SCHUMACHER PC

1901 1st Avenue, First Floor
San Diego, California 92101

Tel.: (619) 344-0800
Email: zach@schumacher-law.com

February 17, 2023

Via Email and Regular U.S. Mail

Nathan Fletcher, Chair of the Board
Jeff Stumbo, Chief Human Resources Officer
SAN DIEGO METROPOLITAN TRANSIT SYSTEM
1255 Imperial Avenue, Suite 1000
San Diego CA 92101-7490
nathan.fletcher@sdcounty.ca.gov
jeff.stumbo@sdmts.com

Re: Demand for Employment Records and Evidence Preservation
Grecia Figueroa v. San Diego Metropolitan Transit System, et al.

Please be advised, this office has been retained by YOUR former employee, Grecia Figueroa ("MS. FIGUEROA"), to represent her legal interests with regard to what we believe are unlawful employment practices committed by San Diego Metropolitan Transit System ("MTS"); Chair of the MTS Board, Nathan Fletcher; and, potentially, other related entities or individuals (hereinafter collectively, "EMPLOYER", "YOU", or "YOUR").

DEMAND FOR EMPLOYMENT RECORDS

Pursuant to Labor Code § 432, we demand that MTS produce to this office, no later than thirty (30) calendar days from this written request, all writings (see Evidence Code § 250) signed by MS. FIGUEROA related to the obtaining or holding of her employment.

Pursuant to Labor Code § 1198.5, we demand that MTS produce to this office, no later than thirty (30) calendar days from this written request, all documents comprising MS. FIGUEROA's personnel file.

Pursuant to Labor Code § 226 (c), we demand that MTS produce to this office, no later than twenty-one (21) calendar days from this written request, all records specified by Labor Code § 226 (b).

DEMAND FOR PRESERVATION OF EVIDENCE

This communication is made in a good-faith anticipation of litigation. (See Civil Code § 47, Briggs v. Eden Council for Hope and Opportunity (1999) 19 Cal.4th 1106, 1115; Digerati Holdings, LLC v. Young Money Entertainment, LLC (2011) 194 Cal.App.4th 873, 887; Malin v. Singer (2014) 228 Cal.App.4th 35.)

YOU have a duty to preserve evidence which is relevant to MS. FIGUEROA's anticipated lawsuit, even without a court order. (See Code of Civil Procedure § 2023.010, et seq.; Ellis v. Toshiba America Information Systems, Inc. (2013) 218 Cal.App.4th 853, 862; Cedars-Sinai Med.Ctr. v. Sup.Ct. (Bowyer) (1998) 18 Cal. 4th 1, 12; Williams v. Russ (2008) 167 Cal.App.4th 1215, 1227.) Because YOUR obligation to preserve some types of evidence (particularly electronic evidence) may be complicated and/or highly technical in nature, we strongly urge YOU to immediately share this demand for preservation of evidence with YOUR legal counsel, YOUR IT department (or YOUR outside IT consultant), and YOUR human resources department so that they can take charge of and ensure YOUR compliance with YOUR preservation obligations.

As used in this demand for preservation of evidence, the terms "YOU" and "YOUR" refers to Nathan Fletcher, an individual, and to MTS and each of its predecessors, successors, parents, subsidiaries, sister companies, divisions and affiliates, and each of their respective owners, partners, officers, directors, executives, managing agents, agents, attorneys, accountants, employees, and other persons occupying similar positions or performing similar functions.

As explained in more detail below, the purpose of this letter is to respectfully request that YOU take immediate, diligent and comprehensive steps to:

(1) Preserve all documents, tangible things, and electronically stored information potentially relevant to:

- MS. FIGUEROA;
- MS. FIGUEROA's employment;
- YOUR interactions with MS. FIGUEROA – including but not limited to interactions outside of the workplace;
- The termination of MS. FIGUEROA's employment;

- Complaints made by any other person at MTS about gender discrimination or sexual harassment;
- Any investigation or other action that YOU took as a result of any person's complaints of gender discrimination or sexual harassment at MTS;
- Complaints made by any other person at MTS about retaliation for reporting gender discrimination or sexual harassment;
- Any investigation or other action that YOU took as a result of any person's complaints about retaliation for reporting gender discrimination or sexual harassment at MTS;
- MS. FIGUEROA's potential legal claims, including allegations that YOU: (1) discriminated against MS. FIGUEROA; (2) sexually harassed MS. FIGUEROA; (3) sexually assaulted MS. FIGUEROA; and (4) retaliated against MS. FIGUEROA because she complained or otherwise protested against sexual harassment that was perpetrated against her; and
- YOUR defenses to MS. FIGUEROA's potential legal claims.

(2) Stop any and all of YOUR processes/policies/practices that would otherwise call for the affirmative or passive destruction of evidence (including the suspension of any so-called "document retention" policies/procedures/practices that would otherwise call for the destruction of documents and other evidence); and

(3) Stop any messaging and email programs or apps that utilize "disappearing" messages/emails (also known as secret messages/emails) and/or messages/emails that are revocable by the sender. As YOU may know, certain messaging/email programs (such as WhatsApp, Instagram, Snapchat, Slack, Signal, Wickr, Telegram, Vaporstream, and now Gmail) allow users to send messages/emails that automatically disappear and do not allow the recipient to save, forward, copy or print the message/email. Likewise, some of these messaging/email programs allow the sender to revoke a message/email. By this Evidence Preservation Letter, we are specifically instructing YOU to ensure none of YOUR owners, partners, officers, directors, executives, managing agents, agents, attorneys, accountants, employees, other persons occupying similar positions or performing similar functions, and anyone affiliated with YOU uses such messages or emails to communicate about MS. FIGUEROA, her hiring, her employment, the termination of her employment, her legal claims against YOU, and YOUR legal defenses.

Broadest Possible Definition of The Terms "DOCUMENT" and "DOCUMENTS"

As used in this letter, the terms "DOCUMENT" and "DOCUMENTS" are used in the broadest possible sense and shall mean and include any kind of object and any kind of handwritten, typewritten, printed, electronically stored, or recorded material whatsoever, whether prepared or received by YOU or by any other person, that is in YOUR possession, custody, or control (a DOCUMENT is deemed to be in YOUR control if YOU have the right to obtain the document or a copy thereof from another person or entity).

The words "DOCUMENT" and "DOCUMENTS" include, but are not limited to, any of the following:

1. Notes; memoranda; charges; complaints; claims; affidavits; statements; papers; files; forms; data; tapes; printouts; letters; books; reports; summaries; prescriptions; prognoses; policies; procedures; manuals; handbooks; guides; minutes; logs; certificates; communications; contracts; agreements; telegrams; records; correspondence; diaries; calendars; faxes, diagrams; drawings; microfilms; invoices; bills; and receipts;

2. E-mails; text messages; instant messages; and instant chat (including, without limitation, text messages and voice messages from apps such as WhatsApp, Instagram, Telegram, Zoom, Skype, Viber, WeChat, hike, Line, Kik, pinger, Tango, Twitter DM, Facebook PM, and text+);

3. Information retrievable from Human Resources Management Systems ("HRMS"), Human Resources Information Systems ("HRIS"), Talent Management Systems ("TMS"), Learning Management Systems ("LMS") (including, by way of example only, Paycor Perform, ClearCompany, Zenefits, GoCo.io, Namely, TinyPulse, Adrenalin HRMS, ADP Vantage HCM, SutiHR, SAP Success Factors, NGA Preceda, OpenHR-Advanced Business Solutions, ADP Workforce Now, UltiPro, Gusto, BambooHR, Deputy, Sage Business Cloud People, Kronos Workforce Central, Deputy, Cornerstone, Dayforce HCM, and SAP SuccessFactors);

4. Information retrievable from payroll provider companies (including, by way of example only, ADP, Paychex, Sage Payroll, and Patriot Payroll);

5. Information retrievable from temporary service agencies (including, by way of example only, Robert Half, Kelly Services, Manpower, Adecco, Integrity Staffing Solutions, Spherion, and Atrium);

6. Information retrievable from team collaboration and communication software (including, by way of example only, Slack, Stride, Yammer, Asana, Trello, Basecamp, Azendoo, Bitrix24, eXo Platform, Fleep, Flock, Jostle, Kaleo Software, Moxtra, Rocket.Chat, Ryver, Team Tracker App, Chanty, Glip, Hive, Work Zone, and Cisco Spark);

7. Information retrievable from social media websites and apps (including, by way of example only, Facebook, Instagram, Snapchat, LinkedIn, Google, Twitter, YOUTube, Qzone, Cloob, V Kontakte, and Odnoklassniki);

8. Electronically stored information including, without limitation:

a. Information retrievable from computer/cloud storage and file-synchronization services (including, by way of example only, Dropbox, box, Amazon Cloud, Backblaze, Igneous, Google Drive, Microsoft OneDrive, Microsoft SharePoint, IDrive, SugarSync, SpiderOak ONE, CertainSafe Digital Safety Deposit Box, Apple iCloud Drive, Flickr, Google Photos, Forever, Adobe Revel, and 500 Pixels);

b. Information retrievable from computers, laptops, servers, network drives, CD-ROMs, CDs, DVDs, Blu-ray Discs, USB Flash Drives, external hard drives, Network Attached Storage devices;

c. Information retrievable from YOUR intranet site; and

d. Information retrievable from cell phones, tablets, and personal digital assistants and devices;

9. Photographs; audiotapes (and transcripts of such recordings); videotapes (and transcripts of such recordings); and

10. Any other writing however produced or reproduced or stored.
The words "DOCUMENT" and "DOCUMENTS" include, without limitation, originals, all file or other copies no matter how prepared, and all drafts, preliminary sketches and renderings prepared in connection with such documents whether used or not.

Demand for Preservation of Documents, Tangible Things, and Electronically Stored Information

YOU should anticipate that much of the information that will be subject to disclosure or responsive to discovery should this matter proceed to litigation will consist of electronically stored information (hereinafter "ESI") and is stored on YOUR current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories, cell phones, and tablets) as well as in the cloud via online productivity and business service companies that provide web-conferencing, hosted email and online storage (such as Office 365, G Suite, Outlook, OpenOffice, WPS Office, HyperOffice, Google Drive, OneDrive, M-Files, SharePoint, Zoho Office, SoftMaker Office, LibreOffice, OfficeSuite UC, ThinkFree, Polaris Office, ONLYOffice, and Bdoc Suite).

YOU should afford ESI the broadest possible definition and deem it to include (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (*e.g.,* e-mail, voice mail, instant messaging);
- Word processed documents (*e.g.,* Word or WordPerfect or Google documents and drafts);
- Spreadsheets and tables (*e.g.,* Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- 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, Yahoo, blog tools);
- 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; and,
- Back Up and Archival Files (*e.g.,* Zip, .GHO)

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 these sources of ESI, even if YOU do not anticipate producing such ESI.
The demand that YOU preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to both the California Code of Civil Procedure and the Federal Rules of Civil Procedure, YOU will be required during litigation to 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. Accordingly, even ESI that YOU deem reasonably inaccessible must be preserved in the interim so as not to deprive MS. FIGUEROA of her right to secure the evidence or the Court of its right to adjudicate the issue.

Evidence Preservation Requires Immediate Intervention

YOU must act immediately to preserve potentially relevant evidence (including ESI) including, without limitation, information concerning:

- MS. FIGUEROA;
- MS. FIGUEROA's employment;
- YOUR interactions with MS. FIGUEROA – including but not limited to interactions outside of the workplace;
- The termination of MS. FIGUEROA's employment;
- Complaints made by any other person at MTS about gender discrimination or sexual harassment;
- Any investigation or other action that YOU took as a result of any person's complaints of gender discrimination or sexual harassment at MTS;
- Complaints made by any other person at MTS about retaliation for reporting gender discrimination or sexual harassment;
- Any investigation or other action that YOU took as a result of any person's complaints about retaliation for reporting gender discrimination or sexual harassment at MTS;
- MS. FIGUEROA's potential legal claims, including allegations that YOU: (1) discriminated against MS. FIGUEROA; (2) sexually harassed MS. FIGUEROA; (3) sexually assaulted MS. FIGUEROA; and (4) retaliated against MS. FIGUEROA because she complained or otherwise protested against sexual harassment that was perpetrated against her; and

- YOUR defenses to MS. FIGUEROA's potential legal claims.

Adequate preservation of ESI requires more than simply refraining 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. Be advised that sources of ESI are altered and erased by continued use of YOUR computers and other devices. Booting a drive, examining its contents or running any application will 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. Nothing in this demand for preservation of ESI should be understood to diminish YOUR concurrent obligation to preserve document, 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 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 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 owners, partners, officers, directors, executives, managing agents, agents, attorneys, accountants, employees, and other persons occupying similar positions or performing similar functions may seek to hide, destroy or alter ESI; accordingly, YOU must act to prevent or guard against such actions. Especially where YOUR machines/devices/systems 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. This concern is not one unique to YOU or YOUR owners, partners, officers, directors, executives, managing agents, agents, attorneys, accountants, employees, other persons occupying similar positions or performing similar functions. It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

Additionally, YOU should take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file. With respect to the hard drives and storage devices of each of the persons named below and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by that person during the period from six months prior to the start of MS. FIGUEROA's employment (*i.e.,* six month prior to **June 2019**) up through and including to the present and going forward in time, as well as recording and preserving the system time and date of each such computer:

- Nathan Fletcher
- Jeff Stumbo
- Mark Olson
- Stacie Bishop
- Lucero Sanchez
- Quincy Marin
- Sharon Cooney
- Karen Landers

- Jan Gardetto
- Samantha Leslie
- Toufic Tabshouri
- Larry Marinesi
- Emily Outlaw
- Brendan Shannon
- Art Langit
- Thuy Larkin
- Bree Wilcox

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

Preservation in Native Form

YOU should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, YOU should preserve ESI in such native forms, and YOU should not select methods to preserve ESI that remove or degrade the ability to search YOUR ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

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. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. 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.

Servers

With respect to servers like those used to manage electronic mail (*e.g.,* Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved.

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, partners, shareholders, 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. This would include, without limitation, any and all such documents and other communications prepared, sent or received by:

- Nathan Fletcher
- Jeff Stumbo
- Mark Olson
- Stacie Bishop
- Lucero Sanchez
- Quincy Marin
- Sharon Cooney
- Karen Landers
- Jan Gardetto
- Samantha Leslie
- Toufic Tabshouri
- Larry Marinesi

- Emily Outlaw
- Brendan Shannon
- Art Langit
- Thuy Larkin
- Bree Wilcox

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 must 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.

Do Not Delay Preservation

YOU should not defer preservation steps as 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 would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Please be advised that this letter is not intended to be privileged. We reserve the right to show this letter, as necessary, to a judge, jury, arbitrator or other finder of fact to prove any claim that YOU engaged in the spoliation of evidence.

If YOU have any questions, please do not hesitate to contact me or have YOUR legal counsel contact me.

Very truly,

Zachary S. Schumacher
Attorney for Grecia Figueroa

Cc:
nathan@nathanfletcher.com