APPLETON REISS
ATTORNEYS AT LAW APPLETONREISS.COM

ERIC N. APPLETON, ESQ.
215 N. Howard Ave. Ste. 200, Tampa, FL 33606
Office: 813.542.8888 | Direct: 813.542.5028
appletonreiss.com | eappleton@appletonreiss.com

February 28, 2023

VIA FEDERAL EXPRESS

Comite Politico PC, Inc.
Attention: Haber Blank, LLP
888 S. Andrews Ave.
Suite 201
Ft. Lauderdale, FL 33316

Re: DEMAND FOR PRESERVATION OF ELECTRONICALLY STORED INFORMATION AND OTHER INFORMATION

Appleton Reiss Clients: South Neighborhood Association, Inc. and Harbour Island Community Services Association, Inc.
Appleton Reiss File No.: 2018-201.1

Dear Comite Politico PC, Inc.:

I write as counsel for South Neighborhood Association, Inc. ("SNA") and Harbour Island Community Services Association, Inc. ("HICSA") to advise you of potential claims for damages and other relief against Comite Politico PC, Inc., among others, concerning and related to the publication of the attached documentation (hereinafter "Claims"). The Claims include potential causes of action for defamation and libel related to the attached documentation, which falsely and maliciously suggests that persons and/or organizations, including SNA and HICSA, bribed a public official as part of their opposition to the construction of a failed hotel project on Harbour Island. As you know, the failed hotel project in question was rejected by City of Tampa officials based upon very sound legal reasons. You are also aware that nothing improper was done by SNA or HICSA as part of their efforts to oppose the failed hotel project.

Under the circumstances, SNA and HICSA demand that you preserve documents, tangible things, and electronically stored information potentially relevant to the Claims. As used in this document, "you" and "your" refers to Comite Politico PC, Inc. and its predecessors, successors, parents, subsidiaries, divisions and affiliates, officers, directors, agents, attorneys, accountants, employees, partners, assigns, customers, clients, and other persons occupying similar positions or performing similar functions.

You must anticipate that information responsive to discovery resides on your current and former computer systems, phones and tablets, in online repositories and on other storage media and sources (including voice and video recording systems, Cloud services and social networking accounts).

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 and on:

- Digital communications (e.g., e-mail, voice mail, text messaging, WhatsApp, SIM cards)
- E-Mail Servers (e.g., Microsoft 365, Gmail, and Microsoft Exchange databases)
- Word processed documents (e.g., Microsoft Word, Apple Pages or Google Docs files and drafts)
- Spreadsheets and tables (e.g., Microsoft Excel, Google Sheets, Apple Numbers)
- Presentations (e.g., Microsoft PowerPoint, Apple Keynote, Prezi)
- Social Networking Sites (e.g., Facebook, Twitter, Instagram, LinkedIn, Reddit, Slack, TikTok)
- Online ("Cloud") Repositories (e.g., Drive, OneDrive, Box, Dropbox, AWS, Azure)
- Databases (e.g., Access, Oracle, SQL Server data, SAP)
- Backup and Archival Files (e.g., Veritas, Zip, Acronis, Carbonite)
- Contact and Customer Relationship Management Data (e.g., Salesforce, Outlook, MS Dynamics)
- Online Banking, Credit Card, Retail and other Relevant Account Records
- Accounting Application Data (e.g., QuickBooks, NetSuite, Sage)
- Image and Facsimile Files (e.g., .PDF, .TIFF, .PNG, .JPG, .GIF., HEIC images)
- Sound Recordings (e.g., .WAV and .MP3 files)
- Video and Animation (e.g., Security camera footage, .AVI, .MOV, .MP4 files)
- Calendar, Journaling and Diary Application Data (e.g., Outlook PST, Google Calendar, blog posts)
- Project Management Application Data
- Internet of Things (IoT) Devices and Apps (e.g., Amazon Echo/Alexa, Google Home, Fitbit)
- Computer Aided Design/Drawing Files
- Online Access Data (e.g., Temporary Internet Files, Web cache, Google History, Cookies)
- Network Access and Server Activity Logs

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 or intend to claim it is confidential or privileged from disclosure.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to the 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 order production of the ESI, even if it is not reasonably accessible. Accordingly, you must preserve ESI that you deem inaccessible so as not to preempt the court's authority or destroy evidence.

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 February 28, 2018, through the date of this demand and continuing thereafter, concerning the Claims.

Adequate preservation of ESI requires more than simply refraining from efforts to delete, destroy or dispose of such evidence. You must intervene to prevent loss due to routine operations or active deletion by employing proper techniques and protocols to preserve ESI. Many routine activities serve to irretrievably alter evidence and constitute unlawful spoliation of evidence.

Preservation Requires Action

Nothing in this demand for preservation of ESI should be read to limit or diminish your concurrent common law and statutory obligations to preserve documents, tangible things and other potentially relevant evidence.

Suspension of Routine Destruction

You are directed 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 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 may include:

- Purging the contents of e-mail and messaging repositories by age, quota, 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 "cleaner" or other programs effecting wholesale metadata alteration
- Releasing or purging online storage repositories or non-renewal of online accounts
- Using metadata stripper utilities
- Disabling server, packet, or local instant messaging logging
- Executing drive or file defragmentation, encryption, or compression programs

Guard Against Deletion

You should anticipate the potential that your officers, employees, or others may seek to hide, destroy or alter ESI. You must act to prevent and guard against such actions. Especially where company machines 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, incriminating or embarrassing, and in so doing, they may also delete or destroy potentially relevant ESI. This concern is not unique to you. It is simply conduct that occurs with such regularity that any custodian of ESI and their counsel must anticipate and guard against its occurrence.

Preservation of Backup Media

You are directed to preserve complete backup media sets (including differentials and incremental backups) that may contain communications or evidence of ESI concerning or related to the Claims.

Act to Prevent Spoliation

You should take affirmative steps to prevent anyone with access to your data, systems, accounts and archives from seeking to modify, destroy or hide potentially relevant ESI wherever it resides (such as by deleting or overwriting files, using data shredding and erasure applications, re-imaging, damaging or replacing media, encryption, compression, steganography or the like).

System Sequestration or Forensically Sound Imaging

As an appropriate and cost-effective means of preservation, you should remove from service and securely sequester the systems, media, and devices housing potentially relevant ESI concerning or related to the Claims. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically significant areas of the media, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

Preservation in Native Forms

You should anticipate that ESI, including but not limited to e-mail, documents, spreadsheets, presentations, and databases, will be sought in the form or forms in which it is ordinarily maintained (i.e., native form). Accordingly, you should preserve ESI in such native forms, and 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 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. 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, tracked changes, speaker notes, 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 header fields.

Metadata may be overwritten or corrupted by careless handling or improper preservation, including by carelessly copying, forwarding, or opening files.

Servers

With respect to servers used to manage e-mail (e.g., Microsoft 365, Microsoft Exchange, Lotus Domino) and network storage (often called a "network share"), the complete contents of each relevant custodian's network share and e-mail account should be preserved. There are several cost-effective ways to preserve the contents of a server without disrupting operations. If you are uncertain whether the preservation method you plan to employ is one that we will deem sufficient, please contact the undersigned.

Home Systems, Laptops, Phones, Tablets, Online Accounts, Messaging Accounts and Other ESI Sources

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 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 external storage drives, thumb drives, CD- R/DVD-R disks and the user's phone, tablet, voice mailbox or other forms of ESI storage.). Similarly, if you used online or browser-based e-mail and messaging accounts or services (such as Gmail, Yahoo Mail, Microsoft 365, Apple Messaging, WhatsApp or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes and messages 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 manuals, schema, 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 and the like.

You must 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. If needed to access or interpret media on which ESI is stored, you must also preserve cabling, drivers, and hardware. This includes tape drives, readers, DBMS, other legacy or proprietary devices and mechanisms.

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 and 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.

Preservation Protocols

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol if you will furnish an inventory and description of the systems and media to be preserved. Alternatively, if you promptly disclose the preservation protocol you intend to employ, we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics so that our experts may work cooperatively to secure a balance between evidence preservation and burden that is fair to both sides and acceptable to the courts.

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 because of delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss, or delay in production of evidence to which SNA and HICSA are entitled, such failure would constitute spoliation of evidence, and this firm's clients will not hesitate to seek sanctions and damages when appropriate.

Confirmation of Compliance

Please confirm by March 6, 2023, 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 in writing to this firm what you have done to preserve potentially relevant evidence and what you will not do. Absent a response, we will rely upon you to complete the preservation sought herein.

Sincerely,

Eric N. Appleton, Esq.
For the Firm

ENA
Enclosure
cc: Clients

LYING LYNN HURTAK

BOUGHT AND PAID FOR

LYING LYNN HURTAK: AT LEAST SHE'S CONSISTENT

Lying Lynn says she's for transparency, but she secretly meets with lobbyists and rubber stamps their socialist agenda.

Lying Lynn claims to be a "big fiscal government watchdog", but one of her first acts as councilwoman was a vote to raise her salary by 42%.

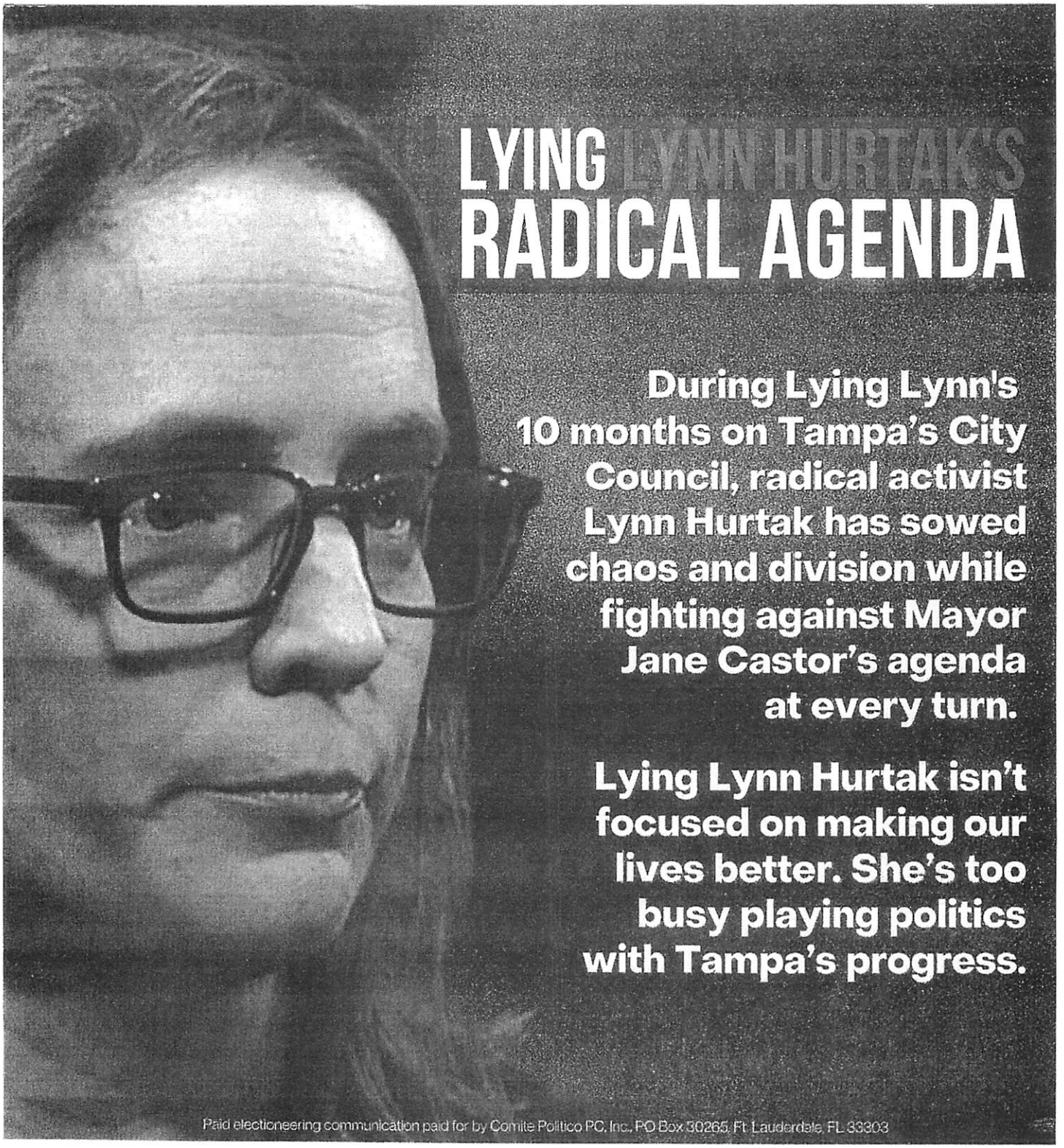
Lying Lynn says she's a fighter for women's rights, but she supports a candidate accused of workplace sexual harassment that cost taxpayers $200k to settle.

Lying Lynn says she works as a consultant for international developments, but will not list her clients or report them on her tax returns and financial disclosures.

Lying Lynn voted to support a massive hotel development then switched her vote after she was paid off by the opposition.

WE CAN'T LET LYING LYNN HURTAK STOP TAMPA'S PROGRESS

CHECK THE FACTS: *WUSF Public Media*, August 22, 2022; *City of Tampa*, Lobbyist Registration; *Tampa Bay Times*, September 22, 2022; WFLA News Channel 8, May 18, 2022; Florida Division of Elections Financial Disclosures; Fox News 13 Tampa Bay, May 13, 2022



PO Box 30265
Ft. Lauderdale, FL 33303

PRSRT STD
U.S. POSTAGE
PAID
TAMPA, FL
PERMIT NO 100