

Direct Dial: 1.561.847.2346

Email: [ddominguez@mcdonaldhopkins.com](mailto:ddominguez@mcdonaldhopkins.com)

August 29, 2018

**VIA XXXXXXXXXX**

Opposing Party

Address

Email

**RE: CASE NAME**

***Mandatory Litigation Hold / Spoliation Letter***

Dear XXXXX:

Please allow this Mandatory Litigation Hold / Spoliation Letter to both introduce myself as counsel for CLIENT (“Our Client”) and to put OPPOSING PARTY on notice to comply with the following litigation hold requests or risk claims of spoliation and other sanctions. As explained more fully below, **you must immediately cease and automatic deletion policies and any manual deletion of evidence.**

This Firm represents Our Client relative to its claims and/or defenses arising from or relating to the following summary of facts (this is not an exclusive list and should be read broadly as there may be facts and circumstances currently unknown to Our Client but known to third parties and/or you): XXXXXXX (“Matter”).

Please be advised that Our Client hereby notifies you, your attorneys, insurers, affiliates, and persons or entity in privity with you, which includes but is not limited to your officers, directors, employees, agents, subsidiaries, affiliates, vendors, and any third parties (collectively, “You”) **to preserve and retain all evidence arising from or relating to this Matter (as described in detail below).**

**Preservation Requires Your Immediate Intervention**

You must act immediately to preserve potentially relevant ESI including, without limitation, information with the earlier of a Created or Last Modified on or after January 1, 2015 through the present.

***Please note that you have an obligation under Florida Rules of Civil Procedure 1.280, 1.350, and 1.380 and Rule 34 of the Federal Rules of Civil Procedure to preserve any and all evidence that could be relevant to, or reasonably calculated to lead to, the discovery of admissible evidence, including those stored in electronic form.*** Nothing in this demand for preservation of evidence should be understood to diminish Your obligation(s) to preserve documents, tangible things, and all other potentially relevant evidence **no matter the form or location**.

Evidence includes any and all relevant, or potentially relevant, Documents, and Electronically Stored Information (“ESI”). The term, Documents, which includes ESI, refers to originals, copies, and drafts of any written, graphic, or otherwise-recorded material. You are required to preserve all relevant paper and electronic documents and data (in their original / native format), including, but not limited to:

**Electronic files.** Retain all relevant electronic files, including active files, archived files, deleted data which is currently recoverable and legacy data, including:

* **Digital Communication** (e.g., electronic mail, facsimiles, chats, texts/Instant Messages, .MSG, and .PST files)
* **Word Processing Documents** (e.g., MS Word, .doc, .docx files)
* **Digital Documents**(e.g., Adobe Acrobat PDF files)
* **Still and Moving Image Files** (e.g., .TIF, .JPG, .GIF, .AVI, .MP4, and .MOV files)
* **Models, Diagrams, Presentations** (e.g., PowerPoint, Sway, and Visio)
* **Legacy Data** (e.g., date created on old or obsolete hardware or software)
* **Social Media** (e.g., Facebook, Twitter, Instagram, Pinterest, Snapchat)

**Paper copies of files.** Preserve all paper copies of files, presentations, calendars, diaries, notebooks, binders, handwritten notes and other physical paperwork related to this matter, even if duplicate copies may exist in electronic format.

**Other materials.** Relevant information is not always presented as a document, such as:

* + - * **Other Digital Communications** (e.g., Voicemail)
      * **Contact and Relationship Management Data** (e.g., Outlook, LotusNotes)
      * **Calendar and Diary Application Data** (e.g. Outlook or Google Calendar)
      * **Spreadsheets and Tables** (e.g., MS Excel, .xslm, .csv files)
      * **Software Applications and Data** (e.g., QuickBooks and WorkForce)
      * **Sound Recordings** (e.g., WAV and .MP3 files)
      * **Databases** (e.g., MS Access, Oracle, .ODB, .DCB files)
      * **Network Access and Server Activity Logs** (e.g., Windows 7/8/10 and server log files)
      * **Internet and/or Web Activity Data** (e.g. temporary Internet files, caches, cookies, and history including but not limited to such content from Explorer, Chrome, and/or Edge)

**Subsequently created documents.** Until informed otherwise, your duty to preserve relevant information is ongoing. Be sure to preserve all relevant documents that are composed or received after your receipt of this letter.

**Electronic Hardware and Software.** Maintain a copy of hardware and software needed to view relevant electronic files, including:

* Encryption and De-Encryption Systems
* Compression and Decompression Software
* Credentials Associated with Relevant User Accounts
* If hardware containing relevant information is replaced or becomes outdated, retain the relevant hardware so that relevant data still may be accessed.

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond what is visible on a printed document. Therefore, even where a paper copy exists, we will seek all documents in their electronic form along with their associated metadata. We will also seek paper documents that contain unique information that was added after the documents were printed (e.g. handwriting, signatures, marginalia, drawings, annotations, highlighting and redactions).

Please be further advised that the specific data or information identified in the following list must be preserved: **[LIST RELEVANT CATEGORIES OF DOCUMENTS and OTHER RECORDS]**

**Your obligation to preserve and retain all evidence, in any from, extends to the following persons:**

**All employees who may possess, have access to, or control evidence, including:**

* Executives and their Assistants;
* Directors, Officers and Agents
* Employees (Permanent and Temporary) in relevant business units;
* Records Department Personnel;
* IT personnel; and
* Other Employees, vendors, agents, parties in privity, or others who may deal with or handle Your document retention or storage of documents or data (including former employees' files).

**All affected third parties who may possess or have access to evidence, including:**

* Former Employees;
* All Parent Companies, Affiliates and Subsidiaries
* Consultants and Professionals (e.g., Attorneys, Accountants)
* Collaborative Software Providers (e.g., Box, Slack);
* Storage Providers: Cloud, Offsite, etc. (e.g., Google Drive, DropBox, iCloud, Iron Mountain)

**Suspension of Routine (and other) Destruction**

**And Your Duty to Guard Against Deletion**

You are directed to immediately initiate a litigation hold for potentially relevant evidence (including but not limited to ESI, Documents and tangible things) and to act diligently and in good faith to secure and audit compliance with such litigation hold.

As a result of this obligation to ensure preservation and retention of all evidence by You, a preservation order (or litigation hold) should be issued by You immediately suspending Your document retention policy and halting the destruction of all relevant documents, or documents reasonably calculated to lead to, the discovery of admissible evidence, whether electronic or not.

**Examples of such features and operations include but are not limited to**:

* + 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;
  + Encrypting files or drives;
  + Rotating or re-using backup tapes or drives;
  + Disabling Windows, server, or IM logging; and
  + Executing drive or file defragmentation or compression programs

You should anticipate that Your officers, directors, employees, agents, or others may seek to hide, destroy, or alter evidence (including ESI) and You must 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 evidence (including ESI). This concern is not one unique to You or your employees and officers. It is simply an event that occurs with such regularity in electronic discovery efforts that any custodian of evidence (including ESI) and their counsel are obliged to anticipate and guard against its occurrence.

**Please forward a copy of this letter to all persons and entities with custodial responsibility for the items referenced in this letter.**

**You should preserve all ESI in its native format (the form in which it is ordinarily accessed and maintained).** You should refrain from any actions which make reasonably accessible ESI less accessible or unavailable.

**In responding to this letter, please retain the following:**

Any and all files and records over which you have control that pertain to the subject matter of this Notice in the following locations:

* File Drawers
* Desk and Office Drawers
* Employees' Personal Devices (e.g., Home Computers, Cell Phones, and Tablet Devices)
* Your employees/personnel’s Google Drive, Drop Box, or other locations where they have kept and/or used Your data
* Personal Files at Home (Hard Copy and Electronic)
* Office Computers and Laptops
  + Active E-mails
  + E-mails in Folders
  + Attachments to E-mails
  + Documents on Hard Drives
  + Portable Storage Devices (e.g., Thumb Drives, CDs, External Drives)
* Servers (e.g., Onsite, Remote, and Internet-based)
* Employees’ Workstations
* Hard Drives
* Shared Drives
* Proprietary Databases
* Company Intranet
* Social Media Platforms (e.g., Facebook, Twitter, Pinterest, Instagram, Snapchat)
* Digital Workspaces (e.g. Slack)
* Archive Media (e.g., Backup Tapes, Backup Disks)
* In order to show preservation compliance, You must maintain a log, documenting all alterations or deletions made to any electronic data storage device or any electronic data processing system. The log should include changes and deletions made by supervisors, employees, contractors, vendors, or any other third parties. This should include documentation of chain of custody.

***Failure to abide by this request could result in sanctions and/or other extreme penalties against You and could form the basis of a legal claim for spoliation against You.***

Compliance with this letter and Your preservation obligations includes forwarding a copy of this letter to all individuals or organizations that are responsible for any of the items referred to in this letter.

Please confirm that You are in receipt of this letter, that You have taken steps to preserve all relevant evidence, including the specific items identified above, and that any document destruction is suspended. If any portion of this letter or any term used in it is unclear, please let me know.

Sincerely,

Christopher B. Hopkins

Christopher B. Hopkins