase Plaintiff's settlement demand. Please be advised that for each nondispositive motion filed by Company, Plaintiff will incorporate an escalator into its settlement demand to cover the costs of its opposition papers and argument.

Preservation Request

Please allow this correspondence to also serve as our request for preservation of evidence to include all documents, tangible things and electronically stored information ("ESI") potentially relevant to the issues in this case. As used in this Preservation Notice, "you" and "your" refers to Company, and its predecessors, successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, partners, agents, attorneys, employees 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 computer systems or other media and devices (including personal digital assistants, smart phones, BlackBerry, iPhone, voice messaging systems, online repositories and cell phones).

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 (c.g., email, voicemail, instant messaging);
- Word processed documents (e.g., Word documents and drafts);
- Spreadsheets and tables (e.g., Excel worksheets);
- Accounting application data (e.g., Quickbooks, 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);
- Databases (c.g., Access, Oracle, SQL, SAP);
- Contact and relationship management data (e.g., Outlook, ACT);
- Calendar and diary application data (e.g., Outlook PST, Gmail, blogs);

- Online access data (e.g., temporary internet files, history, cookies);
- Network access and server activity logs;
- Project management application data;
- Computer aided design; and
- Backup and archival files (e.g., ZIP and .GHO)

ESI resides not only in areas of electronic, magnetic or optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obliged to preserve potentially relevant evidence from both of 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. You will be asked in this litigation to 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 order production of ESI even if it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive Plaintiff of its right to secure this evidence or request that the court order it to be produced.

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, from six (6) years prior to the date of the filing of the Suit up to the present time, and ongoing, in any way relating to the products implicated by the '073 Patent.

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 protocol suited to protection of ESI. You should be advised that sources of ESI that are altered and erased may very well be detectable and subject you to sanctions. You should also be advised that sources of ESI are altered and erased by continued use of your computers and other devices.

Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Suspension of Routine Destruction

We request that you 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 this litigation hold. Your failure to do so is gross negligence. 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 email repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding backup media;
- Reassigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs affecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata or stripper utilities;
- Disabling server or IM logging; and
- Executing drive or file defragmentation or compression programs.

Obligation to Guard Against Deletion

It should be anticipated that your employees, officers or others may seek to hide, destroy or alter ESI and you should act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, it should be anticipated that users may seek to delete or destroy information unrelated to the Suit that they regard as personal, confidential or embarrassing and, in doing so, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees or officers. It is 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.

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. With respect to local hard drives, a method of protecting existing data on local hard drives is through the creation and authentication of a forensically qualified image of the sectors of the drive.

With respect to specific ESI in relevant to the Suit, we understand that Your employees may have frequently used computers and smart phones. We also understand that employees regularly communicate via email. You should take affirmative steps to prevent anyone with access to these systems from seeking to modify, destroy, or delete any ESI contained on their laptops, PCs, or personal smart phones.

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange) or networked storage (often called a user's network share), the complete contents of each user's network share and email accounts should also be preserved.

To the extent that officers, board members or employees have sent or received potentially relevant emails or created potentially relevant documents away from the office, you must preserve the content of the systems, devices and media used for these purposes. Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as Gmail) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes should be preserved.

Agents 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, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation.

System Sequestration

We suggest that with respect to certain individuals with significant knowledge of Company's products implicated by the '073 Patent, that you remove their ESI systems, media and devices from service to properly sequester and protect them. This may be the most appropriate and cost effective preservation step to ensure non-destruction of ESI.

We are available to discuss reasonable preservation steps of ESI in your possession, custody or control. However, you should not defer preservation steps pending such discussion because ESI may be lost or corrupted as a consequence of delay.

Should your failure to preserve potentially relevant ESI result in the loss, corruption or inability to produce evidence in this matter, such failure may constitute spoliation

of evidence and we will not hesitate to seek sanctions, court costs, or an independent action for spoliation where appropriate.

Thank you for your attention to this matter. We look forward to hearing from you as soon as possible.

Very truly yours,

of Aeton Law Partners

Attachments