SILVERMAN
THOMPSON
Silverman Thompson Slutkin White

ATTORNEYS AT LAW

A Limited Liability Company
400 E. Pratt Street
Suite 900
Baltimore, Maryland 21202
Telephone 410.385.2225
Facsimile 410.547.2432
silvermanthompson.com
Annapolis | Baltimore | Towson | Washington, DC

Writer
Pseidel@silverma

NOTICE AND DEMAND

July 25, 2025

VIA FIRST CLASS MAIL

Nick's Pizza & Subs

RE: Notice of Litigation Hold and Demand for Preservation of Documents and Electronically Stored Information in Your Care, Custody, Control, or Possession, Regarding Matthew Scott Banks Schlegel

Dear Nick's Pizza & Subs:

Please be advised that this firm represents Matthew Schlegel ("Mr. Schlegel") in connection with the potential claims he has against multiple individuals (the "Litigation"). The Litigation arises from the false allegations set forth in the criminal case titled: *State of Maryland v. Matthew Banks Schlegel*; Circuit Court for Anne Arundel County (Case No. C-02-CR-24-000908). You have been identified as a potential witness in the Litigation. The purpose of this correspondence is to notify you of your obligations to preserve documents, tangible, things, and electronically stored information ("ESI") that are potentially relevant to the Litigation and any other related claims. This notice and the obligations herein apply to these claims and any potential related claims; are to be construed in the broadest possible sense permitted by Maryland law and the Maryland Rules of Civil Procedure and are continuing in nature.[1]

[1] Appendix A to this letter provides instructions for downloading information from certain platforms. The platforms included in the appendix are not an exclusive list of the platforms that you are required to search to satisfy your obligation to preserve and retain documents, ESI and data related to the Litigation.

To "preserve" as used in this letter includes, but is not limited to, **NOT** destroying, **NOT** concealing, and **NOT** altering any paper or electronic files and other data generated by and/or stored on your computers and storage media, or any other electronic data including, but not limited to, voice mail, electronic mail and text messages.

As used in this letter, "you" and "your" refers not only to you personally, but also your family members, predecessors, successors, assignees, parents, agents, attorneys, accountants, employers, employees, representatives, or any other person or persons acting on your behalf.

You should anticipate that much of the information subject to disclosure, responsive to discovery (which will be issued in connection with any claim filed), and/or evidence in this matter is stored on your current and former computer systems and other media and devices, including, but limited to personal digital assistants, voice-messaging systems, online repositories, and cell phones.

ESI must be afforded the broadest possible definition. It includes, by way of example and not as an exclusive list, potentially relevant information electronically, magnetically or optically stored as:

- Digital or analog communications, both sent and received, whether internally or externally;
- Digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical, or other storage media, including thumb drives, hard drives, floppy disks used by your computers and their backup media (e.g., other hard drives, backup tapes, floppies, Jaz cartridges, CD-ROMs) or otherwise, whether such files have been reduced to paper printouts or not;
- Word processed documents (e.g., without limitation, Word or WordPerfect documents and drafts), including drafts and revisions;
- Spreadsheets and tables (e.g., without limitation, Excel or Lotus 123 worksheets), including drafts and revisions;
- Accounting Application Data (e.g., without limitation, QuickBooks, Money, Peachtree data files);
- Image and Facsimile files (e.g., without limitation, .pdf, .tiff, .jpg, .gif images);
- Sound recordings (e.g., without limitation, .wav and .mp3 files); video and animation recordings (e.g., without limitation, .avi and .mov files, Zoom recordings);
- Databases (e.g., without limitation, Access, Oracle, SQL, Server data, SAP); Contact and relationship management data (e.g., without limitation, Outlook, ACT!, FUB);
- Calendar, task management, diary application data, and personal information management (e.g., without limitation, Outlook PST, Yahoo!, blog tools, Lotus Notes);
- Online Access Data, including Internet and Web-browser generated history files, caches, temporary internet files, artificial intelligence services, and "cookies" files generated at your workstation or the workstation of any employee or agent working on your behalf and on any and all backup storage media;
- Data created with the use of paper and electronic mail logging and routing software;
- [illegible] slide shows (e.g., without limitation, PowerPoint, Corel

Presentations);

- Network access and server activity logs; project management application data, including graphs, charts and other data;
- Computer aided design/drawing files, including drafts and revisions; and
- Back-up and archival files (e.g., without limitation, Zip, .GHQ).

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 of these sources of ESI, even if you do not anticipate being required to produce such ESI.

The demand that you preserve both accessible and inaccessible ESI relevant to the Litigation is limited, reasonable, and necessary. As you are aware, state and federal laws require that you preserve, and at the appropriate time, produce, all sources of ESI.

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. For example, booting a drive, examining its contents or running any application may irretrievably alter the evidence it contains and may result in the unlawful spoliation of evidence. Therefore, 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 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.

Guard Against Deletion

You should anticipate that you or others acting on your behalf may seek to hide, destroy, or alter ESI and act to prevent or guard against such actions. You should anticipate, especially where devices or machines have been used for Internet access or personal communications, which 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. Certainly, this concern is not one unique to you. It is 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 is occurrence.

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 any ensuing 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 that 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 Data, CC, and BCC fields.

Servers

With respect to servers like those used to manage electronic mail (*e.g.*, without limitation, Microsoft Exchange, Lotus Domino, Google) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account must be preserved. There are several ways to preserve the contents of a server depending upon, *e.g.*, its RAID configuration and whether it can be downloaded or must be online 24/7.

Home Systems, Laptops, Online Accounts and Other ESI Venues

We expect that you will act swiftly to preserve data on office workstations and computers. You should also determine if any home or portable systems may contain potentially relevant data. To the extent that you or anyone acting on your behalf have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from his or her office, you must preserve the contents of these 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 or external hard drives, CD-R disks and other PDA devices, smart phones, voice mailboxes, or other forms of ESI storage). Similarly, if you or anyone acting on your behalf have used online or browser-based email accounts or services (such as Facebook, Twitter, AOL, Gmail, Yahoo Mail, or similar) 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. These documents, whether kept in paper or electronic form, must be preserved, as well as all copies of your backup tapes and the software necessary to reconstruct the data on those tapes so that there can be made a complete bit-by-bit "mirror" evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you that are no longer in service.

You must preserve any passwords, keys, or other authenticators required to access encrypted files or to run applications, along with the installation disks, user manuals, and license keys for applications required to access 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. Tape drives, bar code readers, Zip drives, and other legacy or proprietary devices must be preserved.

Paper Preservation of ESI is Inadequate

Hard (printed or paper) 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 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, consultant, 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.

System Sequestration or Forensically Sound Imaging

With respect to the parties directly managing the access and analysis of data contained in any computer system, removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step. In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the model numbers of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective.

We anticipate the need for forensic examination of one or more of these systems and the presence of relevant evidence in forensically accessible areas of the drives. Therefore, you must employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss. By "forensically sound" we mean duplication, for purposes of preservation, 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 the 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 in the so-called "unallocated clusters," holding deleted files.

Preservation Protocols

We intend to work with you to form an agreement regarding an acceptable protocol for forensically sound preservation. If you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them.

Do Not Delay Preservation

I am available to discuss reasonable preservation steps. You should not, however, defer preservation steps pending our discussions if ESI will be lost or corrupted as a consequence of delay. If the failure to preserve potentially relevant evidence results in the corruption, loss, or delay in the production of evidence potentially relevant to any claim, such failure would constitute spoliation of evidence, for which my client would not hesitate to seek sanctions and appropriate remedies, including application of the adverse inference with regard to issues adversely affected by spoliation.

Please confirm within seven calendar days of the date of this letter that you have taken the steps outlined in this letter to preserve potentially relevant documents, tangible, things, and ESI. I look forward to receiving your call to discuss the matters raised in this notice and demand and appreciate your anticipated cooperation.

If You automatically dispose of or recycle digital or paper files, digital back-up tapes, optical diskettes, or other storage media (possibly pursuant to a document retention policy), please suspend such program for the time being. We can then discuss which information should be retained and preserved throughout the Litigation.

Sincerely,

Patrick R. Seidel

Patrick R. Seidel

APPENDIX A

INSTRUCTIONS FOR DOWNLOADING INFORMATION FROM VARIOUS PLATFORMS

Google (Includes YouTube)

1. Log into your Google account from a computer.
2. Select the "**Data & Privacy**" tab near the top of the page.
3. Scroll down to "**Data from Apps and Services You Use**."
4. Select "**Download Your Data**."
5. All data is automatically selected. Unless told otherwise, do not deselect any data categories.
6. Click "**Next Step**."
7. Under "**Delivery Method**," select "**Send Download Link via Email**" and type in the email you would like the download link sent to.
8. Under "**Frequency**," select "**Export Once**."
9. Under "**File Type & Size**," select "**.zip**" and "**2 GB**."
10. Click "**Create Export**."

Facebook

1. Log into your Facebook profile on a computer.
2. Once logged in, click your profile picture icon in the top right corner of the page.
3. Select "**Settings & Privacy**," then click "**Settings**."
4. In the left column, click "**Your Facebook Information**."
5. Next to "**Download Your Information**," click on "**View**."
6. Next, select "**HTML**" as the format of your download.
7. Unless you are told to do otherwise, select "**All Time**" under the "**Data Range**" dropdown menu.
8. Unless you are told to do otherwise, all data and information should be included in the download.
9. Click "**Request a Download**" at the bottom of the page.
10. Once you receive a notification from Facebook that your download is ready, return to the "**Download Your Information**" section from Step #5.
11. Click on "**Available Files**."
12. Click "**Download**" and enter your password.

Instagram

1. Log into your Instagram account from a computer.
2. Once logged in, click on your profile picture in the top right corner.
3. Click on "(gear wheel) **Settings.**"
4. Click on "**Privacy and Security**."
5. Scroll down to "**Data Download**" and click "**Request Download.**"
6. Enter the email address that you want the file to be sent to.
7. Select "**HTML**" as the download format, then click "**Next**."
8. Enter your Instagram account password, then click "**Request Download.**"
9. You will soon receive an email to the previously entered email from Step #6 titled "**Your**

Instagram Data" with a link to your data.

10. Once received, click "**Download Data**" and follow the instructions provided in the email to finish downloading your information.

Twitter/X

1. Log into your Twitter account from a computer.
2. Select "**More**" in the navigation bar.
3. Select "**Your Account**" to go to your account settings.
4. Click "**Download an Archive of your Data**."
5. Enter your password under "**Download an Archive of your Data**," then click "**Confirm**."
6. Verify your identity by clicking "**Send Code**" to your email address and/or phone number associated with your account.
7. After verifying your identity, click "**Request Data**."
8. Once your data file is ready, Twitter will send an email to your connected email account or send a notification if you have the Twitter App installed on your mobile device.
9. If you receive the data file by email, click the "**Download**" button while logged in to your Twitter account and download the "**.zip**" file of your Twitter archive.
10. If you receive the data file by notification from the mobile app, select "**Settings**" in your mobile app and click "**Download Data**."

Snapchat

1. Log into your Snapchat account from a computer by going to **accounts.snapchat.com**
2. Click "**My Data**."
3. Click "**Submit Request**" at the bottom of the page.
4. Enter a valid email address and Snapchat will send you an email with a link once your data is ready to download.
5. Once you receive the email, click the link to download your data.

TikTok

1. Log into your TikTok account on the mobile app.
2. Click on the **3-line icon** in the top right corner.
3. Select "**Settings and Privacy**."
4. Click on "**Privacy**" and select "**Download your Data**."
5. Select "**TXT**" as the file format.
6. Click on "**Request Data**."
7. Once you receive a notification that your download is ready, return to the screen in Step #4 and select the "**Download data**" tab.
8. Select your data file to download.

VSCO

1. Log into your VSCO account from a computer.
2. If prompted to verify your login, sign onto your account from both a computer ***and*** sign into the same account on your VSCO mobile app. If your account is already verified, skip to Step #6.
3. When you sign into vsco.co in a web browser, this registers as a new desktop/laptop

browser session and you will be sent a verification email to the email associated with your VSCO account. You must verify log in from the email that was sent to you before you can proceed with accessing a copy of your data for your VSCO account, otherwise, you will encounter an error.

4. ****Note to all email users**: check your spam folder if you do not see the verification email in your inbox. Please note it could take between 5-10 minutes for this email verification to arrive in your inbox.
5. Once you receive the verification email, select "**Verify Login**."
6. Once your login has been verified, return to the homepage of your VSCO account on your desktop computer.
7. Select the "**Settings**" icon in the top right corner of the screen.
8. Scroll to the bottom of VSCO account to the "**My VSCO Data**" Section.

iCloud

Drive --> iMac

1. Click the iCloud Drive in the sidebar of any Finder window.
2. Press and hold the "**Option**" key and drag the file to a new location.

Drive --> iPhone, iPad, or iPod Touch

1. Open the Files app and tap "**iCloud Drive**."
2. Tap the folder that you want to open, then tap the file to open it.
3. Tap "**Share (box with 'up' arrow)**" in the lower-left corner.
4. Choose how you want to send a copy of the file.

Drive --> iCloud.com

1. Sign into your iCloud account from a computer.
2. Open your iCloud Drive.
3. Find and select the file.
4. Click "**Download (cloud with 'down' arrow)**" at the top of the page or double-click the file.
5. The document will download to your default download location.

Photos and Videos

On a **mobile Apple device** --> open to Setting app.

1. Tap **[your name]** --> **iCloud Photos**
2. Select "**Download**" and "**Keep Originals**" to import the photos to your computer

On an iMac --> open the Photos app.

1. Select the photos and videos to copy
2. Select **"Choose File"** --> **"Export."**

On a PC --> make sure that you set up iCloud for Windows and turn on iCloud Photos.

1. Open **File Explorer**.
2. In the Navigation pane, click "**iCloud Photos**," then select the images you want to keep on your PC.
3. Click the selection and choose **"Always keep on this device."**
4. After the items download, copy them to another folder on your computer.

5. To do this, press and hold the **Ctrl key and drag the items** to the folder.

Mail

1. On your **iMac** --> Select your iCloud inbox from the list of mailboxes in the sidebar.
2. Choose "**Mailbox**" --> "**Export Mailbox**."
3. Choose a destination folder for the archive.
4. Click "**Choose**" to save the archive file.

Notes

On an iPhone --> open the Notes app and select the note that you want to download.

1. Select the "**. . .**" icon in the top right corner.
2. Select "**Send a Copy**."
3. Save your note to Files for download.

On a Mac --> Open the Notes app on your computer and select the note that you want to download.

1. Click "**File**" --> "**Export as PDF**."
2. Choose where to save the download on your computer.

Voice Memos

1. Open the Voice Memos app on your iPhone or iPad.
2. Tap the recording that you want to download.
3. Tap the "**More . . .**" icon and select "**Duplicate**."
4. You can also tap "**Share**" to send the recording via Messages or Mail or save it to Files.