LAW OFFICES OF
FRIEDMAN & ABRAHAMSEN

Tor J. Friedman
Eric Abrahamsen
Tiffany R. Cruz
Catherine Harrington

403 East Park Avenue
Tallahassee, Florida 32301

Telephone: (850) 681-3540
Facsimile: (850) 270-6927

December 6, 2017

VIA E-MAIL
Senate President Joe Negron
Office of the Florida Senate
404 S. Monroe Street
Tallahassee, Florida 32399-1100
Negron.joe@flsenate.gov

RE: Rachel Perrin Rogers – NOTICE OF DEMAND FOR EVIDENCE PRESERVATION

Dear President Negron:

Please regard this letter as my request that you preserve documents, tangible things, and electronically stored information potentially relevant to the issues relating to claims which may be brought against the Florida Senate and Senator Jack Latvala. This letter is being sent in anticipation of litigation under related to violations of Title VII of the Civil Rights Act of 1964, Chapter 760, Florida Statutes, and other statutes related to such violations and the concomitant conduct which my firm has been retained to investigate. As used in this document, "you" and "your" refers to the you in your individual capacity and the individuals referenced above, their predecessors, successors, parents, subsidiaries, divisions, and affiliates as defined under Florida common law, and their respective officers, directors, agents, attorneys, accountants, employees, partners and other persons occupying similar positions or performing similar functions.

You should anticipate that much of the information subject to disclosure or responsive to potential discovery in this matter is stored on your current and former computer systems and other media and devices (including cell phones, voice-messaging systems, online repositories and personal digital assistants). Electronically stored information (hereinafter "ESI") should be afforded the broadest possible meaning and includes, by way of example and not as an exclusive list, potentially relevant information electronically, magnetically, optically, or otherwise stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- E-Mail Server Stores (e.g., Lotus Domino .NSF or Microsoft Exchange .EDB);
- Word processed documents (e.g., Word or WordPerfect files and drafts);
- Spreadsheets and tables (e.g., Excel or Apple Numbers worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data);
- 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 files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, blog entries);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files;
- Backup and Archival Files (e.g., Veritas, Zip, .GHO);
- Phone Messages; and
- Text Messages

ESI resides not only in areas of electronic, magnetic, and 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 sources of ESI, even if you do not anticipate producing such ESI.

Preservation Requires Immediate Intervention

You should act immediately to preserve potentially relevant ESI including, but not limited to, information with a Created or Last Modified date on or after the earlier of January 1, 2010 through the present date. Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must intervene to prevent loss due to routine operations or malfeasance and employ proper techniques and protocols to preserve ESI. Booting a drive, examining its contents, or running any application may irretrievably alter the evidence it contains and constitute unlawful spoliation of evidence, as such, preservation of potentially relevant information requires your immediate attention and action.

Nothing in this request for preservation of ESI should be understood to diminish your concurrent obligation to preserve documents, tangible things, and other potentially relevant evidence. Moreover, this request to preserve information for this litigation is both retroactive and prospective in application, which means that it extends to all documents, tangible things, and electronically stored information that currently exist relating to this anticipated litigation, as well as all documents, tangible things, and electronically stored information that are created in the future during the course of litigation.

Suspension of Routine Destruction

You are requested to 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 such litigation hold. You are further requested 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 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 backup 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;
- Disabling server, packet, or local instant messaging logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion

You should anticipate that your officers, employees, or others may seek to hide, destroy or alter ESI. Especially where state computers were 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 doing so, they may also delete or destroy potentially relevant ESI. These activities are not unique to you. This is simply conduct that occurs with such regularity that any custodian of ESI and their counsel must anticipate its occurrence. You should act to prevent and guard against such actions.

Act to Prevent Spoliation

You should take affirmative steps to prevent anyone with access to your data, systems, and archives from seeking to modify, destroy, or hide ESI on network or local hard drives and on other media or devices (such as by deleting or overwriting files; using data shredding and overwriting applications; defragmentation, re-imaging, damaging, or replacing media; encryption; or compression).

Preservation of Backup Tapes

You are requested to preserve complete backup tape sets (including differentials and incrementals) containing ESI related to this action.

Forensically Sound Imaging

To limit the threat of spoliation and data loss, we request that you employ forensically sound ESI preservation methods to create an image of the systems, media, and devices of any person that has or had the ability to create, read, update, or delete ESI relevant to this matter. Forensically sound ESI preservation means duplication of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including deleted evidence within "unallocated clusters" and "slack space."

Be advised that a conventional copy, backup, or "Ghosting" of a hard drive does not produce a forensically sound image because it only captures active, unlocked data files and fails to preserve other forensically significant data (e.g., data existing in unallocated clusters and slack space).

You should anticipate that ESI will be sought in the form or forms in which it is ordinarily maintained (i.e., native form). The forensically sound image described above will preserve ESI in such native form. You should not employ methods to preserve ESI that remove or degrade the ability to search the ESI by electronic means or that make it difficult or burdensome to access or use the information. You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files, but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields. Metadata may be overwritten or corrupted by careless handling or improper preservation, including by moving, copying or examining the contents of files.

Servers

With respect to servers used to manage e-mail (e.g., Microsoft Exchange, Lotus Domino) and network storage (often called a "network share"), the complete contents of each user's network share and e-mail account should be preserved if that user has potential relevance to this matter. There are several ways to preserve the contents of a server. If you are uncertain whether the preservation method you plan to employ is one that we will accept as sufficient, please immediately contact the undersigned.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems or devices may contain potentially relevant data. To the extent that you have sent or received potentially relevant emails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CDR/DVD-R disks, and the user's smart phone, voice mailbox, or other forms of ESI storage.). Similarly, if you used online or browser-based e-mail accounts or services (such as

Gmail, Outlook, or Yahoo Mail) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted, and Archived Message folders) should be preserved.

Ancillary Preservation

You should preserve documents and other tangible items that may be required to access, interpret, or search potentially relevant ESI, including but not limited to logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, and user ID and password rosters. You should preserve passwords, keys, and other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals, and license keys for applications required to access the ESI. You should preserve cabling, drivers, and hardware, other than a standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives, and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

As hard copies do not preserve electronic search ability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys, 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 should notify any current or former agent, attorney, employee, custodian, and contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you should take reasonable steps to secure their compliance.

Do Not Delay Preservation

I am available to discuss reasonable preservation steps. However, you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss, or delay in production of evidence to which we are entitled, such failure could constitute spoliation of evidence, and we will not hesitate to seek the appropriate remedy.

Confirmation of Compliance

To ensure that appropriate preservation measures are implemented, we request that a copy of this letter with specific instructions from you be promptly provided to each employee, agent, attorney, consultant, or representative who may have relevant materials and that each recipient acknowledge receipt and understanding of your instructions. Please confirm by December 15, 2017 that you have taken the steps outlined in this letter to preserve ESI and

tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Sincerely,

Tiffany R. Cruz

Tiffany R. Cruz, Esq.