IT IS HEREBY ORDERED that, subject to the limitations identified in this Order, Plaintiff shall produce copies of "relevant documents," as that phrase is defined below, from:

1. the private email account of Plaintiff, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,
2. the Facebook account of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, and
3. the iPhone of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

The phrase "relevant documents," as used in this Order, is as stated in <INSERT JURISDICTION>. "Relevant documents" includes documents and information authored or received by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ which are relevant to the subject matter involved in the pending action, including information reasonably calculated to lead to the discovery of admissible evidence.

IT IS FURTHER ORDERED that the Court adopts the date range and keywords identified on Exhibit A which is attached to this Order. The date range and keywords shall be utilized as the scope of the permitted search of any electronic data. Plaintiff's counsel may rely upon <INSERT JURISDICTION> with respect to privileged documents that are produced.

IT IS FURTHER ORDERED that Plaintiff's counsel, or a representative, shall deliver the <INSERT COMPUTER AND/OR SMARTPHONE> (identified in John Smith deposition on page 26 and 27 on January 27, 2012), (“Laptop and Iphone”) to the computer forensic company HaystackID Consulting, in <INSERT SPECIFIC ADDRESS>. Defendants' counsel shall provide HaystackID with a copy of this Order before the laptop is produced and HaystackID must agree in writing to be bound by this Order. HaystackID will then create a forensic image of the Laptop and iPhone to a newly purchased hard drive. A second forensic image of the laptop will be created as a backup immediately following the creation of the first forensic image. The Laptop and iPhone will then be returned Plaintiff's counsel, or a representative. The electronic data on that Laptop and iPhone must be maintained until further order of the Court. HaystackID shall not alter the contents of the Laptop or iPhone in any way. A third working copy of the forensic image of the Laptop hard drive and iPhone contents will then be created and examined by the technicians at HaystackID with its contents identified and categorized.

In order to reduce review costs by all parties, prior to the application of the stipulated keyword filters, HaystackID Consulting will apply industry standard file filters to the files contained within the forensic image copy of the laptop using a list provided by the National Software Reference Library (“NSRL”) in order to remove known system and application files from search results. According to the NSRL, “In most cases, NSRL file data is used to eliminate known files, such as operating system and application files, during criminal forensic investigations. This reduces the number of files which must be manually examined and thus increases the efficiency of the investigation.” (<http://www.nsrl.nist.gov/new.html>). This filtering process is commonly known as “De-NISTing”.

After the identification of known system and application files, HaystackID will identify loose files and email file attachments that do not have searchable text such as PDF and other image files. HaystackID will use a process known as Optical Character Recognition (“OCR”) to make image files that do not have searchable text full-text searchable. Once the OCR process is complete, HaystackID will apply the stipulated keywords to the remaining files, thus identifying a group of documents that are keyword responsive. HaystackID will then process for review all of the keyword responsive collection including documents that are the parents or children documents of the keyword responsive collection of documents. For example, if one of the stipulated keywords is present in a Word file attachment to an email, then HaystackID will include both the parent email as well as the child Word file attachment in the collection to be reviewed by Plaintiff’s counsel. The keyword collection will be processed to industry standard Single Page TIFF images, extracted metadata (e.g. Email Sent Date, Email Subject) and searchable text. HaystackID will load the processed keyword collection TIFF images and related searchable data to HaystackID’s Relativity hosted review platform.

HaystackID will apply the keyword filters to the evidence extracted from the iPhone and upload the keyword filtered evidence to HaystackID’s Relativity hosted platform for review by Plaintiff’s counsel.

Plaintiff’s counsel will be provided with one user account to access HaystackID’s Relativity hosted review platform. A HaystackID project manager will meet with Plaintiff’s counsel to determine and create document tags such as “Responsive”, “Non-responsive”, “Requires Redaction”, “Privileged” within Relativity to facilitate Plaintiff’s counsel’s document review. Documents that are tagged by Plaintiff’s counsel as “Responsive” will have all necessary redactions and designations electronically applied by HaystackID to create a production set of documents. The Plaintiff’s counsel approved production set will include the endorsed images as well as searchable text files and metadata such as “To”, “From” “CC”, “Email Subject”, “File Name” and will be provided by HaystackID to Defendant’s counsel.

At Plaintiff’s counsel’s direction, HaystackID will create a privilege log of documents tagged as “Privileged” including such information as the privileged documents’ privilege claim, author, subject line, and other necessary metadata. Plaintiff’s counsel will provide the privilege log to Defendant’s counsel via email or registered mail. If Defendant’s counsel chooses to dispute the privilege claim for one or more of the documents listed in the privilege log, Plaintiff’s counsel will provide the privilege log in addition to a copy of the disputed document to the Court for further disposition.

Plaintiff’s counsel will be provided with a user access log from Relativity showing all user accounts that accessed the Relativity database to insure that only plaintiff counsel approved user accounts did in fact access the database.

IT IS FURTHER ORDERED that HaystackID, at the direction of Defendant’s counsel, will perform an analysis of the Laptop and iPhone using the forensic images to report on such activities as web browsing history, searches performed, file copying and deletion, and the execution dates and times of programs installed on the laptop. Reports generated by HaystackID will be loaded to Plaintiff’s counsel Relativity database for responsiveness and privilege determination. Elements of HaystackID’s report deemed non-responsive or privileged by Plaintiff’s counsel will be redacted using the Relativity redaction tool. HaystackID will provide a copy of the redacted report(s) to Defendant’s one Plaintiff’s counsel has completed their review. If Defendant’s counsel challenges one or more of the redactions to a report, then HaystackID will provide the court with a version of the report minus the challenged redactions for further disposition.

IT IS FURTHER ORDERED that Plaintiff’s counsel, with the guidance of HaystackID, will download \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_’s Facebook profile to a HaystackID server. HaystackID will convert the downloaded Facebook data to a Relativity friendly format and upload that data to Relativity. Documents that are tagged by Plaintiff’s counsel as “Responsive” will have all necessary redactions and designations electronically applied by HaystackID to create a production set of documents.

At Plaintiff’s counsel’s direction, HaystackID will create a privilege log of Facebook documents tagged as “Privileged” including such information as the privileged documents’ privilege claim, author, subject line, and other necessary metadata. Plaintiff’s counsel will provide the privilege log to Defendant’s counsel via email or registered mail. If Defendant’s counsel chooses to dispute the privilege claim for one or more of the documents listed in the privilege log, Plaintiff’s counsel will provide a copy of the disputed document to the Court for further disposition.

 Pursuant to <INSERT JURISDICTION> the cost of the hard drive imaging, examination, reporting, project management, processing, hosting, production set creation, testimony and all billable activities perform by HaystackID, shall be paid by the Defendants.

Plaintiff's counsel may rely upon <INSERT JURISDICTION> with respect to privileged documents that are inadvertently produced.

IT IS FURTHER ORDERED that any data that exists but does not fall within the scope of this Order for production as identified above by the keywords need not be produced. However, that electronic data must be maintained so that if a dispute arises at a later point in time about whether that data should or should not be produced in accordance with <INSERT JURISDICTION>, the preserved data can be identified.

Dated: \_\_\_\_\_\_\_\_ , 201\_

Hon. \_\_\_\_\_\_\_\_\_\_\_ Circuit Court Judge

AGREED AS TO FORM ONLY:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Attorney for Plaintiff

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Attorneys for Defendants

EXHIBIT A:

Date Range:

\_\_\_\_/\_\_/\_\_\_\_ through \_\_\_\_/\_\_/\_\_\_\_

Keywords: