

CARUSO & CARUSO, LLP

ATTORNEYS AND COUNSELLORS AT LAW

68 MAIN STREET

ANDOVER, MASSACHUSETTS 01810

TELEPHONE: (978) 475-2200

FACSIMILE: (978) 475-1001

PETER J. CARUSO
pcaruso@carusoandcaruso.com

PETER J. CARUSO II*
pcarusoii@carusoandcaruso.com

*Also admitted in New Hampshire

PARALEGAL

KAREN M. BONFIM
kbonfim@carusoandcaruso.com

May 11, 2020

James McCarty, Council Chair
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Steven J. Saba, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Jessica L. Finocchiaro, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Joel P. Faretra, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Allison Mary Saffie
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Mike Simard, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

David D.J. Beauregard, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Nicholas DiZoglio, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

Eunice D. Zeigler, Councilor
Searles Building, Room 310
41 Pleasant Street
Methuen, MA 01844

RE: Joseph Solomon, Gregory Gallant, and Joseph Aiello
Demand for Preservation of Electronically Stored Information

Dear Councilors:

Our office represents members of the Methuen Police Superior Officers Association (MPSOA), including without limitation, Greg Gallant, and Joseph Aiello, as well as Joseph Solomon (our "Clients").

We are investigating allegations of: (i) libel and defamation, (ii) invasion of privacy, (iii) intentional infliction of emotional distress, and (iv) doxing ("Claims"), directly related to the actions of several Councilors, both in their official capacities, as well as their capacities as private citizens and other third party individuals. As used in this document, "you" and "your" refers to the City Council, its members, and its predecessors, successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

We hereby demand that you preserve all documents, tangible things, and electronically stored information potentially relevant to our Clients' potential Claims. We believe that much of the information subject to disclosure or responsive to discovery in this matter is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones). You are directed to immediately initiate a litigation hold for potentially relevant ESI (defined below), documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold.

Electronically Stored Information Definition

Electronically stored information (hereinafter "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exhaustive or exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., e-mail, voice mail, text, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables;
- 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;
- Contact and Relationship Management Data;
- Calendar and Diary Application Data (e.g., Outlook blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint,);
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and
- Back Up and Archival Files (e.g., Zip, .GHO)

ESI may be located 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 under an obligation to preserve potentially relevant evidence from all sources of ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to amendments to the Federal Rules of Civil Procedure you must 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 then order production of the ESI, even if it finds that it is not reasonably accessible. As a result, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive our Clients of their right to secure the evidence or the Court of its right to adjudicate the issue.

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information with the earlier of a Created or Last Modified date on or after December 31, 2018 through the date of this demand and concerning:

- The potential Claims;
- The negotiation of the new MPSOA contract and any comments related to our Clients' and their job performance;
- Communications to, from, and/or between City Councilors and to or from any other third parties to City Councilors related to our Clients;
- Communications to or from Methuen Confidential blog/website (methuenconfidential.notepin.co) related to our Clients;
- Communications to or from City Councilors and methuenconfidential@protonmail.com
- Social Media posts concerning our Clients and the Methuen police department; and
- ESI you may use to support claims or defenses related to the Claims.

You must not only refrain 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 protocols suited to protection of ESI. Booting a drive, examining its contents or running any application could irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. 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

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 text and/or 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;
- Disabling server or IM logging; and
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion

You should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and 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 ESI. You are obliged to anticipate and guard against its occurrence.

Metadata

You may also 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.

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 may contain potentially relevant data. To the extent that officers, board members or employees have sent or received potentially relevant e-mails 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, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as AOL, Gmail, Yahoo Mail or the like) 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 must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like.

You must preserve any passwords, keys or 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 must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or 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 searchability 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

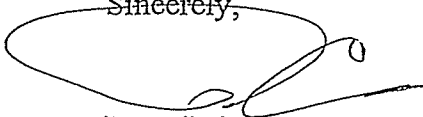
Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

Confirmation of Compliance

Please confirm 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 ESI and evidence.

Should you have any questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Caruso, Sr.", with a large, stylized loop at the end.

Peter J. Caruso, Sr.

Cc: City Solicitor's Office
Mayor's Office