

Case 8:20-cv-00114-WFJ-SPF Document 10 Filed 03/18/20 Page 1 of 207 PageID 128

UMESH HEENDENIYA,

Plaintiff,

V.

Civil Action No. 8:20-CV-114-T-02SPF

THOMAS MILLER, FBI AGENT ASSIGNED TO THE TAMPA-ORLANDO JOINT TERRORISM TASK FORCE (JTTF); SONYA YONGUE, FBI AGENT ASSIGNED TO THE TAMPA-ORLANDO JTTF; DAVID KORTMAN, HERNANDO COUNTY SHERIFF'S DETECTIVE AND HCSO TASK FORCE OFFICER (TFO) ASSIGNED TO THE TAMPA-ORLANDO JTTF; ALVIN NIENHUIS, HERNANDO COUNTY SHERIFF; HERNANDO COUNTY SHERIFF'S OFFICE (HCSO); PAUL WYSOPAL, FBI SPECIAL AGENT IN CHARGE (SAC) OF THE TAMPA-ORLANDO FIELD OFFICE; REGINA LOMBARDO, BATFE SPECIAL AGENT IN CHARGE (SAC) OF THE TAMPA-ORLANDO FIELD OFFICE; JOHN AND/OR JANE DOES 1-50;

Defendant

Honorable William F. Jung
(U.S. District Judge)

Honorable Sean P. Flynn
(U.S. Magistrate Judge)

**PLAINTIFF HEENDENIYA'S DECLARATION NOTIFYING THE COURT
REGARDING THE 'RELATED CASE ORDER,' THE 'CERTIFICATE OF
INTERESTED PERSONS ORDER,' AND THE 'DEMAND FOR
IMMEDIATE AND/OR CONTINUING EVIDENCE
PRESERVATION' NOTICE SENT TO DEFENDANTS
AND 3RD PARTY WITNESSES.**

STATE OF FLORIDA)
) SS.:
COUNTY OF HERNANDO)

I, Umesh Heendeniya, being a resident of Hernando County, Florida, pursuant to 28 U.S.C. § 1746, declare under the penalties of perjury that the following statements are true and correct except as to the statements which I aver on knowledge, information, or belief formed after reasonable inquiry, and as to them, I believe them to be true:

1. I am the indigent, *pro se* non-attorney, mentally and physically disabled Plaintiff in this case, who has applied to The Court to be granted *in forma pauperis* status.
2. On Jan. 15, 2020, I filed a lawsuit against 3 agents/deputies/troopers/officers of the Tampa-Orlando Joint Terrorism Task Force (JTTF) and the Hernando County Sheriff's Office (henceforth, "HCSO"), in The U.S. District Court for The Middle District of Florida.
3. On Jan. 21, 2020, The Court entered the 'Related Case Order' and the 'Certificate of Interested Persons Order,' which was required to be filled out.
4. On or about Feb. 06, 2020, I filed the completed (i.e., filled out) 'Related Case Order' and the 'Certificate of Interested Persons Order' with The Court.
5. On the same day, I asked for an extension of 2-weeks to serve the 'Related Case Order' and the 'Certificate of Interested Persons Order' on the Defendants, which The Court granted on Feb. 10, 2020.
6. With deep respect to The Court, unfortunately due to financial and other reasons, I was unable to print and serve the 'Related Case Order' and the 'Certificate of Interested Persons Order' on the named Defendants and other potential Defendants within the 2-weeks period.
7. Instead, it took me until early March to print each of the approx. 121-page documents¹ at an office supply store, and then mail each of the documents *via* USPS certified mail, to each of the 8 named Defendants and potential Defendants.
8. In addition to each document containing the filled-out 'Related Case Order' and the 'Certificate of Interested Persons Order,' each document also contained an 'Immediate and/or Continuing Evidence Preservation Demand' letter, and a copy of the 'Suggested Protocol for Discovery of Electronically Stored Information' and a copy of the 'Principles for the Discovery

¹ Henceforth, "documents" or "document."

of Electronically Stored Information in Civil Cases' that had been issued several years ago (as helpful guidance for litigants) by The U.S. District Court for The District of Maryland.

9. Each set of documents that was mailed also contained within each mailing package/packet, a CD-Rom that was protected in a jewel case, that contained an exact copy of that document as an Adobe PDF file. This was done so that each Defendant could e-mail the approx. 121-page PDF document to other persons or entities to whom it might pertain/concern.

10. The 8 (eight) named Defendants and potential Defendants to whom the above described packages/packets were mailed were:

- i. Hon. William P. Barr
Attorney General of the United States of America
U.S. Department of Justice (U.S. DOJ)
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001
- ii. Christopher A. Wray
Director of the FBI
FBI Headquarters
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001
- iii. Regina Lombardo
Acting Director of the ATF
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
99 New York Avenue, NE
Washington, DC 20226
- iv. Megan J. Brennan
Postmaster General of the United States and Chief Executive Officer
United States Postal Service (USPS) and U.S. Postal Inspection Service (USPIS)
Attn: Legal Department
475 L'Enfant Plaza SW
Washington DC 20260-2101
and
U.S. Postal Inspection Service (USPIS)
3400 Lakeside Drive, #6
Miramar
FL - 33027
and

U.S. Postal Inspection Service (USPIS)
25 Dorchester Avenue
Boston
MA – 02205

- v.** Michael F. McPherson
Special Agent-in-Charge (SAC)
Federal Bureau of Investigation (FBI)
Tampa Field Office
5525 West Gray Street
Tampa
FL - 33609
(813)-253-1000
<http://tampa.fbi.gov>
E-mail: michael.mcpherson@ic.fbi.gov
- vi.** Daryl R. McCrary
Special Agent-in-Charge (SAC)
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
Tampa Field Division
400 North Tampa Street, Suite 2100
Tampa, Florida 33602
(813)-202-7300
TampaDiv@atf.gov
E-mail: daryl.mccrary@atf.gov
- vii.** Joseph R. Bonavolonta
Special Agent-in-Charge (SAC)
Federal Bureau of Investigation (FBI)
Boston Field Office
201 Maple Street
Chelsea
MA - 02150
(857)-386-2000
<http://boston.fbi.gov>
E-mail: joseph.bonavolonta@ic.fbi.gov
- viii.** Sheriff Alvin D. Nienhuis
Hernando County Sheriff's Office
18900 Cortez Boulevard
Brooksville
FL - 34601
(352)-754-6830
<https://www.hernandosheriff.org>
E-mail: anienhuis@hernandosheriff.org

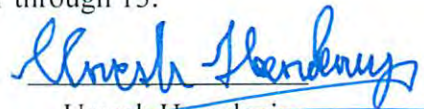
11. Due to the already incurred substantial cost of printing at least 8-sets of the above described approx. 121-page documents at an office supply store and the already incurred cost of mailing, by certified USPS mail, each set of documents (plus a CD-Rom) to each of the 8 named Defendants or potential Defendants, I respectfully state that a hard-copy of the printout (approx. 121-pages) for only Tampa FBI Special Agent-in-Charge Michael F. McPherson is attached herein, as "Exhibit λ."² At the end of that document, a 2-page printout of the USPS tracking information is included showing successful delivery of the packet that was mailed to Tampa FBI Special Agent-in-Charge McPherson.

12. The tracking information for each of the 8 packets that was mailed, was obtained using USPS's mail tracking URL-- https://tools.usps.com/go/TrackConfirmAction_input

13. For the remaining 7 named Defendants or potential Defendants, I respectfully state that due to the cost of printing and mailing, only the first 8-pages of each of the approx. 121-page documents are attached herein, within "Exhibit δ." At the end of each 8-page document, a 2-page printout of the USPS tracking information is included showing successful delivery of each of the 7 packets to each of the 7 named Defendants or potential Defendants.

This concludes my Declaration that contains paragraphs numbered 1 through 13.

Dated: March 17, 2020.
Hernando County,
Florida.


Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com

² Within the attached exhibits are documents from prior filings, where I've had to resort to using A, B, C,... and 1, 2, 3,... and Alpha, Bravo,... as exhibit separators/designators. Thus, to avoid confusion, I have named "Exhibit δ" and "Exhibit λ" as the exhibit separators/designators for the instant Declaration, which consists of 118 sheets of paper.

EXHIBIT δ

EXHIBIT -
121 Page
Document to
Attorney General
of the United
States of America
Hon. William P.
Barr

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Wednesday, March 04, 2020.

United States of America (For purposes of future possible FTCA claims)

Hon. William P. Barr

Attorney General of the United States of America

Any Officials in the U.S. DOJ and/or any Officials in any Agency within the DOJ (i.e., FBI officials, BATFE officials, etc.,) and/or any Civilians¹ who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)

U.S. Department of Justice (U.S. DOJ)

950 Pennsylvania Avenue, NW

Washington, D.C. 20530-0001

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear Attorney General Barr (representing both The United States of America and the U.S. Dept. of Justice), and

Any Officials in the U.S. DOJ and/or any Officials in any Agency within the DOJ (i.e., FBI officials, BATFE officials, etc.,) and/or any Civilians who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and

Any other Officials who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

I'm also submitting an 'Immediate and/or Continuing Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the free Adobe Acrobat Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and to email the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") 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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue

is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I’m 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

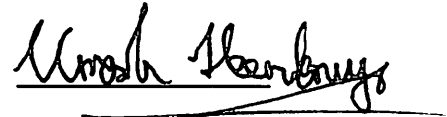
Please confirm within 2-weeks of the date of this notice letter that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Please mail all correspondence to my P. O. Box, which is:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611**

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', written over a horizontal line.

Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com

USPS Tracking®[FAQs >](#)**Track Another Package +****Tracking Number:** 70192970000074717706[Remove X](#)

Your item was delivered at 5:02 am on March 9, 2020 in WASHINGTON, DC 20530.

✓ Delivered

March 9, 2020 at 5:02 am
 Delivered
 WASHINGTON, DC 20530

Get Updates ✓**Text & Email Updates****Tracking History****March 9, 2020, 5:02 am**

Delivered
 WASHINGTON, DC 20530

Your item was delivered at 5:02 am on March 9, 2020 in WASHINGTON, DC 20530.

March 8, 2020, 11:25 am

Available for Pickup
 WASHINGTON, DC 20530

U.S. Postal Service™		CERTIFIED MAIL® RECEIPT	
Domestic Mail Only			
For delivery information, visit our website at www.usps.com ®.			
WASHINGTON, DC 20530			
Certified Mail Fee	\$3.55		
Extra Services & Fees (check box, add fee as appropriate)			
<input type="checkbox"/> Return Receipt (hardcopy)	\$0.00		
<input type="checkbox"/> Return Receipt (electronic)	\$0.00		
<input type="checkbox"/> Certified Mail Restricted Delivery	\$0.00		
<input type="checkbox"/> Adult Signature Required	\$0.00		
<input type="checkbox"/> Adult Signature Restricted Delivery	\$0.00		
Postage	\$8.25		
Total Postage and Fees	\$11.80		
Sent To		Hon. William Barr	
Street and Apt. No., or PO Box No.			
City, State, ZIP+4®		Washington, DC 20530	
PS Form 3800, April 2015 PSN 7530-02-000-9047		See Reverse for Instructions	

7019 2970 0000 7471 7706

0131
MAR 05 2020
Postmark Here
SPRING HILL, FL
03/05/2020

March 8, 2020, 10:14 am

Arrived at Hub

WASHINGTON, DC 20018

March 8, 2020, 4:35 am

Departed USPS Regional Facility

WASHINGTON DC DISTRIBUTION CENTER

March 7, 2020, 10:26 pm

Arrived at USPS Regional Facility

WASHINGTON DC DISTRIBUTION CENTER

March 7, 2020, 2:00 am

Departed USPS Regional Facility

YBOR CITY FL DISTRIBUTION CENTER

March 6, 2020, 9:10 pm

Arrived at USPS Regional Origin Facility

YBOR CITY FL DISTRIBUTION CENTER

March 6, 2020

In Transit to Next Facility

March 5, 2020, 7:02 pm

USPS in possession of item

SPRING HILL, FL 34606

Feedback

Product Information



See Less

EXHIBIT -
121 Page
Document to
Director of the FBI
Christopher A.
Wray

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Friday, February 28, 2020.

Christopher A. Wray
Director of the Federal Bureau of Investigation (FBI)
Any other Agents/Deputies/Troopers/Officers or Civilians¹, who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)
FBI Headquarters
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear FBI Director Wray,
Any other Officials or Civilians, who were/are involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and
Any other Officials or Civilians, who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

I'm also submitting an 'Immediate Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the Adobe Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") 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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I’m 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

Please confirm within 2-weeks of the date of this notice letter 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.

Please mail all correspondence to my P. O. Box, which is:

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', written over a horizontal line.

~~Umesh Heendeniya~~
umeshheendeniyavsthefbi@gmail.com

USPS Tracking®

[FAQs >](#)[Track Another Package +](#)**Tracking Number:** 70040750000303211281[Remove X](#)

Your item was delivered at 5:14 am on March 3, 2020 in WASHINGTON, DC 20535.

✓ Delivered

March 3, 2020 at 5:14 am
 Delivered
 WASHINGTON, DC 20535

[Get Updates ✓](#)[Text & Email Updates](#)

Tracking History

March 3, 2020, 5:14 am

Delivered

WASHINGTON, DC 20535

Your item was delivered at 5:14 am on March 3, 2020 in WASHINGTON, DC 20535.

March 2, 2020, 10:28 am

Available for Pickup

WASHINGTON, DC 20535

U.S. Postal Service™	
CERTIFIED MAIL™ RECEIPT	
(Domestic Mail Only; No Insurance Coverage Provided)	
For delivery information visit our website at www.usps.com	
WASHINGTON, DC 20535	
OFFICIAL USE	
Postage	\$3.55
Certified Fee	\$0.00
Return Receipt Fee (Endorsement Required)	\$0.00
Restricted Delivery Fee (Endorsement Required)	\$0.00
Total Postage & Fees	\$11.80
Sent To Christopher Wray Street, Apt. No., or PO Box No. FBI Director City, State, ZIP+4 Washington, D.C. 20535	
PS Form 3800, June 2002 See Reverse for Instructions	

March 2, 2020, 10:00 am

Arrived at Unit

WASHINGTON, DC 20018

March 2, 2020, 3:41 am

Arrived at USPS Regional Destination Facility

WASHINGTON DC DISTRIBUTION CENTER

March 1, 2020, 3:14 am

Arrived at USPS Regional Origin Facility

YBOR CITY FL DISTRIBUTION CENTER

February 29, 2020, 9:29 pm

Departed Post Office

TAMPA, FL 33630

February 29, 2020, 7:23 pm

USPS in possession of item

TAMPA, FL 33630

Feedback

Product Information



See Less ^

Can't find what you're looking for?

Go to our FAQs section to find answers to your tracking questions.

FAQs

EXHIBIT -
121 Page
Document to
Acting Director of
the ATF
Regina Lombardo

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Friday, February 28, 2020.

Regina Lombardo

Acting Director of the ATF

Any other Agents/Deputies/Troopers/Officers or Civilians¹, who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
99 New York Avenue, NE
Washington, DC 20226

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear ATF Director Lombardo,

Any other Officials or Civilians, who were/are involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and

Any other Officials or Civilians, who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

I'm also submitting an 'Immediate Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the Adobe Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") 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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I’m 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

Please confirm within 2-weeks of the date of this notice letter 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.

Please mail all correspondence to my P. O. Box, which is:

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', written over a horizontal line.

Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com

USPS Tracking®[FAQs >](#)**Track Another Package +****Tracking Number:** 70040750000303211298[Remove X](#)

Your item was delivered at 5:21 am on March 3, 2020 in WASHINGTON, DC 20226.

✓ Delivered

March 3, 2020 at 5:21 am
 Delivered
 WASHINGTON, DC 20226

Get Updates ✓**Text & Email Updates****Tracking History****March 3, 2020, 5:21 am**

Delivered
 WASHINGTON, DC 20226

Your item was delivered at 5:21 am on March 3, 2020 in WASHINGTON, DC 20226.

March 2, 2020, 10:30 am

Available for Pickup
 WASHINGTON, DC 20226

U.S. Postal Service™	
CERTIFIED MAIL™ RECEIPT	
(Domestic Mail Only; No Insurance Coverage Provided)	
For delivery information visit our website at www.usps.com	
WASHINGTON, DC 20226	
OFFICIAL USE	
Postage	\$3.55
Certified Fee	\$0.00
Return Receipt Fee (Endorsement Required)	\$0.00
Restricted Delivery Fee (Endorsement Required)	\$0.00
Total Postage & Fees	\$3.55
	\$11.00
Sent To <i>Regina Lombardo</i>	
Street, Apt. No., or PO Box No. <i>Acting Director, ATF</i>	
City, State, ZIP+4 <i>Washington, D.C. 20226</i>	
PS Form 3800, June 2002 See Reverse for Instructions	

7004 0750 0003 0321 1298

FL 3363 8606 69

02/29/2020

March 2, 2020, 9:38 am

Arrived at Unit

WASHINGTON, DC 20018

March 2, 2020, 3:42 am

Arrived at USPS Regional Destination Facility

WASHINGTON DC DISTRIBUTION CENTER

March 1, 2020, 3:13 am

Arrived at USPS Regional Origin Facility

YBOR CITY FL DISTRIBUTION CENTER

February 29, 2020, 9:29 pm

Departed Post Office

TAMPA, FL 33630

February 29, 2020, 7:23 pm

USPS in possession of item

TAMPA, FL 33630

Feedback

Product Information



See Less ^

Can't find what you're looking for?

Go to our FAQs section to find answers to your tracking questions.

FAQs

EXHIBIT -

121 Page

Document to

Postmaster General of

the United States, and

USPS and USPIS

Chief Executive Officer

Megan J. Brennan

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Wednesday, March 04, 2020.

Megan J. Brennan
Postmaster General of the United States and Chief Executive Officer
United States Postal Service (USPS) and U.S. Postal Inspection Service (USPIS)
Attn: Legal Department
475 L'Enfant Plaza SW
Washington DC 20260-2101

and
U.S. Postal Inspection Service (USPIS)
3400 Lakeside Drive, #6
Miramar
FL - 33027

and
U.S. Postal Inspection Service (USPIS)
25 Dorchester Avenue
Boston
MA – 02205

and
Any Officials in the USPS and/or any Officials in the USPIS and/or any Civilians¹ who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya and his mail, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear Postmaster General and Chief Executive Brennan, and
Any Officials in the USPS and/or any Officials in the USPIS and/or any Civilians who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya and his mail, and

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

Any other Officials who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

I'm also submitting an 'Immediate and/or Continuing Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the free Adobe Acrobat Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and to email the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") must also intervene to prevent loss

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic

evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I'm 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

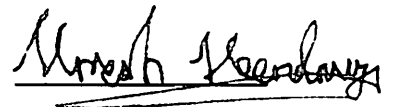
Please confirm within 2-weeks of the date of this notice letter that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Please mail all correspondence to my P. O. Box, which is:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611**

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', with a horizontal line drawn underneath it.

Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com


[FAQs >](#)
[Track Another Package +](#)
Tracking Number: 70192970000074717683

[Remove X](#)

Your item was delivered to the front desk, reception area, or mail room at 10:24 am on March 9, 2020 in WASHINGTON, DC 20260.

✓ Delivered

March 9, 2020 at 10:24 am
Delivered, Front Desk/Reception/Mail Room
WASHINGTON, DC 20260

[Get Updates ✓](#)
[Text & Email Updates](#)
[Tracking History](#)

March 9, 2020, 10:24 am

Delivered, Front Desk/Reception/Mail Room
WASHINGTON, DC 20260

Your item was delivered to the front desk, reception area, or mail room at 10:24 am on March 9, 2020 in WASHINGTON, DC 20260.

March 8, 2020, 11:15 am

Available for Pickup
WASHINGTON, DC 20260

U.S. Postal Service™ CERTIFIED MAIL® RECEIPT Domestic Mail Only	
For delivery information, visit our website at www.usps.com ®.	
WASHINGTON, DC 20260	
Certified Mail Fee	\$3.55
Extra Services & Fees (check box, add fee appropriate)	\$0.00
<input type="checkbox"/> Return Receipt (hardcopy)	\$0.00
<input type="checkbox"/> Return Receipt (electronic)	\$0.00
<input type="checkbox"/> Certified Mail Restricted Delivery	\$0.00
<input type="checkbox"/> Adult Signature Required	\$0.00
<input type="checkbox"/> Adult Signature Restricted Delivery	\$0.00
Postage	\$8.25
Total Postage and Fees	\$11.80
Sent To <u>Megan Brennan</u>	
Street and Apt. No., or PO Box No.	
City, State, ZIP+4® <u>Washington, DC 20260</u>	
PS Form 3800, April 2015 PSN 7530-02-000-9047 See Reverse for Instructions	

7019 2970 0000 7471 7683

SPRINGFIELD, MA 01104

MAR 09 2020

03/05/2020

March 8, 2020, 9:21 am

Arrived at Hub

WASHINGTON, DC 20018

March 8, 2020, 4:35 am

Departed USPS Regional Facility

WASHINGTON DC DISTRIBUTION CENTER

March 7, 2020, 10:26 pm

Arrived at USPS Regional Facility

WASHINGTON DC DISTRIBUTION CENTER

March 7, 2020, 2:00 am

Departed USPS Regional Facility

YBOR CITY FL DISTRIBUTION CENTER

March 6, 2020, 9:10 pm

Arrived at USPS Regional Origin Facility

YBOR CITY FL DISTRIBUTION CENTER

March 6, 2020

In Transit to Next Facility

March 5, 2020, 7:04 pm

USPS in possession of item

SPRING HILL, FL 34606

Feedback

Product Information



See Less

EXHIBIT -
121 Page
Document to
Tampa ATF Special
Agent-in-Charge
Daryl R. McCrary

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Friday, February 28, 2020.

Daryl R. McCrary

[ATF Special Agent in Charge (SAC)]

Any other Agents/Deputies/Troopers/Officers or Civilians¹, who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
Tampa Field Division
400 North Tampa Street, Suite 2100
Tampa, Florida 33602

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear Special Agent-in-Charge McCrary,

Any other Officials or Civilians, who were/are involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and

Any other Officials or Civilians, who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

I'm also submitting an 'Immediate Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the Adobe Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") 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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I’m 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

Please confirm within 2-weeks of the date of this notice letter 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.

Please mail all correspondence to my P. O. Box, which is:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611**

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', written over a horizontal line.

Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com


[FAQs >](#)
[Track Another Package +](#)
Tracking Number: 70040750000303211311

[Remove X](#)

Your item has been delivered and is available at a PO Box at 7:27 am on March 3, 2020 in TAMPA, FL 33601.

✓ Delivered

March 3, 2020 at 7:27 am
Delivered, PO Box
TAMPA, FL 33601

[Get Updates ✓](#)

[Text & Email Updates](#)

Tracking History

March 3, 2020, 7:27 am

Delivered, PO Box
TAMPA, FL 33601

Your item has been delivered and is available at a PO Box at 7:27 am on March 3, 2020 in TAMPA, FL 33601.

March 2, 2020, 9:02 am

Out for Delivery
TAMPA, FL 33602

U.S. Postal Service TM	
CERTIFIED MAILTM RECEIPT	
(Domestic Mail Only; No Insurance Coverage Provided)	
For delivery information visit our website at www.usps.com	
TAMPA, FL 33602	
OFFICIAL USE	
Postage	\$3.55
Certified Fee	\$0.00
Return Receipt Fee (Endorsement Required)	\$0.00
Restricted Delivery Fee (Endorsement Required)	\$0.00
	\$7.50
Total Postage & Fees	\$11.05
Sent To <u>Daryl McCrary</u>	
Street, Apt. No., or PO Box No. <u>ATF SAC</u>	
City, State, ZIP+4 <u>Tampa, FL 33602</u>	
PS Form 3800, June 2002	
See Reverse for Instructions	

7004 0750 0003 0321 1311

TAMPA, FL 33602
FEB 29 2020
Postmark Here

March 2, 2020, 8:51 am

Arrived at Unit

TAMPA, FL 33605

March 1, 2020, 3:11 am

Arrived at USPS Regional Facility

YBOR CITY FL DISTRIBUTION CENTER

February 29, 2020, 9:29 pm

Departed Post Office

TAMPA, FL 33630

February 29, 2020, 7:23 pm

USPS in possession of item

TAMPA, FL 33630

Product Information



Feedback

See Less

Can't find what you're looking for?

Go to our FAQs section to find answers to your tracking questions.

FAQs

EXHIBIT -
121 Page
Document to
Boston FBI Special
Agent-in-Charge
Joseph R.
Bonavolonta

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Wednesday, March 04, 2020.

Joseph R. Bonavolonta

[FBI Special Agent in Charge (SAC)]

All Agents/Deputies/Troopers/Officers who were/are assigned/attached to any of the Joint Terrorism Task Forces (JTTFs) in Massachusetts and/or Civilians¹, who were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)
Federal Bureau of Investigation (FBI)

Boston Field Office

201 Maple Street

Chelsea

MA - 02150

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear Special Agent-in-Charge Bonavolonta,

Any other Officials who were/are assigned/attached to any of the Joint Terrorism Task Forces (JTTFs) in Massachusetts and/or Civilians, who were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and

Any other Officials who were/are assigned/attached to any of the Joint Terrorism Task Forces (JTTFs) in Massachusetts and/or Civilians, who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

I'm also submitting an 'Immediate and/or Continuing Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the free Adobe Acrobat Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and to the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") 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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue

is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I’m 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

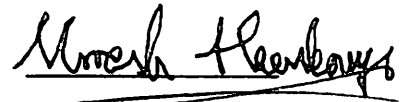
Please confirm within 2-weeks of the date of this notice letter that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Please mail all correspondence to my P. O. Box, which is:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611**

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', written over a horizontal line.

Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com


[FAQs >](#)
[Track Another Package +](#)
Tracking Number: 70192970000074717713

[Remove X](#)

Your item was delivered to an individual at the address at 1:00 pm on March 9, 2020 in CHELSEA, MA 02150.

✓ Delivered

March 9, 2020 at 1:00 pm
Delivered, Left with Individual
CHELSEA, MA 02150

[Get Updates ✓](#)
[Text & Email Updates](#)

Tracking History

March 9, 2020, 1:00 pm

Delivered, Left with Individual
CHELSEA, MA 02150

Your item was delivered to an individual at the address at 1:00 pm on March 9, 2020 in CHELSEA, MA 02150.

March 9, 2020, 7:10 am

Out for Delivery
CHELSEA, MA 02150

U.S. Postal Service™ CERTIFIED MAIL® RECEIPT Domestic Mail Only	
For delivery information, visit our website at www.usps.com ®.	
CHELSEA, MA 02150 90978	
Certified Mail Fee	\$3.55
Extra Services & Fees (check box, add fee as appropriate)	
<input type="checkbox"/> Return Receipt (hardcopy)	\$0.00
<input type="checkbox"/> Return Receipt (electronic)	\$0.00
<input type="checkbox"/> Certified Mail Restricted Delivery	\$0.00
<input type="checkbox"/> Adult Signature Required	\$0.00
<input type="checkbox"/> Adult Signature Restricted Delivery	\$0.00
Postage	\$8.45
Total Postage and Fees	\$12.00
Sent To <u>Joseph Bonarcolonta</u>	
Street and Apt. No., or P.O. Box No.	
City, State, Zip+4® <u>CHELSEA, MA-02150</u>	
PS Form 3800, April 2015 PSN 7530-02-000-9047 See Reverse for Instructions	

7019 2970 0000 7471 7713

0131 77
MAR 05 2020
Postmark Here
SPRING HILL, FL
03/05/2020

March 8, 2020, 9:43 am

Arrived at Hub

CHELSEA, MA 02150

March 8, 2020, 6:27 am

Arrived at USPS Facility

CHELSEA, MA 02150

March 8, 2020, 6:10 am

Departed USPS Regional Facility

BOSTON MA DISTRIBUTION CENTER

March 8, 2020, 12:58 am

Arrived at USPS Regional Destination Facility

BOSTON MA DISTRIBUTION CENTER

March 7, 2020

In Transit to Next Facility

March 6, 2020, 9:08 pm

Arrived at USPS Regional Origin Facility

YBOR CITY FL DISTRIBUTION CENTER

March 5, 2020, 7:03 pm

USPS in possession of item

SPRING HILL, FL 34606

Feedback

Product Information



See Less ^

EXHIBIT -
121 Page
Document to
Hernando County
Sheriff Alvin D.
Nienhuis

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Friday, February 28, 2020.

Hernando County Sheriff Alvin Nienhuis
Hernando County Sheriff's Detective David Kortman
Hernando County Deputy Sheriff Richard Kramer
Any other Officials with the Hernando County Sheriff's Office or Civilians¹, who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved with any of Plaintiff Heendeniya's Florida Public Records' Law Requests
18900 Cortez Boulevard
Brooksville
FL – 34601.

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear Sheriff Nienhuis, Sheriff's Detective Kortman, Deputy Sheriff Kramer,
Any other Officials with the Hernando County Sheriff's Office (HCSO) or Civilians, who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and
Any other Officials with the HCSO or Civilians, who were involved with any of Plaintiff Heendeniya's Florida Public Records' Law Requests:

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

Furthermore, in approx. September, 2014 and January, 2019, I delivered to you 'Immediate Evidence Preservation Demand' letters. Herewith, I'm submitting a continuing demand of evidence preservation on you and your office. In addition, in enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Requests that are given below and were submitted to you prior in approx. September, 2014 and January, 2019.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the Adobe Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") 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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I’m 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance

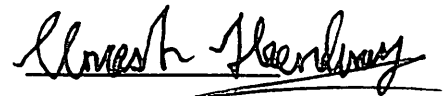
Please confirm within 2-weeks of the date of this notice letter that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Please mail all correspondence to my P. O. Box, which is:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611**

If you have any questions or concerns regarding the contents of this document and/or its 4 exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Umesh Heendeniya', with a horizontal line drawn underneath it.

Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com


[FAQs >](#)
[Track Another Package +](#)
Tracking Number: 70040750000303211274

[Remove X](#)

Your item was delivered to the front desk, reception area, or mail room at 1:42 pm on March 2, 2020 in BROOKSVILLE, FL 34601.

✓ Delivered

March 2, 2020 at 1:42 pm
Delivered, Front Desk/Reception/Mail Room
BROOKSVILLE, FL 34601

[Get Updates ✓](#)
[Text & Email Updates](#)

Tracking History

March 2, 2020, 1:42 pm

Delivered, Front Desk/Reception/Mail Room
BROOKSVILLE, FL 34601

Your item was delivered to the front desk, reception area, or mail room at 1:42 pm on March 2, 2020 in BROOKSVILLE, FL 34601.

March 2, 2020, 8:12 am

Out for Delivery
BROOKSVILLE, FL 34601

U.S. Postal Service™	
CERTIFIED MAIL™ RECEIPT	
(Domestic Mail Only; No Insurance Coverage Provided)	
For delivery information visit our website at www.usps.com	
BROOKSVILLE, FL 34601	
Postage	\$3.55
Certified Fee	\$0.00
Return Receipt Fee (Endorsement Required)	\$0.00
Restricted Delivery Fee (Endorsement Required)	\$0.00
	\$7.50
Total Postage & Fees	\$11.05
Sent To <u>HCSO Al Nienhuis</u>	
Street, Apt. No., or PO Box No. <u>Brookville, FL 34601</u>	
City, State ZIP+4 <u>Brookville, FL 34601</u>	
PS Form 3800, June 2002	
See Reverse for Instructions	

7004 0750 0003 0321 1274

02/29/2020 0600

Postmark Here

March 2, 2020, 8:01 am

Arrived at Unit
BROOKSVILLE, FL 34601

March 2, 2020, 3:25 am

Departed USPS Regional Facility
YBOR CITY FL DISTRIBUTION CENTER

March 1, 2020, 3:10 am

Arrived at USPS Regional Facility
YBOR CITY FL DISTRIBUTION CENTER

February 29, 2020, 9:29 pm

Departed Post Office
TAMPA, FL 33630

February 29, 2020, 7:22 pm

USPS in possession of item
TAMPA, FL 33630

Feedback

Product Information



See Less ^

Can't find what you're looking for?

Go to our FAQs section to find answers to your tracking questions.

FAQs

EXHIBIT λ

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Friday, February 28, 2020.

Michael F. McPherson
[FBI Special Agent in Charge (SAC)]
Thomas Miller
[FBI Special Agent and Task Force Officer (TFO) who is/was assigned/attached to the Tampa Joint Terrorism Task Force (Tampa JTTF)]
Sonya Yongue
[FBI Special Agent and TFO who is/was assigned/attached to the Tampa JTTF]
David Kortman
[Hernando County Sheriff's Detective and TFO who is/was assigned/attached to the Tampa JTTF]
Any other Agents/Deputies/Troopers/Officers who are/were assigned/attached to the 'Tampa JTTF' or the 'Orlando JTTF' or Civilians¹, who are/were involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, or who were involved in any manner with any of Plaintiff Heendeniya's public records requests that were made from 2015 to the Present pursuant to the Privacy Act (PA) and/or the Freedom of Information Act (FOIA)
Federal Bureau of Investigation (FBI)
Tampa Field Office
5525 West Gray Street
Tampa
FL - 33609

**Re: Lawsuit No. 8:2020-CV-114T02SPF Filed on Jan. 15, 2020 in The U.S. District Court for The Middle District of Florida;
Plaintiff Umesh Heendeniya's Request for Immediate and/or Continuing Evidence Preservation; and
The 'Notice of Pendency of Other Actions (Related Case)' and The 'Certificate of Interested Persons and Corporate Disclosure Statement' Submitted by Plaintiff Umesh Heendeniya.**

Dear Special Agent-in-Charge McPherson, Special Agent Miller, Special Agent Yongue, Sheriff's Detective Kortman,
Any other Officials who were/are assigned/attached to the 'Tampa JTTF' or the 'Orlando JTTF' or Civilians, who were/are involved with any investigation or surveillance of Plaintiff Umesh Heendeniya, and
Any other Officials who were/are assigned/attached to the 'Tampa JTTF' or the 'Orlando JTTF' or Civilians, who were involved in any manner with any of Plaintiff Heendeniya's public records

¹ Some examples of civilians include those from the FBI cover program and operation named "Stagehand," the FBI's National Security Recruitment Program, or the CIA's National Resources Division (the agency's clandestine Domestic Operational Wing), etc.

requests that were made from 2015 to the Present utilizing the Privacy Act (PA) and/or the Freedom of Information Act (FOIA):

The above-cited lawsuit has been filed against you, or alternatively, you may be added as a party defendant in this lawsuit in the future, or alternatively, a subpoena may be issued pertaining to you, requesting evidence that you possess (or possessed) or your testimony may be taken as a third-party deposition-deponent. A copy of the 1st page of the lawsuit has been attached to this document as "Exhibit Alpha²."

Pursuant to The Court's orders, I have enclosed completed and signed copies of the 'Notice of Pendency of Other Actions (Related Case)' and the 'Certificate of Interested Persons and Corporate Disclosure Statement' that were submitted by me to The Court. They're contained within "Exhibit Delta."

I'm also submitting an 'Immediate Evidence Preservation Demand' on you and your office. In the enclosed Exhibits Bravo and Charlie, I have attached copies of 'Suggested Protocol for Discovery of Electronically Stored Information' and 'Principles for the Discovery of Electronically Stored Information in Civil Cases' that had been issued several years ago by The U.S. District Court for The District of Maryland as helpful guidance for litigants. I request that you use the information contained in these 2 documents (contained within Exhibits Bravo and Charlie), as supplements to the Evidence Preservation Request that is given below.

Lastly, I have enclosed an exact copy of this signed document (that contains approx. 110 pages on approx. 64 sheets of paper), as an Adobe PDF document/file in the enclosed CD-Rom. The CD-Rom is enclosed and protected by a CD jewel case, and prior to mailing, I double-checked to make sure that the single Adobe PDF document/file is accessible *via* the Adobe Reader software application. Thus, I ask that you promptly email, any and all Officials or Civilians to whom this document/letter is addressed and the agencies or companies they work for, Adobe PDF copies of this approx. 110-page document/letter/file, so that they're put on notice and are aware of its contents.

DEMAND for IMMEDIATE and/or CONTINUING EVIDENCE PRESERVATION

ESI Preservation

ESI That I May Use to Support Any Claims or Defenses in This Case

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. The people to whom this document/letter is addressed and the agencies or companies they work for (henceforth, "You" or "Your") must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of

² The exhibit in this document that has been demarcated as "Exhibit Delta" has several exhibits that have been marked as Exhibit 1, 2, etc., or Exhibit A, B, etc., and thus I've had to resort to using Alpha, Bravo, etc., as demarcations in this document to separate its own exhibits and avoid confusion.

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.

Electronically Stored Information

This information preservation demand concerns both physical and electronic information.

You should anticipate 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).

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information, such as:

- communications (e.g., e-mail, voice mail, instant messaging);
- documents (e.g., Word documents and drafts);
- spreadsheets and tables (e.g., Excel worksheets);
- image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- sound and/or video recordings (e.g., .WAV, .MP3, .AVI, and .MOV files);
- databases (e.g., Access, Oracle, SQL Server data, SAP);
- backup and archival files (e.g., Zip, .GHO, tapes, etc.); etc.

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 amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/2006), 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. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive the Plaintiff's 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 Monday, Sep. 18, 1989 through the date of this demand and concerning:

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 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. This concern is not one unique to you or your employees and officers. 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.

Preservation by Imaging

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 described above, as well as recording and preserving the system time and date of each such computer.

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. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that I will accept as sufficient, please email me to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though I 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.

System Sequestration or Forensically Sound Imaging

I suggest that, with respect to the named personnel above, 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, I believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As I anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, I demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By “forensically sound,” I 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 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

I would like to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps I 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, I urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that’s fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I'm 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 I am entitled, such failure would constitute spoliation of evidence, and I will not hesitate to seek sanctions.

Confirmation of Compliance


Please confirm within 2-weeks of the date of this notice letter 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.

Please mail all correspondence to my P. O. Box, which is:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611**

If you have any questions or concerns regarding the contents of this document and/or its exhibits, please contact me by my email which is: umeshheendeniyavsthefbi@gmail.com.

Sincerely,



Umesh Heendeniya
umeshheendeniyavsthefbi@gmail.com

EXHIBIT

ALPHA

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION**

UMESH HEENDENIYA,

Plaintiff,

v.

THOMAS MILLER, FBI AGENT ASSIGNED TO
THE TAMPA-ORLANDO JOINT TERRORISM
TASK FORCE (JTTF); SONYA YONGUE, FBI
AGENT ASSIGNED TO THE TAMPA-ORLANDO
JTTF; DAVID KORTMAN, HERNANDO COUNTY
SHERIFF'S DETECTIVE AND HCSO TASK FORCE
OFFICER (TFO) ASSIGNED TO THE
TAMPA-ORLANDO JTTF; ALVIN NIENHUIS,
HERNANDO COUNTY SHERIFF; HERNANDO
COUNTY SHERIFF'S OFFICE (HCSO); PAUL
WYSOPAL, FBI SPECIAL AGENT IN CHARGE
(SAC) OF THE TAMPA-ORLANDO FIELD OFFICE;
REGINA LOMBARDO, BATFE SPECIAL AGENT
IN CHARGE (SAC) OF THE TAMPA-ORLANDO
FIELD OFFICE; JOHN AND/OR JANE DOES 1-50;

Defendants.

Civil Action No. 8:2020cv114 Torg

FILED
2020 JAN 15 PM 3:54
CLERK, US DISTRICT COURT
MIDDLE DISTRICT FLORIDA
TAMPA, FLORIDA

Complaint for Monetary Damages,
Injunctive Relief, and Declaratory
Relief.

COMPLAINT AND JURY DEMAND

Umesh Heendeniya v. Thomas Miller, et al.

File

EXHIBIT BRAVO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN RE: ELECTRONICALLY STORED
INFORMATION

SUGGESTED PROTOCOL FOR DISCOVERY OF
ELECTRONICALLY STORED INFORMATION

1. On December 1, 2006, amendments to Fed.R.Civ.P. 16, 26, 33, 34, 37, and 45, and Form 35, became effective, creating a comprehensive set of rules governing discovery of electronically stored information, (“ESI”).

Given these rule changes, it is advisable to establish a suggested protocol regarding, and a basic format implementing, only those portions of the amendments that refer to ESI. The purpose of this Suggested Protocol for Discovery of Electronically Stored Information (the “Protocol”) is to facilitate the just, speedy, and inexpensive conduct of discovery involving ESI in civil cases, and to promote, whenever possible, the resolution of disputes regarding the discovery of ESI without Court intervention.

While this Protocol is intended to provide the parties with a comprehensive framework to address and resolve a wide range of ESI issues, it is not intended to be an inflexible checklist. The Court expects that the parties will consider the nature of the claim, the amount in controversy, agreements of the parties, the relative ability of the parties to conduct discovery of ESI, and such other factors as may be relevant under the circumstances. Therefore not all aspects of this Protocol may be applicable or practical for a particular matter, and indeed, if the parties do not intend to seek discovery of ESI it may be entirely inapplicable to a particular case. The Court encourages the parties to use this Protocol in cases in which there will be discovery of ESI, and to resolve ESI

issues informally and without Court supervision whenever possible. In this regard, compliance with this Protocol may be considered by the Court in resolving discovery disputes, including whether sanctions should be awarded pursuant to Fed.R.Civ.P. 37;

SCOPE

2. This Protocol applies to the ESI provisions of Fed.R.Civ.P. 16, 26, 33, 34, or 37, and, insofar as it relates to ESI, this Protocol applies to Fed.R.Civ.P. 45 in all instances where the provisions of Fed.R.Civ.P. 45 are the same as, or substantially similar to, Fed.R.Civ.P. 16, 26, 33, 34, or 37. In such circumstances, if a Conference pursuant to Fed.R.Civ.P. 26(f) is held, it may include all parties, as well as the person or entity served with the subpoena, if said Conference has not yet been conducted. If the Conference has been conducted, upon written request of any party or the person or entity served with the subpoena, a similar conference may be conducted regarding production of ESI pursuant to the subpoena. As used herein, the words “party” or “parties” include any person or entity that is served with a subpoena pursuant to Fed.R.Civ.P. 45. Nothing contained herein modifies Fed.R.Civ.P. 45 and, specifically, the provision of Rule 45(c)(2)(B) regarding the effect of a written objection to inspection or copying of any or all of the designated materials or premises.

3. In this Protocol, the following terms have the following meanings:

- A. “Meta-Data” means: (i) information embedded in a Native File that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native File; and (ii) information generated automatically

by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted or otherwise manipulated by a user of such system. Meta-Data is a subset of ESI.

- B. “Native File(s)” means ESI in the electronic format of the application in which such ESI is normally created, viewed and/or modified. Native Files are a subset of ESI.
- C. “Static Image(s)” means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. In the absence of agreement of the parties or order of Court, a Static Image should be provided in either Tagged Image File Format (TIFF, or .TIF files) or Portable Document Format (PDF). If load files were created in the process of converting Native Files to Static Images, or if load files may be created without undue burden or cost, load files should be produced together with Static Images.

CONFERENCE OF PARTIES AND REPORT

4. The parties are encouraged to consider conducting a Conference of Parties to discuss discovery of ESI regardless of whether such a Conference is ordered by the Court. The Conference of Parties should be conducted in person whenever practicable. Within 10 calendar days thereafter, the parties may wish to file, or the Court may order them to file, a joint report regarding the results of the Conference. This process is also encouraged if applicable, in connection with a subpoena

for ESI under Fed.R.Civ.P. 45. The report may state that the parties do not desire discovery of ESI, in which event Paragraphs 4A and B are inapplicable.

- A. The report should, without limitation, state in the section captioned “Disclosure or discovery of electronically stored information should be handled as follows,” the following:
 - (1) Any areas on which the parties have reached agreement and, if any, on which the parties request Court approval of that agreement;
 - (2) Any areas on which the parties are in disagreement and request intervention of the Court.
- B. The report should, without limitation, if it proposes a “clawback” agreement, “quick peek,” or testing or sampling, specify the proposed treatment of privileged information and work product, in a manner that, if applicable, complies with the standard set forth in *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), and other applicable precedent. On-site inspections of ESI under Fed.R.Civ.P. 34(b) should only be permitted in circumstances where good cause and specific need have been demonstrated by the party seeking disclosure of ESI (the “Requesting Party”), or by agreement of the parties. In appropriate circumstances the Court may condition on-site inspections of ESI to be performed by independent third party experts, or set such other conditions as are agreed by the parties or deemed appropriate by the Court.

- C. Unless otherwise agreed by the parties, the report described by this provision should be filed with the Court prior to the commencement of discovery of ESI.

NEED FOR PRIOR PLANNING

5. Insofar as it relates to ESI, prior planning and preparation is essential for a Conference of Parties pursuant to Fed.R.Civ.P. 16, 26(f), and this Protocol. Counsel for the Requesting Party and Counsel for the party producing, opposing, or seeking to limit disclosure of ESI (“Producing Party”) bear the primary responsibility for taking the planning actions contained herein. Failure to reasonably comply with the planning requirements in good faith may be a factor considered by the Court in imposing sanctions.

EXCHANGE OF INFORMATION BEFORE RULE 26(f) CONFERENCE

6. Insofar as it relates to ESI, in order to have a meaningful Conference of Parties, it may be necessary for parties to exchange information prior to the Fed.R.Civ.P. 26(f) Conference of Parties. Parties are encouraged to take the steps described in ¶7 of this Protocol and agree on a date that is prior to the Fed.R.Civ.P. 26(f) Conference of Parties, on which agreed date they will discuss by telephone whether it is necessary or convenient to exchange information about ESI prior to the conference.

- A. A reasonable request for prior exchange of information may include information relating to network design, the types of databases, database dictionaries, the access control list and security access logs and rights of individuals to access the system and specific files and applications, the ESI

document retention policy, organizational chart for information systems personnel, or the backup and systems recovery routines, including, but not limited to, tape rotation and destruction/overwrite policy.

- B. An unreasonable request for a prior exchange of information should not be made.
- C. A reasonable request for a prior exchange of information should not be denied.
- D. To the extent practicable, the parties should, prior to the Fed.R.Civ.P. 26(f) Conference of Parties, discuss the scope of discovery of ESI, including whether the time parameters of discoverable ESI, or for subsets of ESI, may be narrower than the parameters for other discovery.
- E. Prior to the Fed.R.Civ.P. 26(f) Conference of Parties, Counsel should discuss with their clients and each other who will participate in the Fed.R.Civ.P. 26(f) Conference of Parties. This discussion should specifically include whether one or more participants should have an ESI coordinator (*see* Paragraph 7.B) participate in the Conference. If one participant believes that the other should have an ESI coordinator participate, and the other disagrees, the Requesting Party should state its reasons in a writing sent to all other parties within a reasonable time before the Rule 26(f) Conference. If the Court subsequently determines that the Conference was not productive due

to the absence of an ESI coordinator, it may consider the letter in conjunction with any request for sanctions under Fed.R.Civ.P. 37.

PREPARATION FOR RULE 26(f) CONFERENCE

7. Prior to the Fed.R.Civ.P. 26(f) Conference of Parties, Counsel for the parties should:
 - A. Take such steps as are necessary to advise their respective clients, including, but not limited to, “key persons” with respect to the facts underlying the litigation, and information systems personnel, of the substantive principles governing the preservation of relevant or discoverable ESI while the lawsuit is pending. As a general principle to guide the discussion regarding litigation hold policies, Counsel should consider the following criteria:
 - (1) Scope of the “litigation hold,” including:
 - (a) A determination of the categories of potentially discoverable information to be segregated and preserved;
 - (b) Discussion of the nature of issues in the case, as per Fed.R.Civ.P. 26(b)(1);
 - (i) Whether ESI is relevant to only some or all claims and defenses in the litigation;
 - (ii) Whether ESI is relevant to the subject matter involved in the action;
 - (c) Identification of “key persons,” and likely witnesses and persons with knowledge regarding relevant events;

- (d) The relevant time period for the litigation hold;
- (2) Analysis of what needs to be preserved, including:
 - (a) The nature of specific types of ESI, including, email and attachments, word processing documents, spreadsheets, graphics and presentation documents, images, text files, hard drives, databases, instant messages, transaction logs, audio and video files, voicemail, Internet data, computer logs, text messages, or backup materials, and Native Files, and how it should be preserved;
 - (b) the extent to which Meta-Data, deleted data, or fragmented data, will be subject to litigation hold;
 - (c) paper documents that are exact duplicates of ESI;
 - (d) any preservation of ESI that has been deleted but not purged;
- (3) Determination of where ESI subject to the litigation hold is maintained, including:
 - (a) format, location, structure, and accessibility of active storage, backup, and archives;
 - (i) servers;
 - (ii) computer systems, including legacy systems;
 - (iii) remote and third-party locations;

- (iv) back-up media (for disasters) vs. back-up media for archival purposes/record retention laws;
 - (b) network, intranet, and shared areas (public folders, discussion databases, departmental drives, and shared network folders);
 - (c) desktop computers and workstations;
 - (d) portable media; laptops; personal computers; PDA's; paging devices; mobile telephones; and flash drives;
 - (e) tapes, discs, drives, cartridges and other storage media;
 - (f) home computers (to the extent, if any, they are used for business purposes);
 - (g) paper documents that represent ESI.
- (4) Distribution of the notification of the litigation hold:
- (a) to parties and potential witnesses;
 - (b) to persons with records that are potentially discoverable;
 - (c) to persons with control over discoverable information; including:
 - (i) IT personnel/director of network services;
 - (ii) custodian of records;
 - (iii) key administrative assistants;
 - (d) third parties (contractors and vendors who provide IT services).

- (5) Instructions to be contained in a litigation hold notice, including that:
- (a) there will be no deletion, modification, alteration of ESI subject to the litigation hold;
 - (b) the recipient should advise whether specific categories of ESI subject to the litigation hold require particular actions (*e.g.*, printing paper copies of email and attachments) or transfer into “read only” media;
 - (c) loading of new software that materially impacts ESI subject to the hold may occur only upon prior written approval from designated personnel;
 - (d) where Meta-Data, or data that has been deleted but not purged, is to be preserved, either a method to preserve such data before running compression, disk defragmentation or other computer optimization or automated maintenance programs or scripts of any kind (“File and System Maintenance Procedures”), or the termination of all File and System Maintenance Procedures during the pendency of the litigation hold in respect of Native Files subject to preservation;

- (e) reasonably safeguarding and preserving all portable or removable electronic storage media containing potentially relevant ESI;
 - (f) maintaining hardware that has been removed from active production, if such hardware contains legacy systems with relevant ESI and there is no reasonably available alternative that preserves access to the Native Files on such hardware.
- (6) Monitoring compliance with the notification of litigation hold, including:
- (a) identifying contact person who will address questions regarding preservation duties;
 - (b) identifying personnel with responsibility to confirm that compliance requirements are met;
 - (c) determining whether data of "key persons" requires special handling (*e.g.*, imaging/cloning hard drives);
 - (d) periodic checks of logs or memoranda detailing compliance;
 - (e) issuance of periodic reminders that the litigation hold is still in effect.
- B. Identify one or more information technology or information systems personnel to act as the ESI coordinator and discuss ESI with that person;

- C. Identify those personnel who may be considered “key persons” by the events placed in issue by the lawsuit and determine their ESI practices, including those matters set forth in Paragraph 7.D, below. The term “key persons” is intended to refer to both the natural person or persons who is/are a “key person(s)” with regard to the facts that underlie the litigation, and any applicable clerical or support personnel who directly prepare, store, or modify ESI for that key person or persons, including, but not limited to, the network administrator, custodian of records or records management personnel, and an administrative assistant or personal secretary;
- D. Become reasonably familiar¹ with their respective clients’ current and relevant past ESI, if any, or alternatively, identify a person who can participate in the Fed.R.Civ.P. 26(f) Conference of Parties and who is familiar with at least the following:
- (1) Email systems; blogs; instant messaging; Short Message Service (SMS) systems; word processing systems; spreadsheet and database systems; system history files, cache files, and cookies; graphics, animation, or document presentation systems; calendar systems; voice mail systems, including specifically, whether such systems

¹ As used herein, the term “reasonably familiar” contemplates a heightened level of familiarity with any ESI that is identified by opposing counsel pursuant to Paragraph 6 of this Protocol, however, that level of familiarity is conditioned upon the nature of the pleadings, the circumstances of the case, and the factors contained in Fed.R.Civ.P. 26(b)(2)(C).

include ESI; data files; program files; internet systems; and, intranet systems. This Protocol may include information concerning the specific version of software programs and may include information stored on electronic bulletin boards, regardless of whether they are maintained by the party, authorized by the party, or officially sponsored by the party; provided however, this Protocol extends only to the information to the extent such information is in the possession, custody, or control of such party. To the extent reasonably possible, this includes the database program used over the relevant time, its database dictionary, and the manner in which such program records transactional history in respect to deleted records.

- (2) Storage systems, including whether ESI is stored on servers, individual hard drives, home computers, “laptop” or “notebook” computers, personal digital assistants, pagers, mobile telephones, or removable/portable storage devices, such as CD-Roms, DVDs, “floppy” disks, zip drives, tape drives, external hard drives, flash, thumb or “key” drives, or external service providers.
- (3) Back up and archival systems, including those that are onsite, offsite, or maintained using one or more third-party vendors. This Protocol may include a reasonable inquiry into the back-up routine, application, and process and location of storage media, and requires

inquiry into whether ESI is reasonably accessible without undue burden or cost, whether it is compressed, encrypted, and the type of device on which it is recorded (*e.g.*, whether it uses sequential or random access), and whether software that is capable of rendering it into usable form without undue expense is within the client's possession, custody, or control.

- (4) Obsolete or "legacy" systems containing ESI and the extent, if any, to which such ESI was copied or transferred to new or replacement systems.
- (5) Current and historical website information, including any potentially relevant or discoverable statements contained on that or those site(s), as well as systems to back up, archive, store, or retain superseded, deleted, or removed web pages, and policies regarding allowing third parties' sites to archive client website data.
- (6) Event data records automatically created by the operation, usage, or polling of software or hardware (such as recorded by a motor vehicle's GPS or other internal computer prior to an occurrence), if any and if applicable, in automobiles, trucks, aircraft, vessels, or other vehicles or equipment.

- (7) Communication systems, if any and if applicable, such as ESI records of radio transmissions, telephones, personal digital assistants, or GPS systems.
- (8) ESI erasure, modification, or recovery mechanisms, such as Meta-Data scrubbers or programs that repeatedly overwrite portions of storage media in order to preclude data recovery, and policies regarding the use of such processes and software, as well as recovery programs that can defeat scrubbing, thereby recovering deleted, but inadvertently produced ESI which, in some cases, may even include privileged information.
- (9) Policies regarding records management, including the retention or destruction of ESI prior to the client receiving knowledge that a claim is reasonably anticipated.
- (10) “Litigation hold” policies that are instituted when a claim is reasonably anticipated, including all such policies that have been instituted, and the date on which they were instituted.
- (11) The identity of custodians of key ESI, including “key persons” and related staff members, and the information technology or information systems personnel, vendors, or subcontractors who are best able to describe the client’s information technology system.

(12) The identity of vendors or subcontractors who store ESI for, or provide services or applications to, the client or a key person; the nature, amount, and a description of the ESI stored by those vendors or subcontractors; contractual or other agreements that permit the client to impose a “litigation hold” on such ESI; whether or not such a “litigation hold” has been placed on such ESI; and, if not, why not.

E. Negotiation of an agreement that outlines what steps each party will take to segregate and preserve the integrity of relevant or discoverable ESI. This agreement may provide for depositions of information system personnel on issues related to preservation, steps taken to ensure that ESI is not deleted in the ordinary course of business, steps taken to avoid alteration of discoverable ESI, and criteria regarding the operation of spam or virus filters and the destruction of filtered ESI.

TOPICS TO DISCUSS AT RULE 26(f) CONFERENCE

8. The following topics, if applicable, should be discussed at the Fed.R.Civ.P. 26(f) Conference of Parties:

A. The anticipated scope of requests for, and objections to, production of ESI, as well as the form of production of ESI and, specifically, but without limitation, whether production will be of the Native File, Static Image, or other searchable or non-searchable formats.

- (1) If the parties are unable to reach agreement on the format for production, ESI should be produced to the Requesting Party as Static Images. When the Static Image is produced, the Producing Party should maintain a separate file as a Native File and, in that separate file, it should not modify the Native File in a manner that materially changes the file and the Meta-Data. After initial production in Static Images is complete, a party seeking production of Native File ESI should demonstrate particularized need for that production.
- (2) The parties should discuss whether production of some or all ESI in paper format is agreeable in lieu of production in electronic format.
- (3) When parties have agreed or the Court has ordered the parties to exchange all or some documents as electronic files in Native File format in connection with discovery, the parties should collect and produce said relevant files in Native File formats in a manner that preserves the integrity of the files, including, but not limited to, the contents of the file, the Meta-Data (including System Meta-Data, Substantive Meta-Data, and Embedded Meta-Data, as more fully described in Paragraph 11 of this Protocol) related to the file, and the file's creation date and time. The general process to preserve the data integrity of a file may include one or more of the following procedures: (a) duplication of responsive files in the file system (*i.e.*,

creating a forensic copy, including a bit image copy, of the file system or pertinent portion), (b) performing a routine copy of the files while preserving Meta-Data (including, but not limited to, creation date and time), and/or (c) using reasonable measures to prevent a file from being, or indicate that a file has been, modified, either intentionally or unintentionally, since the collection or production date of the files. If any party desires to redact contents of a Native File for privilege, trade secret, or other purposes (including, but not limited to, Meta-Data), then the Producing Party should indicate that the file has been redacted, and an original, unmodified file should be retained at least during the pendency of the case.

- B. Whether Meta-Data is requested for some or all ESI and, if so, the volume and costs of producing and reviewing said ESI.
- C Preservation of ESI during the pendency of the lawsuit, specifically, but without limitation, applicability of the “safe harbor” provision of Fed.R.Civ.P. 37, preservation of Meta-Data, preservation of deleted ESI, back up or archival ESI, ESI contained in dynamic systems², ESI destroyed or overwritten by the routine operation of systems, and, offsite and offline ESI (including ESI stored on home or personal computers). This discussion

² A “dynamic system” is a system that remains in use during the pendency of the litigation and in which ESI changes on a routine and regular basis, including the automatic deletion or overwriting of such ESI.

should include whether the parties can agree on methods of review of ESI by the responding party in a manner that does not unacceptably change Meta-Data.

- (1) If Counsel are able to agree, the terms of an agreed-upon preservation order may be submitted to the Court;
- (2) If Counsel are unable to agree, they should attempt to reach agreement on the manner in which each party should submit a narrowly tailored, proposed preservation order to the Court for its consideration.

D. Post-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and/or other privileges in light of “clawback,” “quick peek,” or testing or sampling procedures, and submission of a proposed order pursuant to the holding of *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), and other applicable precedent. If Meta-Data is to be produced, Counsel may agree, and should discuss any agreement, that Meta-Data not be reviewed by the recipient and the terms of submission of a proposed order encompassing that agreement to the Court. Counsel should also discuss procedures under which ESI that contains privileged information or attorney work product should be immediately returned to the Producing Party if the ESI appears on its face to have been inadvertently produced or if there is prompt written notice of

inadvertent production by the Producing Party. The Producing Party should maintain unaltered copies of all such returned materials under the control of Counsel of record. This provision is procedural and return of materials pursuant to this Protocol is without prejudice to any substantive right to assert, or oppose, waiver of any protection against disclosure.

- E. Identification of ESI that is or is not reasonably accessible without undue burden or cost, specifically, and without limitation, the identity of such sources and the reasons for a contention that the ESI is or is not reasonably accessible without undue burden or cost, the methods of storing and retrieving that ESI, and the anticipated costs and efforts involved in retrieving that ESI. The party asserting that ESI is not reasonably accessible without undue burden or cost should be prepared to discuss in reasonable detail, the information described in Paragraph 10 of this Protocol.
- F. Because identifying information may not be placed on ESI as easily as bates-stamping paper documents, methods of identifying pages or segments of ESI produced in discovery should be discussed, and, specifically, and without limitation, the following alternatives may be considered by the parties: electronically paginating Native File ESI pursuant to a stipulated agreement that the alteration does not affect admissibility; renaming Native Files using bates-type numbering systems, *e.g.*, ABC0001, ABC0002, ABC0003, with some method of referring to unnumbered “pages” within each file; using

software that produces “hash marks” or “hash values” for each Native File; placing pagination on Static Images; or any other practicable method. The parties are encouraged to discuss the use of a digital notary for producing Native Files.

- G. The method and manner of redacting information from ESI if only part of the ESI is discoverable. As set forth in Paragraph 11.D, if Meta-Data is redacted from a file, written notice of such redaction, and the scope of that redaction, should be provided.
- H. The nature of information systems used by the party or person or entity served with a subpoena requesting ESI, including those systems described in Paragraph 7.D above. This Protocol may suggest that Counsel be prepared to list the types of information systems used by the client and the varying accessibility, if any, of each system. It may suggest that Counsel be prepared to identify the ESI custodians, for example, by name, title, and job responsibility. It also may suggest that, unless impracticable, Counsel be able to identify the software (including the version) used in the ordinary course of business to access the ESI, and the file formats of such ESI.
- I. Specific facts related to the costs and burdens of preservation, retrieval, and use of ESI.
- J. Cost sharing for the preservation, retrieval and/or production of ESI, including any discovery database, differentiating between ESI that is

reasonably accessible and ESI that is not reasonably accessible; provided however that absent a contrary showing of good cause, *e.g.*, Fed.R.Civ.P. 26(b)(2)(C), the parties should generally presume that the Producing Party bears all costs as to reasonably accessible ESI and, provided further, the parties should generally presume that there will be cost sharing or cost shifting as to ESI that is not reasonably accessible. The parties may choose to discuss the use of an Application Service Provider that is capable of establishing a central repository of ESI for all parties.

- K. Search methodologies for retrieving or reviewing ESI such as identification of the systems to be searched; identification of systems that will not be searched; restrictions or limitations on the search; factors that limit the ability to search; the use of key word searches, with an agreement on the words or terms to be searched; using sampling to search rather than searching all of the records; limitations on the time frame of ESI to be searched; limitations on the fields or document types to be searched; limitations regarding whether back up, archival, legacy or deleted ESI is to be searched; the number of hours that must be expended by the searching party or person in conducting the search and compiling and reviewing ESI; and the amount of pre-production review that is reasonable for the Producing Party to undertake in light of the considerations set forth in Fed.R.Civ.P. 26(b)(2)(C).

- L. Preliminary depositions of information systems personnel, and limits on the scope of such depositions. Counsel should specifically consider whether limitations on the scope of such depositions should be submitted to the Court with a proposed order that, if entered, would permit Counsel to instruct a witness not to answer questions beyond the scope of the limitation, pursuant to Fed.R.Civ.P. 30(d)(1).
- M. The need for two-tier or staged discovery of ESI, considering whether ESI initially can be produced in a manner that is more cost-effective, while reserving the right to request or to oppose additional more comprehensive production in a latter stage or stages. Absent agreement or good cause shown, discovery of ESI should proceed in the following sequence: 1) after receiving requests for production of ESI, the parties should search their ESI, other than that identified as not reasonably accessible without undue burden or cost, and produce responsive ESI within the parameters of Fed.R.Civ.P. 26(b)(2)(C); 2) searches of or for ESI identified as not reasonably accessible should not be conducted until the prior step has been completed; and, 3) requests for information expected to be found in or among ESI that was identified as not reasonably accessible should be narrowly focused, with a factual basis supporting each request.
- N. The need for any protective orders or confidentiality orders, in conformance with the Local Rules and substantive principles governing such orders.

- O. Any request for sampling or testing of ESI; the parameters of such requests; the time, manner, scope, and place limitations that will voluntarily or by Court order be placed on such processes; the persons to be involved; and the dispute resolution mechanism, if any, agreed-upon by the parties.
- P. Any agreement concerning retention of an agreed-upon Court expert, retained at the cost of the parties, to assist in the resolution of technical issues presented by ESI.

PARTICIPANTS

- 9. The following people:
 - A. Should, absent good cause, participate in the Fed.R.Civ.P. 26(f) Conference of Parties: lead counsel and at least one representative of each party.
 - B. May participate in the Fed.R.Civ.P. 26(f) Conference of Parties: clients or representatives of clients or the entity served with a subpoena; the designated ESI coordinator for the party; forensic experts; and in-house information system personnel. Identification of an expert for use in a Fed.R.Civ.P. 26(f) Conference of Parties does not, in and of itself, identify that person as an expert whose opinions may be presented at trial within the meaning of Fed.R.Civ.P. 26(b)(4)(A, B).
 - C. If a party is not reasonably prepared for the Fed.R.Civ.P. 26(f) Conference of Parties in accordance with the terms of this Protocol, that factor may be

used to support a motion for sanctions by the opposing party for the costs incurred in connection with that Conference.

REASONABLY ACCESSIBLE

10. No party should object to the discovery of ESI pursuant to Fed.R.Civ.P. 26(b)(2)(B) on the basis that it is not reasonably accessible because of undue burden or cost unless the objection has been stated with particularity, and not in conclusory or boilerplate language. Wherever the term “reasonably accessible” is used in this Protocol, the party asserting that ESI is not reasonably accessible should be prepared to specify facts that support its contention.

PRINCIPLES RE: META-DATA

11. The production of Meta-Data apart from its Native File may impose substantial costs, either in the extraction of such Meta-Data from the Native Files, or in its review for purposes of redacting non-discoverable information contained in such Meta-Data. The persons involved in the discovery process are expected to be cognizant of those costs in light of the various factors established in Fed.R.Civ.P. 26(b)(2)(C). The following principles should be utilized in determining whether Meta-Data may be discovered:

- A. Meta-Data is part of ESI. Such Meta-Data, however, may not be relevant to the issues presented or, if relevant, not be reasonably subject to discovery given the Rule 26(b)(2)(C) cost-benefit factors. Therefore, it may be subject to cost-shifting under Fed.R.Civ.P. 26(b)(2)(C).
- B. Meta-Data may generally be viewed as either System Meta-Data, Substantive Meta-Data, or Embedded Meta-Data. System Meta-Data is data that is

automatically generated by a computer system. For example, System Meta-Data often includes information such as the author, date and time of creation, and the date a document was modified. Substantive Meta-Data is data that reflects the substantive changes made to the document by the user. For example, it may include the text of actual changes to a document. While no generalization is universally applicable, System Meta-Data is less likely to involve issues of work product and/or privilege.

- C. Except as otherwise provided in sub-paragraph E, below, Meta-Data, especially substantive Meta-Data, need not be routinely produced, except upon agreement of the requesting and producing litigants, or upon a showing of good cause in a motion filed by the Requesting Party in accordance with the procedures set forth in the Local Rules of this Court. Consideration should be given to the production of System Meta-Data and its production is encouraged in instances where it will not unnecessarily or unreasonably increase costs or burdens. As set forth above, upon agreement of the parties, the Court will consider entry of an order approving an agreement that a party may produce Meta-Data in Native Files upon the representation of the recipient that the recipient will neither access nor review such data. This Protocol does not address the substantive issue of the duty to preserve such Meta-Data, the authenticity of such Meta-Data, or its admissibility into evidence or use in the course of depositions or other discovery.

- D. If a Producing Party produces ESI without some or all of the Meta-Data that was contained in the ESI, the Producing Party should inform all other parties of this fact, in writing, at or before the time of production.
- E. Some Native Files contain, in addition to Substantive Meta-Data and/or System Meta-Data, Embedded Meta-Data, which for purposes of this Protocol, means the text, numbers, content, data, or other information that is directly or indirectly inputted into a Native File by a user and which is not typically visible to the user viewing the output display of the Native File on screen or as a print out. Examples of Embedded Meta-Data include, but are not limited to, spreadsheet formulas (which display as the result of the formula operation), hidden columns, externally or internally linked files (*e.g.*, sound files in Powerpoint presentations), references to external files and content (*e.g.*, hyperlinks to HTML files or URLs), references and fields (*e.g.*, the field codes for an auto-numbered document), and certain database information if the data is part of a database (*e.g.*, a date field in a database will display as a formatted date, but its actual value is typically a long integer). Subject to the other provisions of this Protocol related to the costs and benefits of preserving and producing Meta-Data (see generally Paragraph 8), subject to potential redaction of Substantive Meta-Data, and subject to reducing the scope of production of Embedded Meta-Data, Embedded Meta-Data is generally discoverable and in appropriate cases, *see*

Fed.R.Civ.P. 26(b)(2)(C), should be produced as a matter of course. If the parties determine to produce Embedded Meta-Data, either in connection with a Native File production or in connection with Static Image production in lieu of Native File production, the parties should normally discuss and agree on use of appropriate tools and methods to remove other Meta-Data, but preserve the Embedded Meta-Data, prior to such production.

EXHIBIT GAMMA

In the United States District Court
for the District of Maryland

PRINCIPLES FOR THE DISCOVERY OF
ELECTRONICALLY STORED INFORMATION IN CIVIL CASES

GENERAL PRINCIPLES

Principle 1.01 (Purpose)

Electronic discovery is now routinely encountered in civil litigation. At the same time, the Court is aware that the discovery of ESI is a potential source of cost, burden, and delay. The purpose of these ESI Principles is to encourage reasonable electronic discovery, in cases where it is appropriate to conduct such discovery, with the goal of reducing cost, burden, and delay and to “secure the just, speedy, and inexpensive determination of every action and proceeding” pursuant to Fed. R. Civ. P. 1. These ESI Principles also promote the avoidance or early resolution of disputes regarding the discovery of ESI without Court intervention. While parties are encouraged to discuss these ESI Principles in individual cases, compliance with them is voluntary and not required by the Court.

Principle 1.02 (Cooperation and Exchange of Information)

The Court recognizes the principles of The Sedona Conference® Cooperation Proclamation¹ and expects cooperation on issues relating to the preservation, collection, search, review, production, integrity, and authentication of ESI. The Court particularly emphasizes the importance, of cooperative exchanges of information about ESI at the earliest stages of litigation. An early exchange about ESI that will be relevant to the case may help ensure that conferences between the parties, as well as agreements between the parties, are meaningful.

¹ <https://thesedonaconference.org/cooperation-proclamation>

Each case is different, and the type of information exchanged should be tailored to best meet the needs of the case. Depending on the case, the parties may consider exchanging a data map (either in list form or visual) and information about the following types of technologies, systems, tools, or protocols as used by the parties: software applications or platforms, including databases; document management, mail, and messaging systems; types of computing devices (including portable computing and storage devices); use of home computers or personally-owned devices; the identity and rights of individuals to access the systems and specific files, services, and applications; network and database design and structure; use of cloud, off-site, or other third-party services, including social media and personal email; and backup and recovery routines, including backup media rotation practices. The parties may also consider exchanging organizational charts for key custodians of ESI and relevant policies, including those relating to computer usage, document management, ESI, or document retention or destruction.

Principle 1.03 (Proportionality)

The parties should apply the proportionality standard set forth in Fed. R. Civ. P. 26(b) to all phases of the discovery of ESI, including the identification, preservation, collection, search, review, and production of ESI while maintaining the integrity of the ESI. To assure reasonableness and proportionality in electronic discovery, parties should consider the factors described in Fed. R. Civ. P. 26(b). To facilitate adherence to the proportionality standard, requests for production of ESI and related responses should be prepared in consultation with custodians, IT custodians, and/or IT administrators so the resulting discovery is reasonably targeted, clear, complete, accurate, and as particularized as practicable.

ESI CASE MANAGEMENT PRINCIPLES

Principle 2.01 (Preservation of ESI)

- a) Parties should take measures to preserve ESI as required by law. Parties should discuss preservation of ESI as early in the litigation as feasible. Such discussions should continue to occur periodically as the case and issues evolve.
- b) In determining what ESI to preserve, parties should apply the proportionality standard referenced in Principle 1.03.
- c) Parties are not required to use preservation notices to notify an opposing party of a preservation obligation, but if a party does so, the notice should apply the proportionality standard referenced in Principle 1.03 and be reasonably targeted, clear, complete, accurate, and as specific as practicable.
- d) If there is a dispute concerning the scope of a party's preservation efforts, the parties should comply with the process outlined in Local Rule 104.7 and fully discuss the reasonableness and proportionality of the preservation. If the parties are unable to resolve a preservation issue, then the issue should be promptly raised with the Court.
- e) Consistent with Proportionality Principle 1.03, the parties should discuss limiting the preservation, search, review, and production requirements imposed on each party by determining what ESI sources can be excluded from preservation and production because they are marginally relevant or not reasonably accessible.

Principle 2.02 (Conference of the Parties)

- a) In cases involving ESI, a conference of the parties is helpful. Before such a conference, counsel should discuss who will participate with their clients and each other to ensure the participation of one or more persons for each party who are well-informed concerning the potentially relevant systems and data.
- b) Topics the parties should be prepared to discuss include:
 - 1) The sources, scope, and type of ESI that has been and will be preserved, including: date ranges; identity and number of potential custodians or sources; preservation and production by third parties in possession of relevant ESI, and their costs, capabilities, and policies; and other details that help clarify the scope of preservation;
 - 2) The appropriate form and forms of production;
 - 3) Any difficulties or exceptional costs related to preservation;
 - 4) Search and culling methodologies (including keywords or technology assisted review, as appropriate) and suitable methods to query and produce responsive ESI;
 - 5) The phasing of discovery, where appropriate, to prioritize discovery from custodians or sources most likely to contain discoverable information, including ESI, and those accessible at the lowest cost; and, as warranted, to defer or avoid discovery from sources unlikely to contain discoverable information or that are costliest to access;
 - 6) The potential need for a protective order (see, e.g., Local Rule 104.13 and Appendix D), “clawback” agreement, and any procedure pursuant to Fed. R. Evid. 502(d) or (e), including a Rule 502(d) order; and
 - 7) Opportunities to reduce costs and increase the efficiency and speed of the discovery process.

A more detailed checklist of information that may be helpful in guiding such discussions is included as Appendix 1: Suggested Topics for ESI Discussion. The Court encourages the parties to address any agreements or disagreements related to the above matters in the status report required by the scheduling order.

Principle 2.03 (E-Discovery Liaison)

In many cases, and where consistent with the proportionality factors in Rule 26(b), the discovery of ESI will be aided by the participation of electronic discovery liaisons. In addition, if a dispute arises that involves technical aspects of electronic discovery, as part of its obligations under Local Rule 104 concerning discovery disputes, each party should consider appointing an ESI liaison who will be well-informed concerning the relevant systems and information. An ESI liaison should be knowledgeable about the location, nature, accessibility, format, collection, searching, authenticity, integrity, and production of ESI in the matter. The ESI liaison should, at a minimum:

- a) Be prepared to participate in the resolution of any discovery disputes relating to ESI so as to limit the need for Court intervention;
- b) Be knowledgeable about the party's ESI discovery efforts;
- c) Be familiar with, or gain knowledge about, the party's electronic systems and capabilities in order to explain those systems and answer related questions; and
- d) Be familiar with, or gain knowledge about, the technical aspects of electronic discovery in the matter, including electronic document storage and organization, form/format issues, accessibility, and relevant information retrieval technology (including search methodology).

- e) The failure to appoint an ESI liaison in a case where one is appropriate is one factor the Court may consider in granting relief in any discovery dispute or request for sanctions.

Principle 2.04 (Production of ESI)

- a) Production Format: Production will be (1) in any form or forms agreed to by the parties, or (2) if no agreement is reached, in any reasonable form or forms specified by the requesting party if such format is consistent with Proportionality Principle 1.03, including native production. However, no party shall be compelled, except by Court order, to accept production in a form that substantially degrades or jeopardizes the utility, integrity, and/or authenticity of ESI. The parties may wish to discuss the use of a mutually accessible third-party service for the storage and sharing of discovery documents to minimize potential costs. Sample production protocols are attached as Appendix 2.
- b) Privilege Logs: The parties should confer about the nature and scope of privilege logs for the case, including whether categories of information may be excluded from any logging requirements and whether an alternative to a document-by-document log will suffice.
- c) The Discovery of Search Methodologies and Litigation Hold Material: Depending on the circumstances of a particular case, communications implementing or otherwise facilitating efforts to comply with the duty to preserve information, review for privileged information, or cull for responsive documents may or may not be protected from disclosure and discovery under Fed. R. Civ. P. 26. Unless the parties reach an agreement as to the production of this material, questions of discovery of this material are a matter of substantive law that will be decided on a case-by-case basis. Parties discussing these issues may wish to consider the use of a Fed. R. Evid. 502(d) order.

- d) Metadata: Metadata is an important part of ESI and should be considered for production in every case. The production of metadata should be consistent with the proportionality principles of Fed. R. Civ. P. 26 and Principle 1.03. A detailed discussion of metadata can be found in Appendix 3: Metadata Reference Guide.
- e) Cost-Shifting: Parties are generally responsible for their own costs of production of ESI. However, electronic discovery costs may be shifted in accordance with the applicable provisions of Fed. R. Civ. P. 26. Likewise, a party's nonresponsive or dilatory discovery tactics may prompt cost-shifting considerations. Cost-shifting can be negotiated by agreement of the parties or requested by appropriate motion to the Court.
- f) Integrity of ESI: Parties should discuss how to produce the metadata and/or native files so that ESI maintains its integrity from when it is collected until when it is used in proceedings so that the parties have a method to confirm the integrity of the ESI throughout the litigation.

Principle 2.05 (Disputes Regarding ESI)

Disputes regarding ESI that the parties are unable to resolve shall be presented to the Court at the earliest reasonable opportunity. If the Court determines that any party or counsel has failed to cooperate and participate in good faith in electronic discovery or the Local Rule 104 process (including by the failure to appoint an ESI liaison under Principle 2.03, where appropriate), the Court may require additional discussions between the parties, order the appointment of an ESI liaison, and, if warranted, may consider discovery sanctions, including costs to the aggrieved party.

EXPECTATIONS OF COUNSEL

Principle 3.01 (Preparedness of Counsel)

It is expected that counsel for the parties, including all counsel who have appeared, as well as all others responsible for making representations to the Court or opposing counsel (whether or not they make an appearance), will be familiar with the following:

- a. The electronic discovery provisions of the Federal Rules of Civil Procedure, including Rules 26, 33, 34, 37, and 45, and Federal Rule of Evidence 502;
- b. The applicable rules of professional responsibility and other duties of counsel that are relevant to electronic discovery; and
- c. The Local Rules and Discovery Guidelines (Appendix A) of this Court.

APPENDICES

Appendix 1: Suggested Topics for ESI Discussions

Appendix 2: Sample Production Protocols

Appendix 3: Metadata Reference Guide

Appendix 1: Suggested Topics for ESI Discussions

Early discussions are often helpful in cases involving ESI. Potential topics for the parties to discuss may, in the appropriate case, include the following, subject to the proportionality analysis contained in Rule 26 of the Federal Rules of Civil Procedure and Proportionality Principle 1.03:

Preservation

1. What are the key factual issues of the case?
2. What are the sources of potentially responsive ESI? Who are the custodians?
3. Can the custodians/sources be prioritized?
4. What are the date ranges for which data should be preserved?
5. Is an organizational chart encompassing the potentially responsive custodians available?
6. Is a data map encompassing the potentially responsive custodians available? What ESI sources exist from which data should be preserved? This could include, but not be limited to, data that is on premise, off-site and in the cloud; structured and unstructured data; network and standalone equipment; applications; removable storage; phones, tablets, mobile devices; social media; voice messaging; and instant messaging systems.
7. What repositories may contain relevant data, but are not reasonably accessible because of undue burden or cost? Will such repositories be preserved?
8. What repositories may contain relevant data, but will not be preserved?
9. What are each party's pertinent information management policies, computer usage policies, retention and destruction policies, "Bring Your Own Device" (BYOD) policies, and any other policies related to information management or governance?
10. Which non-custodial repositories should be preserved? Examples include department share drive, ShareFile locations, etc.
11. Has automatic deletion and purging of potentially responsive ESI been suspended?
12. What methodologies will be used to preserve and collect ESI? Will they account for chain of custody, integrity of ESI, and pertinent metadata and audit trail information?
13. Are there third parties who may possess potentially responsive ESI? If such third parties exist, how will that data be preserved?
14. Are there any disputes related to preservation that need to be presented to the Court for resolution?

Liaison

1. The parties should discuss whether each side will designate an ESI liaison for the duration of the litigation; and
2. If so, how they will be utilized.

Collection

1. What has been preserved; what will be collected?
2. How will it be collected?
3. How will it be processed?

4. Will phased collection and processing be efficient for the case?
5. Is there an agreement on a method for dealing with collection exceptions for which remediation is impossible or too costly?

Search

1. What methods of searching the data will be used to identify responsive ESI and filter out ESI that is not responsive?
2. Parties may discuss, if and as applicable, search and review methodologies and technologies.
3. Parties may discuss whether or not a search protocol should be presented to the Court for prior approval.

Production

1. In what forms and formats will ESI be produced, including decisions concerning:
 - a. Which metadata fields, if any, will be provided;
 - b. Whether OCR should be produced for non-text searchable files;
 - c. The form and format of load files, if any, accompanying the production of documents;
 - d. The naming conventions and Bates numbering of produced documents, including native files, full-text documents, OCRRed documents and images;
 - e. What, if any, files should be produced in native format;
 - f. The image format, if any, to be produced;
 - g. Whether the parties shall produce ESI in phases; and
 - h. The media upon which the ESI productions will be delivered.
2. Are there any security or privacy issues applicable to any produced ESI?

Privilege

1. The parties should discuss a plan for dealing with privileged information, including obtaining an order from the Court pursuant to Fed. R. Evid. 502, if necessary.
2. The parties should discuss, if necessary, the production, exchange, and format of privilege logs.

Appendix 2: Sample Production Protocols

One of the easiest ways to minimize waste and unnecessary dispute is for parties to reach early agreement on the form or forms of production. Where the parties have not already agreed upon a production protocol, these sample production protocols are offered as a starting point for negotiation of the form or forms in which electronically stored information (“ESI”) is exchanged. Any production protocol should be tailored to the needs of the parties and to the types of systems and data subject to discovery. If appropriate, the parties may discuss the procedure for maintaining the integrity of produced ESI throughout the litigation.

These sample protocols attempt to suggest best practices as of the writing of this appendix. As the types of ESI and the tools used to support electronic discovery evolve over time, so too must the manner in which ESI is produced. An overview of each sample is included below.

Appendix 2.1: Hybrid Production Protocol – This protocol permits the conversion of ESI to static image format. By creating a static image of each page, the parties are able to cite to a normalized representation of each page, aiding in creating a clearer record. Though searchability and application metadata is stripped away by image conversion, it is largely restored by the production of attendant extracted or OCR text and metadata in ancillary “load files.” Imaged production protocols necessitate upfront expenditure to convert records, much of which may never be used in proceedings. Furthermore, the conversion of all produced ESI to image increases the size of the files ultimately exchanged, which has the potential to increase downstream processing and storage costs. To ameliorate some of these shortcomings, this hybrid production protocol provides for production of certain ESI in native formats, cross-referenced to Bates numbered image placeholders. This protocol assumes the parties have access to the resources and litigation support software required to generate and work with images and load files.

Appendix 2.2: Native Production Protocol – This protocol recognizes that conversion of ESI from its native format may impose an undue burden on the parties and may render the production less complete and usable. A native production permits technically-proficient parties to make more efficient use of the production and enables parties with limited resources to utilize low-cost and commonly-available tools to conduct search and review, eliminating the need to procure additional software required to pair images with text and metadata. Moreover, native productions offer greater flexibility, and because of their smaller size, native formats can reduce the cost to process and store data on a per-gigabyte basis. For use in proceedings, parties may wish to convert selected native documents to static images or present the information digitally. In the case of the former, the parties may consider reaching agreement on the procedure for stipulation to the image format.

Appendix 2.1

Sample HYBRID PRODUCTION PROTOCOL

1. “Information items” as used here encompasses individual documents and records (including associated metadata), whether on paper, as discrete “files” stored electronically, optically or magnetically, or as a record within a database, archive, or container file. The term should be read broadly to include e-mail, text messages, word processed documents, digital presentations, social media posts, webpages, and spreadsheets.
2. Responsive electronically stored information (“ESI”) (except for spreadsheets, presentation files, or other information items containing speaker notes, animated text, embedded comments, or tracked changes) should be converted to image, Bates numbered, and produced with fully searchable text. A single-page TIFF placeholder bearing the Bates number for each record not converted to image shall also be produced. This Protocol describes the specifications for producing hybrid productions and attendant load files.
3. Images
 - a. Images should be single-page, Group IV TIFF files, scanned at 300 dpi.
 - b. File names cannot contain embedded spaces.
 - c. The number of TIFF files per folder should not exceed 2,000.
 - d. If an information item contains color, it shall be produced in color, unless the color is merely decorative (*e.g.*, company logo or signature block).
4. Image Cross-Reference File

A comma-delimited image cross-reference file (*e.g.*, .OPT or .LFP) to link the images to the metadata and text should be supplied. Such a cross-reference file typically consists of nine fields per line, with a line for every file in the database.

For example, the .OPT format is as follows:

```
ABC00000001,VOL0001,\IMAGES\0001\ABC00000001.TIF,Y,,,4
ABC00000002,VOL0001,\IMAGES\0001\ABC00000002.TIF,,,,
ABC00000003,VOL0001,\IMAGES\0001\ABC00000003.TIF,,,,
ABC00000004,VOL0001,\IMAGES\0001\ABC00000004.TIF,,,,
```

5. Text

Searchable text of the entire document must be provided for every record, at the document level.

- a. Searchable text must be provided for all documents that originated in electronic format but are not produced in their native forms. Text files should include page breaks that correspond to the pagination of the image files. Any document in which

text cannot be extracted must be processed using optical character recognition (OCR), including PDFs without embedded text.

- b. OCR text must be provided for all documents that originated in hard copy format. A page marker should be placed at the beginning, or end, of each page of text, *e.g.*, *** IMG0000001 *** whenever possible. The data surrounded by asterisks is the ImageID.
- c. For redacted documents, provide the full text for the redacted version.
- d. Text should be delivered as multi-page ASCII text files with the files named to conform to the ImageID field. Text files should be placed in separate subfolders with each subfolder limited to 500 files.

6. Data File

The data file (*e.g.*, .DAT or .CSV) is another delimited file containing all of the fielded information and associated metadata for each information item produced.

- a. The first line of the data file must be a header row identifying the field names.
- b. Date fields should be provided in the format: MM/DD/YYYY.
- c. All family relationships should be preserved, and all attachments should sequentially follow the parent document/email.
- d. All metadata associated with email, audio, and native electronic document collections must be produced per the table below.
- e. In some cases, it may be appropriate to specify the data file delimiters for certain litigation support systems. For example, default .DAT file delimiters for Concordance are:

Comma	,	ASCII character (020)
Quote	"	ASCII character (254)
Newline	␣	ASCII character (174)

The text and metadata of email and attachments, and all other native file document collections, should be extracted and provided in a data file using the field definition and formatting described below:

Field Position	Field Name	Type	Description/Metadata
1.	BEGDOC	Paragraph	Beginning bates number
2.	ENDDOC	Paragraph	Ending bates number
3.	BEGATTACH	Paragraph	Beginning bates number of family
4.	ENDATTACH	Paragraph	Ending bates number of family
5.	ATTCOUNT	Paragraph	Attachment count

Field Position	Field Name	Type	Description/Metadata
6.	PARENTID	Paragraph	Bates number of family parent
7.	DOCDATE	Date	Date of document or creation date (MM/DD/YYYY)
8.	DATESENT	Date	Date Email Sent (MM/DD/YYYY)
9.	TIMESENT	Time	Time Email Sent (HH:MM:SS AM/PM)
10.	DATERECEIVED	Date	Date Email Received (MM/DD/YYYY)
11.	TIMERECEIVED	Time	Time Email Received (HH:MM:SS AM/PM)
12.	TIMEZONE	Paragraph	Time zone used to process custodian data
13.	AUTHOR	Paragraph	Who created document (LASTNAME, FIRST)
14.	FROM	Paragraph	Who is document sent from (LASTNAME, FIRST)
15.	TO	Paragraph	Who is document sent to (LASTNAME, FIRST)
16.	CC	Paragraph	Who is copied on document (LASTNAME, FIRST)
17.	BCC	Paragraph	Who is blind copied on document (LASTNAME, FIRST)
18.	DOCTYPE	Paragraph	What type of document this is (e.g., Message or attachment)
19.	FILEEXT	Paragraph	File Extension (e.g., .msg or .doc)
20.	EMAILSUBJECT	Paragraph	Email subject line
21.	EMAIL MESSAGE ID	Paragraph	Message ID for email
22.	FILENAME	Paragraph	Original file name
23.	LASTMOD	Date	Date last modified (MM/DD/YYYY)
24.	CUSTODIAN	Paragraph	Custodian (LASTNAME, FIRST)
25.	SOURCE	Paragraph	Where did document come from?
26.	ORIGFOLDER	Paragraph	Original file folder (e.g., Personal Folders\Deleted Items\)
27.	PAGES	Number	Number of pages in document
28.	DOCLINK	Paragraph	This will be used if there is a native, path to folder where data LINK record is located
29.	HASH	Paragraph	MD5 or SHA Hash Value (unique file signature)
30.	HASH DE-DUPLICATE	Paragraph	Instances of hash de-duplication (by full path)

Field Position	Field Name	Type	Description/Metadata
	INSTANCES		
31.	CONVERSATION INDEX ID	Paragraph	Microsoft Conversation index number generated by Microsoft Outlook to identify email conversations.

7. Linked Native Files

Spreadsheets must be produced in their native electronic formats. Also, Microsoft Office files, or other information items containing speaker notes, animated text, embedded comments, or tracked changes must be produced in their native electronic formats.

- a. Native file documents must be named per the BEGDOC (beginning bates number).
- b. The full path of the native file must be provided in the .data file for the DOCLINK field.
- c. The number of native files per folder should not exceed 2,000 files.

8. Image Handling

For any records converted to image, the following settings should be applied at conversion.

Microsoft Word		
Option	Setting	Description
Show Track Changes	Yes/No	If yes, 'Final Showing Markup' will be used. If not, 'Final' view will be used.
Show Hidden Text	Yes/No	If yes, text marked as hidden will be printed.
Show Comments	Yes/No	If yes, comments will be printed.
Print Headers	Yes/No	If yes, headers will be printed.
Print Footers	Yes/No	If yes, footers will be printed.
Print Field Codes	Yes/No	If not yes, fields containing PRINT code are cleared to prevent output TIFF corruption.
Use SavedDate Instead of CurrentDate	Yes/No	Any auto date/time fields will be replaced with Saved Date/Time instead of current date.
Use Filename Only for Auto Filename Fields	Yes/No	If yes, any auto filename fields will be printed with just the filename, not the path.
Disable Auto Hyphenation	Yes/No	If yes, auto hyphenation will not be used for foreign language docs.
Microsoft Excel		
Option	Setting	Description
Unhide Columns	Yes/No	If yes, all hidden columns will be printed.
Unhide Rows	Yes/No	If yes, all hidden rows will be printed.
Unhide Worksheets	Yes/No	If yes, all hidden worksheets will be printed.

Unhide Charts	Yes/No	If yes, all hidden charts will be printed.
Print Order	Over Then Down	This is the order that excel pages are printed.
Print Orientation	Portrait/Landscape	This will enforce the print orientation to portrait or landscape.
Paper Size	Letter/Legal	This will force the paper size to letter or legal.
Print Comments	None	Choose where to print comments on the converted image.
Unhide Formulas	Hidden/Visible	If set to Hidden, the cell values will be displayed. If set to Visible, formulas will be displayed.
Set Scaling to Fit	Yes/No	If yes, the width of the Excel file will be squeezed to fit on one page.
Autofit Column and Row Sizes	Yes/No	If yes, height and width is increased to fit contents.
Disable Custom Filters	Yes/No	If yes, custom filters are disabled.
Black Font	Yes/No	If yes, font color of all cells is set to black so that content is displayed.
Reset Print Area	Yes/No	If yes, the print area is reset.
Set Header Margin	0.5	Top margin is checked and adjusted to prevent truncation.
Margin Handling Header	Keep Offset	Define how the margin of the header is calculated.
Set Footer Margin	0.5	Bottom margin is checked and adjusted to prevent truncation.
Margin Handling Footer	Keep Offset	Define how the margin of the footer is calculated.
Use Filename Only For Auto Filename Fields	Yes/No	If yes, auto filename fields will be printed with just the filename, not the path.
Show Auto File Name	Yes/No	If yes, the English code will be shown, not the value.
Show Auto Date	Yes/No	If yes, the English code will be shown, not the value.
Show Auto Time	Yes/No	If yes, the English code will be shown, not the value.
Limit Output to ### Pages	250	The output for each file will be limited to the given number of pages (0 means no limitation)
Microsoft PowerPoint		
Option	Setting	Description
Print Hidden Slides	Yes/No	If yes, all hidden slides will be printed.
Scale to Fit the Paper	Yes/No	If yes, the converted slide will be scaled to fit the page.
Print Comments	Yes/No	If yes, comments will be printed.
Print Type	Unchanged	Number of slides per page. Notes page will print both the slide and the notes on the same page.
Print Notes at End	Yes/No	If yes, all notes will be displayed at the end of the document.
Use Default Theme	Yes/No	Default theme can be used to display text that will not print because it blends within the image.

Appendix 2.2

Sample NATIVE FORMAT PRODUCTION PROTOCOL

1. "Information items" as used here encompasses individual documents and records (including associated metadata), whether on paper, as discrete "files" stored electronically, optically or magnetically, or as a database, archive, or container file. The term should be read broadly to include all forms of electronically stored information (ESI), including but not limited to e-mail, messaging, word processed documents, digital presentations, social media posts, webpages, and spreadsheets.
2. Responsive ESI shall be produced in its native form; that is, in the form in which the information was created, used, and stored by the native application employed by the producing party in the ordinary course of business.
3. If it is infeasible or unduly burdensome to produce an item of responsive ESI in its native form, it may be produced in an agreed upon near-native form; that is, in a form in which the item can be imported into an application without a material loss of content, structure, or functionality as compared to the native form. Static image production formats serve as near-native alternatives only for information items that are natively static images (*i.e.*, faxes and scans).
4. Examples of agreed-upon native or near-native forms in which specific types of ESI should be produced are:

Source ESI	Native or Near-Native Form or Forms Sought
Microsoft Word documents	.DOC, .DOCX
Microsoft Excel spreadsheets	.XLS, .XLSX
Microsoft PowerPoint presentations	.PPT, .PPTX
Microsoft Access Databases	.MDB, .ACCDB
WordPerfect documents	.WPD
Adobe Acrobat documents	.PDF
Photographs	.JPG, .PDF
E-mail	.PST, .MSG, .EML ¹
Webpages	.HTML

¹ Messages should be produced in a form or forms that readily support import into standard e-mail client programs; that is, the form of production should adhere to the conventions set out in RFC 5322 (the Internet e-mail standard). For Microsoft Exchange or Outlook messaging, .PST format will suffice. Single message production formats like .MSG or .EML may be furnished if source foldering metadata is preserved and produced (*see* paragraph 13). For Lotus Notes mail, furnish .NSF files or convert messages to .PST. If your workflow requires that attachments be extracted and produced separately from transmitting messages, attachments should be produced in their native forms with parent/child relationships to the message and container(s) preserved and produced in a delimited text file.

5. Where feasible, when a party produces reports from databases that can be generated in the ordinary course of business (*i.e.*, without specialized programming skills), these shall be produced in a delimited electronic format preserving field and record structures and names. The parties will meet and confer regarding programmatic database productions, as necessary.
6. Information items that are paper documents or that require redaction shall be produced in static image formats, *e.g.*, single-page .TIF or multipage .PDF images. If an information item contains color, it shall be produced in color unless the color is merely decorative (*e.g.*, company logo or signature block).
7. Individual information items requiring redaction shall (as feasible) be redacted natively or produced in .PDF or .TIF format and redacted in a manner that does not downgrade the ability to electronically search the unredacted portions of the item. The unredacted content of each redacted document should be extracted by optical character recognition (OCR) or other suitable method to a searchable text file produced with the corresponding page image(s) or embedded within the image file. Parties shall take reasonable steps to ensure that text extraction methods produce usable, accurate and complete searchable text.
8. Except as set out in this Protocol, a party need not produce identical information items in more than one form and may globally deduplicate identical items across custodians using each document's unique MD5 or other mutually agreeable hash value. The content, metadata, and utility of an information item shall all be considered in determining whether information items are identical, and items reflecting different information shall not be deemed identical. Parties may need to negotiate alternate hashing protocols for items (like e-mail) that do not lend themselves to simple hash deduplication.
9. Production should be made using commercially reasonable electronic media of the producing party's choosing, provided that the production media chosen not impose an undue burden or expense upon a recipient.
10. Each information item produced shall be identified by naming the item to correspond to a Bates identifier according to the following protocol:
 - a. The first four (4) or more characters of the filename will reflect a unique alphanumeric designation identifying the party making production.
 - b. The next nine (9) characters will be a unique, consecutive numeric value assigned to the item by the producing party. This value shall be padded with leading zeroes as needed to preserve its length.
 - c. The final six (6) characters are reserved to a sequence beginning with a dash (-) followed by a four (4) or five (5) digit number reflecting pagination of the item when printed to paper or converted to an image format for use in proceedings or when attached as exhibits to pleadings.
 - d. By way of example, a Microsoft Word document produced by ABC Corporation in its native format might be named: ABCC000000123.docx. Were the document printed out

for use in deposition, page six of the printed item must be embossed with the unique identifier ABCC000000123-00006.

11. Information items designated "Confidential" may, at the Producing Party's option:

- a. Be separately produced on electronic production media or in a folder prominently labeled to comply with the requirements of paragraph ____ of the Protective Order entered in this matter; or, alternatively,
- b. Each such designated information item shall have appended to the file's name (immediately following its Bates identifier) the following protective legend:
~CONFIDENTIAL-SUBJ TO PROTECTIVE ORDER IN CAUSE MDL-13-0123.

When any "Confidential" item is converted to a printed or imaged format for use in any submission or proceeding, the printout or page image shall bear the protective legend on each page in a clear and conspicuous manner, but not so as to obscure content.

12. The producing party shall furnish a delimited load file supplying the metadata field values listed below for each information item produced (to the extent the values exist and as applicable):

Field
BeginBates
EndBates
BeginAttach
EndAttach
Custodian/Source
Source File Name
Source File Path
From/Author
To
CC
BCC
Date Sent
Time Sent
Subject/Title
Last Modified Date
Last Modified Time
Document Type
Redacted Flag (yes/no)
Hidden Content/Embedded Objects Flag (yes/no)
Confidential flag (yes/no)
E-mail Message ID
E-mail Conversation Index
Parent ID
MD5 or other mutually agreeable hash value
Hash De-Duplicated Instances (by full path)

13. Each production should include a cross-reference load file that correlates the various files, images, metadata field values and searchable text produced.

Questions and Answers about the Native Production Protocol

- Q. If our company used a PDF or TIFF file in the ordinary course of business, do we have to convert that to some “native” form?
- A. No, if the information item originated natively in the usual course of business (such as by scanning a paper document to PDF or a receiving a fax as a TIFF image), those forms are the native forms and should not be converted to another form.
- Q. If we have a printout of a document and an electronic version that we think is the file used to create the printout, do we have to deduplicate them? Which do we produce?
- A. No, this protocol recognizes that they are not the same. The electronic file holds more information than the printed page (*e.g.*, comments and application metadata) and the printout may reflect different information (*e.g.*, signatures, highlighting, and margin notes). Furthermore, the electronic version is inherently searchable and sortable by metadata, where the paper document is not. If responsive, you produce both, as they are not identical under the protocol.
- Q. So, what items are identical and must be deduplicated?
- A. Only items with matching hash values are deemed sufficiently identical that just one instance need be produced. If you have been deduplicating in other matters or producing as TIFF images and load files, computing and matching hash values is something you already do. If not, it’s a very low-cost undertaking that saves a lot of wasted effort and money.
- Q. Won’t it cost more to produce in native and near-native forms?
- A. No. The forms of production in this protocol require considerably fewer steps because there is no need to convert the items from the forms in which the parties use and store them in the ordinary course of business to other, less utile and complete forms. Further, producing in native and near-native forms minimizes the expensive and error-prone processes of extracting searchable text and converting it to images. Especially with Microsoft Office productivity formats (Excel, Word, and PowerPoint documents), conversion to image formats significantly downgrades utility and completeness of the evidence.
- Q. But won’t we lose the ability to Bates number production? I want my Bates numbers!

A. Not at all. Electronic productions are “Bates numbered” consecutively, and when items are printed out or imaged for use in proceedings or as exhibits, they will bear embossed Bates numbers, page numbers, and protective legends, just as they always have. What changes is that you don’t have to emboss all that on each page until you actually need that information in a paginated format. Still, the electronic forms always carry a Bates number (in their file name) and even a protective legend for items designated “confidential.” It’s a little different than paper, but then, ESI is a lot different than paper. This protocol saves a great deal of money without adding complexity, so the difference is a change for the better.

Q. Footnote 1 states: “[T]he form of production [for e-mail] should adhere to the conventions set out in RFC 5322.” What does that mean?

A. It’s just a shorthand way to tell your technical people they shouldn’t downgrade the e-mail for production. RFC 5322 is the current international Internet standard that sets out what needs to be present in an e-mail for it to be complete and functional. By using any of the everyday forms of e-mail that are RFC 5322-compliant (*e.g.*, PST, MSG, EML, EMLX, MBOX, etc.), you will be preserving the content and structure of the e-mail that allows it to be reviewed in any of the tools that support e-mail, including all major e-discovery platforms. These forms afford the parties maximum flexibility at lowest cost. Plus, they are less costly because they come straight out of the mail servers and archives in RFC 5322-compliant formats. Conversion to TIFF and load files requires costly parsing and processing of e-mail contents with the result that, *e.g.*, message header values needed for threading conversations and message IDs helpful to deduplication are lost or corrupted. Moreover, family relationships between messages and attachments that support efficient review are often lost or misplaced. Trying to dissect and rebuild e-mail messages as TIFF images and load file data often leads to contentious motions, expensive experts, and sanctions, all of which could have been avoided by sticking to the forms e-mails are intended to take.

Q. Why do we have to extract searchable text and embedded metadata values from native and near-native files?

A. You don’t. Unlike TIFF images, native and near-native forms are inherently electronically searchable and carry application metadata within the files. So there’s no need to extract text for search as it’s already in the file produced. The metadata production requirement speaks to production of fields “as applicable.” If the metadata is in the file produced, extracting the same data to a load file is redundant and, accordingly, not “applicable.”

Q. Our lawyers don’t have the tools to review native forms. Their review tools are pretty old and only support review of TIFF images. What do they do?

A. They can keep on using their tools. Native and near-native forms are easily downgraded to forms that lawyers with older tools can manage. That's what they've been doing and one reason why e-discovery has been so costly. Any party who needs downgraded forms of production can go on paying to convert the data for their use. This protocol serves to eliminate that cost and hardship to those capable of dealing with the evidence in the same forms in which the witnesses and parties do. If you don't mind the higher cost, use any old tool you want to review; just *produce* in native and near-native forms.

Q. We want to produce on CDs. Is that an "appropriate" medium of production?

A. That depends upon the volume of data you're producing. If your production can fit on 2-3 CDs, it's appropriate. If your production will span 20 CDs, it's a waste of everyone's time and money to spend hours extracting from 20 CDs what would have taken minutes to pull from a ten buck thumb drive.

Q. We prefer to produce as TIFF images because then no one can see the hidden metadata—like collaborative comments, speaker notes, formulas, tracked changes, and such. Isn't that just metadata?

A. The information listed is user-generated content, and dismissing it as "just metadata" doesn't justify its eradication. It is evidence, like margin notes on paper documents and comments written on Post-Its. If you've been ignoring it without consequence, consider yourself lucky. This protocol treats it as part and parcel of the ESI to be produced.

Q. If we don't convert everything to TIFF or PDF, what will prevent you from changing the evidence? Aren't TIFF and PDF images harder to alter than native forms?

A. Nothing prevents a dishonest litigant from seeking to change the evidence, save the certainty that any change important enough to impact the outcome of a case will be checked against the source and exposed. Because of the ability to digitally fingerprint or "hash" native and near-native productions, it's far easier to quickly and reliably detect alterations. Contrary to popular misconceptions, it's simple to alter TIFF and PDF files in ways that are difficult for a reader to detect. Adobe Acrobat has supported extensive editing of PDF files for years. TIFF images are just pictures, so can be modified using the same off-the-shelf tools used to enhance snapshots. It's an urban myth that producing TIFFs and PDFs is more secure.

Q. Why must MD5 hashes of each production item be furnished?

A. Though parties are free to negotiate an agreement to produce alternate metadata, parties are cautioned to always calculate, supply, and preserve the hash value of each electronic information item produced as a simple and reliable method by which to ascertain if an item has been inadvertently or deliberately altered following production.

Appendix 3: Metadata Reference Guide

Metadata is information that helps us use and make sense of other information. More particularly, metadata is information, typically stored electronically, that describes the characteristics, origins, usage, structure, alteration, and validity of other electronically stored information (“ESI”). Metadata occurs in many forms within and without digital files. Some is supplied by the user, but most metadata is generated by systems and software.

Some define metadata simply as “data about data,” where others characterize metadata as data that is not user-generated but is created by a computer system or application to keep track of a file’s attributes. However, even user-generated data may qualify as metadata. For example, a Bates number is metadata, although assigned by counsel.

Because metadata is defined so broadly, a blanket request for the production of metadata may be unhelpful. The metadata values associated with a particular file or information item vary according to the nature of the item and its use. For example, the relevant metadata from a word processed document differs from e-mail metadata and from metadata pertinent to a database.

Metadata is unlike almost any other discoverable information because its import may flow from its probative value as relevant evidence, its utility in functionally abetting the searching, sorting, and interpretation of ESI, or both. If the origin, use, distribution, destruction, or integrity of electronic evidence is at issue, the relevant “digital DNA” of metadata is probative evidence that should be preserved and produced. Likewise, if the metadata materially facilitates the searching, sorting, and management of ESI, it should be preserved and produced for its utility.

Absent a specific agreement between parties or instruction from the Court as to the form or forms of production, parties typically produce information in the form or forms the information is ordinarily maintained or in some other reasonably usable form. In determining what form or forms to produce data, a producing party should take into account the need to make metadata as accessible both to display and to search, for the receiving party as it is to the producing party, where appropriate and necessary, after consideration of proportionality factors outlined in Principle 1.03.

Metadata can be generally categorized as System Metadata or Application Metadata.

System Metadata reflects context, being information about a file that is not embedded within the file it describes, but is stored externally by the computer’s file management system, which uses system metadata to track file locations and store demographics about each file, *e.g.*, file name, size, creation, modification, and usage. System metadata may be crucial to electronic discovery because so much of our ability to identify, find, sort, and cull information depends on its system metadata values. For example, system metadata helps identify the custodians of files, when files were created or altered, and the folders in which they were stored.

Other metadata, called Application Metadata, reflects content. It is information that the software application creates and stores within the file. As an example, Microsoft Word stores the date when a document was last printed and the time expended editing the document.

The following are suggestions for producing different types of metadata.

1. Application metadata is, by definition, embedded within native files; so native production of ESI obviates the need to selectively preserve or produce application metadata. When ESI is converted to other forms for production, the producing party should assess what metadata will be lost or corrupted by conversion and identify, preserve, and extract relevant or useful application metadata fields for production. The extracted metadata is produced in ancillary production formats called “load files,” designed to be ingested by tools used to review electronic documents. Not all metadata lends itself to production in load files because some metadata (like tracked changes in a Word document) must be seen in context within the native application or an e-discovery review platform.
2. For e-mail messages, this is a fairly straightforward process, notwithstanding the dozens of metadata values that may be introduced by e-mail client and server applications. The metadata essentials for e-mail messages are typically:
 - Custodian – Owner of the mail container file or account collected;
 - To – Addressee(s) of the message;
 - From – The e-mail address of the person sending the message;
 - CC – Person(s) copied on the message;
 - BCC – Person(s) blind copied on the message;
 - Date Sent – Date the message was sent;
 - Time Sent – Time the message was sent with UTC/UMG offset;
 - Subject – Subject line of the message;
 - Date Received – Date the message was received;
 - Time Received – Time the message was received;
 - Attachments – Name(s) or other unique identifier(s) of attachments;
 - Mail Folder Path – Path of the message from the root folder to the mail folder (to permit the threading of messages as a “conversation”);
 - Message ID – Microsoft Outlook or similar unique message identifier; and
 - In-Reply-To – Microsoft Outlook or similar unique message identifier.
3. Other Mail Metadata: E-mail messages that traverse the Internet contain so-called “header data” detailing the routing and other information about message transit and delivery. Header data may be useful to address questions concerning authenticity, receipt, or timing of messages. Certain header values are essential to support the ability to thread messages into intelligible conversations. Metadata essentials may also include metadata values generated by the discovery and production process itself,

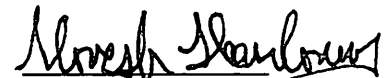
such as Bates numbers and ranges, hash values, production paths, extracted or OCR text, family designations, and time zone offset values.

4. The system metadata values that should typically be considered for preservation and production include:
 - File name;
 - File size;
 - File path;
 - Last modified date and time; and
 - Source or custodian.
5. Parties should discuss the production of metadata at an early practicable stage in the litigation and use proportionality principles in determining the scope of such production. The fields of metadata to be produced, if any, and the form(s) of production should be addressed by the parties and memorialized in a written agreement.

EXHIBIT DELTA

4. I am waiting for The Court to rule on the prior filed ex-parte motion (*See*, Dkt. No. 4), so that hopefully I will have ECF Filing privileges, so I can complete and file the amended complaint electronically using the ECF filing system.
5. Pursuant to The Court's Jan. 21st order, I am filing the enclosed 'Related Case Order' AND the 'Certificate of Interested Persons Order,' that has been filled out to the extent possible, and are contained herein.
6. I will serve the documents noted in ¶5, on the known and named parties, within 1-week of today (Feb. 04, 2020), and will notify The Court once the mailing has been completed.
7. Since I don't know the office addresses of Defendants Thomas Miller, Sonya Yongue, Paul Wysopal, and Regina Lombardo, I will mail/serve them the documents noted in ¶5, at the FBI Headquarters and the BATFE/ATF Headquarters.

Respectfully submitted,
pro se, mentally and physically disabled Plaintiff,



Umesh Heendeniya

P. O. Box 5104

Spring Hill, FL-34611

(508)-630-6757

umeshheendeniyavsthefbi@gmail.com

Dated : Feb. 04, 2020-

**CERTIFICATE OF INTERESTED PERSONS
AND CORPORATE DISCLOSURE STATEMENT**

I hereby disclose the following pursuant to this Court's interested persons order:

1.) the name of each person, attorney, association of persons, firm, law firm, partnership, and corporation that has or may have an interest in the outcome of this action — including subsidiaries, conglomerates, affiliates, parent corporations, publicly-traded companies that own 10% or more of a party's stock, and all other identifiable legal entities related to *any* party in the case:

Based on information, and legal knowledge and factual knowledge that is known to Heendeniya at the present time, the answer is None.

2.) the name of every other entity whose publicly-traded stock, equity, or debt may be substantially affected by the outcome of the proceedings:

Based on information, and legal knowledge and factual knowledge that is known to Heendeniya at the present time, the answer is None.

3.) the name of every other entity which is likely to be an active participant in the proceedings, including the debtor and members of the creditors' committee (or twenty largest unsecured creditors) in bankruptcy cases:

Based on information, and legal knowledge and factual knowledge that is known to Heendeniya at the present time, the answer is None.

4.) the name of each victim (individual or corporate) of civil and criminal conduct alleged to be wrongful, including every person who may be entitled to restitution:


Based on information, and legal knowledge and factual knowledge that is known to Heendeniya at the present time, the answer is None.

I hereby certify that, except as disclosed above, I am unaware of any actual or potential conflict of interest involving the district judge and magistrate judge assigned to this case and will immediately notify the Court in writing on learning of any such conflict.

[Date]

February 04, 2020.

[Certificate of Service]


[Counsel of Record or Pro Se Party]
[Address and Telephone]

I will mail and/or email this document to the known and named parties within 1-week of filing this document.

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL - 34611.
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION**

UMESH HEENDENIYA,

Plaintiff,

v.

Case No: 8:20-cv-114-T-02SPF

THOMAS MILLER, SONYA YONGUE,
DAVID KORTMAN, ALVIN NIENHUIS,
HERNANDO COUNTY SHERIFF'S OFFICE,
PAUL WYSOPAL, REGINA LOMBARDO
and JOHN DOES,

Defendants.

NOTICE OF PENDENCY OF OTHER ACTIONS

In accordance with Local Rule 1.04(d), I certify that the instant action:



IS

related to pending or closed civil or criminal case(s) previously filed in this Court, or any other Federal or State court, or administrative agency as indicated below:

See, attached document marked as "Exhibit A".

 IS NOT

related to any pending or closed civil or criminal case filed with this Court, or any other Federal or State court, or administrative agency.

I further certify that I will serve a copy of this NOTICE OF PENDENCY OF OTHER ACTIONS upon each party no later than fourteen days after appearance of the party.

Dated:

February 04, 2020.

Counsel of Record or Pro Se Party

[Address and Telephone]

Umesh Heendeniya

P. O. Box 5104

Spring Hill, FL - 34611.

(508)-630-6757

umeshheendeniyavsthefbi@gmail.com

EXHIBIT A

Notice of Pendency of Other Actions

The following 2 cases where the Plaintiff is Heendeniya,

1. *Heendeniya vs. St. Joseph's Hospital Health Center, et al.*, 15-CV-01238-GTS-TWD (N.D. New York Oct. 19, 2015);
2. *Heendeniya vs. St. Joseph's Hospital Health Center, et al.*, 18-3553 (2d Cir. Nov. 27, 2018),

did contain at some point in time, 2 of the Defendants, presently named in the instant lawsuit:

1. Paul Wysopal, FBI Special Agent in Charge (SAC) of The Tampa-Orlando Field Office;
2. Regina Lombardo, BATFE Special Agent in Charge (SAC) of The Tampa-Orlando Field Office.

However, both Defendants were dismissed on Feb. 25, 2016 by the N.D. New York before any of the Defendants in that lawsuit were served with summons and complaint. But, the key point is, they were not dismissed due to a final judgment based on the merits of the claims.

This point is demonstrated by the following controlling authorities:

The doctrine of res judicata, or claim preclusion, bars the parties to an action from litigating claims that were or could have been litigated in a prior action between the same parties. *Jaffree v. Wallace*, 837 F.2d 1461, 1466 (11th Cir.1988). The party asserting claim preclusion as a defense must establish four elements: (1) the prior decision must have been rendered by a court of competent jurisdiction; (2) there must have been a final judgment on the merits; (3) both cases must involve the same parties or their privies; and (4) both cases must involve the same causes of action. *In re Piper Aircraft Corp.*, 244 F.3d 1289, 1296 (11th Cir.2001). We review a claim preclusion decision de novo. *Id.* at 1295.

Lobo v. Celebrity Cruises, Inc., 704 F. 3d 882, 892 (11th Cir. 2013).

'When deciding whether claims are barred by res judicata, federal courts apply the law of the state in which they sit. *Burr & Forman v. Blair*, 470 F.3d 1019, 1030 (11th Cir.2006) (citing *NAACP v. Hunt*, 891 F.2d 1555, 1560 (11th Cir.1990)).' *Starship Enterprises of Atlanta, Inc. v. Coweta County*, 708 F. 3d 1243 (11th Circuit February 14, 2013).

The purpose of the res judicata doctrine is that the "full and fair opportunity to litigate protects [a party's] adversaries from the expense and vexation attending multiple lawsuits, conserves judicial resources and fosters reliance on judicial action by minimizing the possibility of inconsistent decisions." *Ragsdale v. Rubbermaid, Inc.*, 193 F.3d 1235, 1238 (11th Cir. 1999) (quoting *Montana v. U.S.*, 440 U.S. 147 (1979)). "Res judicata bars the filing of claims which were raised or could have been raised in an earlier proceeding." *Id.* "[A] claim will be

barred by prior litigation if all four of the following elements are present: (1) there is a final judgment on the merits; (2) the decision was rendered by a court of competent jurisdiction; (3) the parties, or those in privity with them, are identical in both suits; and (4) the same cause of action is involved in both cases." *Id.*

Thomas v. City of Lakeland, 16CV2029 (M.D. Florida July 07, 2017).

The doctrine of collateral estoppel precludes a party from relitigating an issue that was fully litigated in a previous action. The courts have recognized three prerequisites to the application of the doctrine:

- 1) that the issue at stake be identical to the one involved in the prior litigation;
- 2) that the issue have been actually litigated in the prior litigation; and
- 3) that the determination of the issue in the prior litigation have been a critical and necessary part of the judgment in that earlier action.

Stovall v. Price Waterhouse Co., 652 F.2d 537, 540 (5th Cir. 1981); see *Rufenacht v. Iowa Beef Processors, Inc.*, 656 F.2d 198, 202 (5th Cir. 1981).[2]

Collateral estoppel may be used by the defendant to preclude the plaintiff from relitigating an issue he has lost in a prior case (defensive collateral estoppel) or by a plaintiff to preclude the defendant from relitigating such an issue (offensive collateral estoppel).

Deweese v. Town of Palm Beach, 688 F. 2d 731, 733(11th Cir. 1982).

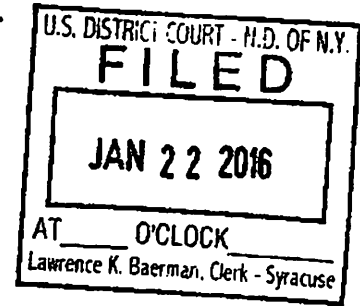
"Nonappealable interlocutory orders are not entitled to collateral estoppel or res judicata effect" Lobo v. Celebrity Cruises, Inc., 704 F. 3d 882, 892 (11th Cir. 2013).

"This court reviews a district court's conclusions on res judicata and collateral estoppel de novo and the legal conclusion that an issue was actually litigated in a prior action under the clearly erroneous standard." *Richardson v. Miller*, 101 F.3d 665, 667-68 (11th Cir. 1996).’ Wiggins v. Loar, 18-12012 (11th Circuit January 14, 2019).

After the unlawful and coerced interrogation, on Jan. 15, 2016 (Almost 3 months after I had filed the lawsuit in the Federal District Court for the N.D. of New York), that I was subjected to by Defendants in the instant lawsuit FBI Agents Thomas Miller and Sonya Yongue, and Hernando County Sheriff’s Detective David Kortman, who were attached to the Tampa-Orlando JTTF, I filed the following 2 documents with the Federal District Court for the N.D. of New York (Dkt. Nos. 11 and 12). Relevant pages from those 2 filings are attached herein, demarcated as ‘Exhibit A-1’ and ‘Exhibit A-2.’

EXHIBIT A-1

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**



UMESH HEENDENIYA,)
) **Plaintiff,**)
) **v.**)
))
ST. JOSEPH'S HOSPITAL HEALTH CENTER;)
ROGER GARY LEVINE, MD; LISA MARIE)
O'CONNOR, MD; GEORGE O. TREMITI, MD;)
HORATIUS ROMAN, MD; JOANNE MARY)
FRENCH, RN; WENDY BRISCOE, RN; SUSAN)
LYNN CATE, LMFT; ROSALINE SPUNELKA, RN;)
ROBERT MICHAEL CONSTANTINE, MD;)
MITCHELL BRUCE FELDMAN, MD; CYNTHIA A.)
RYBAK, NP; KATHRYN HOWE RUSCITTO,)
PRESIDENT and CEO; LOWELL A. SEIFTER, JD,)
SENIOR VP and GENERAL COUNSEL; MEREDITH)
PRICE, VP of FINANCIAL SERVICES and CFO;)
DEBORAH WELCH, VP; GAEL GILBERT, RN,)
DIRECTOR; SJHHC DOES 1-5 INCLUSIVE;)
) **Defendants.**)

**Affidavit Regarding Request for
Reasonable Disability Accommodations
From 18 Federal and NY State Persons
and Entities, per Title II, III, and V of
The ADA, Section 504 of The Rehabilitation
Act, and Other Applicable Federal and
State Laws, in Order for Plaintiff
Heendeniya to Purchase and Possess
Firearms and Ammunition.**

STATE OF FLORIDA)
) **ss**
COUNTY OF HERNANDO)

Umesh Heendeniya, being duly sworn, deposes and says:

1. I have been working on completing and filing the Objections to the 'Report and Recommendation' Dated Nov. 30, 2015, and Motion for Reconsideration in regards to the Report and Recommendation, in the above titled legal action.
2. As part of the theory of my case, I am requesting reasonable disability accommodations from 18 (eighteen) federal and New York state persons and entities, per Title II, III, and V of The Americans with Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws, in order for me to purchase and possess firearms and ammunition and thereby exercise my Second Amendment rights.

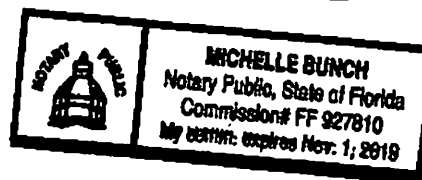
- 3. Therefore, I wrote a letter to each of the 18 federal and NY state persons and entities, requesting reasonable disability accommodations.**
- 4. I mailed 17 of the letters on Saturday, January 16, 2016 using the U.S. postal mailing service offered at an Office Depot store. I mailed the 18th letter, to New York State Office of Mental Health, on Tuesday, January 19, 2016 using the U.S. postal mailing service offered at the Office Depot store.**
- 5. Each letter was 2 (two) pages in length, and had 2 (two) exhibits containing medical documentation attesting to my mental and physical disabilities, and a printout of the docket sheet of the instant case.**
- 6. The first exhibit was 13 (thirteen) pages in length, and the second exhibit was 3 (three) pages in length.**
- 7. The names of the 18 federal and NY state persons and entities that I wrote to requesting reasonable disability accommodations in order for me to exercise my Second Amendment rights are: (i) Honorable Loretta E. Lynch; (ii) Honorable Eric T. Schneiderman; (iii) James B. Comey, Jr., Esq.; (iv) Thomas E. Brandon; (v) A. Lee Bentley, III. Esq.; (vi) Paul Wysopal; (vii) Regina Lombardo; (viii) Dr. Ann Marie T. Sullivan; (ix) Joshua Pepper, Esq.; (x) Michael C. Green; (xi) United States Department of Justice; (xii) Federal Bureau of Investigation; (xiii) Bureau of Alcohol, Tobacco, Firearms and Explosives; (xiv) National Instant Background Check System; (xv) FBI Criminal Justice Information Services Division; (xvi) New York State Office of Mental Health; (xvii) New York State Division of Criminal Justice Services; (xviii) New York State Office of Mental Health - NICS Appeals Office.**
- 8. A true and correct copy of the 7-page receipt from Office Depot, giving each mail recipient's address and U.S. postal tracking number, is annexed hereto as Exhibit 1.**

9. The contents of the 2-page letters that were mailed to 16 (sixteen) of the persons and entities are almost identical. That is because each of them are named defendants in this legal action.
10. The contents of the 2 exhibits that that were mailed to all 18 persons and entities are identical, and were 16 (sixteen) pages in length.
11. The letter I mailed to Mr. Bentley on Jan. 16, 2016, contained an inadvertent error; hence, I corrected the error and mailed a second letter on Monday, January 18, 2016, using the U.S. postal mailing service offered at the Office Depot store.
12. Mr. Bentley is not a named defendant in this legal action. However, I wrote the letter to him requesting reasonable disability accommodations in order for me to exercise my Second Amendment rights, because he is the United States Attorney for the Middle District of Florida and thus has the discretion to prosecute any violations of 18 USC § 922(g)(4) in Hernando County, FL.
13. To save on Xeroxing costs and postage costs, I have only attached to this affidavit, copies of the letters and identical exhibits that were mailed to 2 of the defendants: Honorable Loretta E. Lynch and Honorable Eric T. Schneiderman.
14. A true and correct copy of the 20-page correspondence that was mailed on Jan. 16, 2016, to Hon. Loretta E. Lynch, is annexed hereto as Exhibit 2.
15. A true and correct copy of the 20-page correspondence that was mailed on Jan. 16, 2016, to Hon. Eric T. Schneiderman, is annexed hereto as Exhibit 3.

This concludes my affidavit.

Sworn to before me this 19th day of January, 2016.


Notary Public



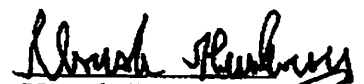

Umesh Heendaniya

EXHIBIT 1







Store:
Office Depot Store 02162
Copy and Print
13173 CORTEZ BLVD
BROOKSVILLE, FL 34613
3526927966

Employee: od02162

Customer Information:
Pro Se Litigant
Umash Heendeniya
P O Box 5104
Spring Hill, FL 34811
Telephone: 5082630145

Ship Date: 01/16/2016

SKU	Description	Price	Recipient Information
 00164826000002244	First Class Mail	\$2.24	Bureau of Alcohol Tobacco Firearm
	Insured Value Fee:	\$0.00	Headquarters
	Delivery Confirmation	\$0.00	99 New York Avenue NE
	Signature Confirmation	\$0.00	
	Insured Value: \$ 0.00		Washington, DC, 20226, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200793853014524	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2016	* Weight entered manually	
 00164826000002244	First Class Mail	\$2.24	Mr Joshua Pepper Esq
	Insured Value Fee:	\$0.00	Deputy Commissioner Office of Col
	Delivery Confirmation	\$0.00	NY State Office of Mental Health
	Signature Confirmation	\$0.00	44 Holland Avenue
	Insured Value: \$ 0.00		Albany, NY, 12229, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200828883224077	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/25/2016	* Weight entered manually	
 00164826000002244	First Class Mail	\$2.24	United States Department of Justice
	Insured Value Fee:	\$0.00	
	Delivery Confirmation	\$0.00	950 Pennsylvania Avenue NW
	Signature Confirmation	\$0.00	
	Insured Value: \$ 0.00		Washington, DC, 20535, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200828883225676	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2016	* Weight entered manually	
 00164826000002244	First Class Mail	\$2.24	Mr Thomas E Brandon
	Insured Value Fee:	\$0.00	Acting Director
	Delivery Confirmation	\$0.00	Bureau of Alcohol Tobacco Firearm
	Signature Confirmation	\$0.00	99 New York Avenue NE
	Insured Value: \$ 0.00		Washington, DC, 20226, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200828883228228	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2016	* Weight entered manually	

**Store:**

Office Depot Store 02182
Copy and Print
13173 CORTEZ BLVD
BROOKSVILLE, FL 34613
3528927988

Employee: cd02182

Customer Information:

Pro Se Litigant
Umash Heendeniya
P O Box 5104
Spring Hill, FL 34611
Telephone: 5082830145

Ship Date: 01/16/2018

SKU	Description	Price	Recipient Information
 00164826000002244	First Class Mail	\$2.24	Mr Michael C Green
	Insured Value Fee:	\$0.00	Executive Deputy Commissioner
	Delivery Confirmation	\$0.00	NY State Division of Criminal Justice
	Signature Confirmation	\$0.00	80 South Swan Street
	Insured Value: \$ 0.00		Albany, NY, 12210, US
	Contents: Other : Docs		
	Tracking #:		
	940011020082883229980	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/25/2018	* Weight entered manually	
 00164826000002244	First Class Mail	\$2.24	NY State Division of Criminal Justice
	Insured Value Fee:	\$0.00	Alfred E Smith Building
	Delivery Confirmation	\$0.00	80 South Swan Street
	Signature Confirmation	\$0.00	
	Insured Value: \$ 0.00		Albany, NY, 12210, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200829883168596	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/25/2018	* Weight entered manually	
 00164826000002244	First Class Mail	\$2.24	NICS Appeals Office
	Insured Value Fee:	\$0.00	OMH Central Files
	Delivery Confirmation	\$0.00	NY State Office of Mental Health
	Signature Confirmation	\$0.00	44 Holland Avenue
	Insured Value: \$ 0.00		Albany, NY, 12229, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200829883167203	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/25/2018	* Weight entered manually	
 00164826000002244	First Class Mail	\$2.24	Mr James B Comey Jr
	Insured Value Fee:	\$0.00	Director
	Delivery Confirmation	\$0.00	Federal Bureau of Investigation Hea
	Signature Confirmation	\$0.00	935 Pennsylvania Avenue NW
	Insured Value: \$ 0.00		Washington, DC, 20535, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200829883170678	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2018	* Weight entered manually	



Store:
Office Depot Store 02162
Copy and Print
13173 CORTEZ BLVD
BROOKSVILLE, FL 34613
3525927966

Employee: od02162

Customer Information:
Pro Se Litigant
Umash Heendeniya
P O Box 5104
Spring Hill, FL 34611
Telephone: 5082630145

Ship Date: 01/16/2016

SKU	Description	Price	Recipient Information
 0016482600002244	First Class Mail	\$2.24	Dr Ann Marie Sullivan
	Insured Value Fee:	\$0.00	Commissioner
	Delivery Confirmation	\$0.00	NY State Office of Mental Health
	Signature Confirmation	\$0.00	44 Holland Avenue
	Insured Value: \$ 0.00		Albany, NY, 12229, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200829883171668	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/25/2016	* Weight entered manually	
 0016482600002244	First Class Mail	\$2.24	Federal Bureau of Investigation
	Insured Value Fee:	\$0.00	Headquarters
	Delivery Confirmation	\$0.00	935 Pennsylvania Avenue NW
	Signature Confirmation	\$0.00	
	Insured Value: \$ 0.00		Washington, DC, 20535, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200881883077524	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2016	* Weight entered manually	
 0016482600002244	First Class Mail	\$2.24	Mr Paul Wysopal
	Insured Value Fee:	\$0.00	Special Agent in Charge SAC
	Delivery Confirmation	\$0.00	Federal Bureau of Investigation
	Signature Confirmation	\$0.00	5525 West Gray Street
	Insured Value: \$ 0.00		Tampa, FL, 33609, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200881883078682	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/20/2016	* Weight entered manually	
 0016482600002244	First Class Mail	\$2.24	Honorable Loretta E Lynch
	Insured Value Fee:	\$0.00	Attorney General of the United Stat
	Delivery Confirmation	\$0.00	950 Pennsylvania Avenue NW
	Signature Confirmation	\$0.00	
	Insured Value: \$ 0.00		Washington, DC, 20530, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200881883079882	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2016	* Weight entered manually	

**Store:**

Office Depot Store 02162
Copy and Print
13173 CORTEZ BLVD
BROOKSVILLE, FL 34613
3525927946

Employee: od02162

Customer Information:

Pro Se Litigant
Umash Heendaniya
P O Box 5104
Spring Hill, FL 34611
Telephone: 5082630145

Ship Date: 01/16/2016

SKU	Description	Price	Recipient Information
	First Class Mail	\$2.24	National Instant Background Check
	Insured Value Fee:	\$0.00	Federal Bureau of Investigation Hes
	Delivery Confirmation	\$0.00	935 Pennsylvania Avenue NW
	Signature Confirmation	\$0.00	Washington, DC, 20535, US
	Insured Value: \$ 0.00		
00164826000002244	Contents: Other : Docs		
	Tracking #:		
	9400110200881883080173	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/23/2016	* Weight entered manually	
	First Class Mail	\$2.24	Honorable Eric T Schneideman
	Insured Value Fee:	\$0.00	NY State Attorney General
	Delivery Confirmation	\$0.00	Empire State Plaza
	Signature Confirmation	\$0.00	2nd Floor Justice Building
	Insured Value: \$ 0.00		Albany, NY, 12242, US
00164826000002244	Contents: Other : Docs		
	Tracking #:		
	9400110200881883088274	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/25/2016	* Weight entered manually	
	First Class Mail	\$2.24	Mr A Lee Bentley III Esq
	Insured Value Fee:	\$0.00	US Attorney Middle District FL
	Delivery Confirmation	\$0.00	400 North Tampa Street
	Signature Confirmation	\$0.00	Suite 3200
	Insured Value: \$ 0.00		Tampa, FL, 33602, US
00164826000002244	Contents: Other : Docs		
	Tracking #:		
	9400110200883821387091	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/20/2016	* Weight entered manually	
	First Class Mail	\$2.24	Ms Regina Lombardo
	Insured Value Fee:	\$0.00	Special Agent in Charge SAC
	Delivery Confirmation	\$0.00	Bureau of Alcoho Tobacco Firearms
	Signature Confirmation	\$0.00	400 North Tampa Street Suite 2100
	Insured Value: \$ 0.00		Tampa, FL, 33602, US
00164826000002244	Contents: Other : Docs		
	Tracking #:		
	9400110200883821387428	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/20/2016	* Weight entered manually	

**Store:**

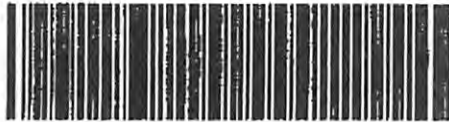
Office Depot Store 02162
Copy and Print
13173 CORTEZ BLVD
BROOKSVILLE, FL 34613
3525927966

Employee: od02162

Customer Information:

Office Depot Store 02162
Umesh Heendeniya
P O Box 5104
Spring Hill, FL 34611
Telephone: 6082830145

Ship Date: 01/16/2016

SKU

0016482600002244

Description

First Class Mail \$2.24
Insured Value Fee: \$0.00
Delivery Confirmation \$0.00
Signature Confirmation \$0.00
Insured Value: \$ 0.00

Contents: Other : Legal Documents

Tracking #:

9400110200528563139026 Weight 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.

Delivery Date: 1/23/2016 * Weight entered manually

Recipient Information

Federal Bureau of Investigation
Criminal Justice Information Service
NICS Section
P O Box 4278
Clarksburg, WV, 26302, US

Total

\$2.24

- I understand that Office Depot is not liable for packages improperly packed.
- I understand that Office Depot will not ship any hazardous materials, as designated by the Department of Transportation, or any other materials restricted by UPS or US Post Office rules. Please see an Office Depot associate if you have any item in question.
- I represent that my description of the materials I am shipping is accurate.
- Packing guidelines and Restricted Items are available at the Copy & Print Depot counter.
- I have declared a value for my package and paid for insurance if optioned.
- To ensure your packages are shipped your receipt must be validated by a cashier at the time of purchase. The validated copy will be retained by the cashier.
- Please retain this receipt as proof of shipment in the event a claim needs to be filed with UPS or USPS.
- USPS claims are to be made by the shipper directly to a local USPS office or through their website www.usps.com
- UPS claims for lost or damaged parcels are to be made at the same Office Depot location the parcels were shipped from.

Customer Signature

**IMPORTANT INFORMATION REGARDING
PACKING SHIPPING PROGRAM**

UPS - Your package can be tracked online at www.ups.com

USPS - Your package can be tracked online at www.usps.com only if you purchased this additional service.



Store:

Office Depot Store 02162
Copy and Print
13173 CORTEZ BLVD
BROOKSVILLE, FL 34813
3525927866

Customer Information:

Pro Se Litigant
Umesh Heendaniya
P O Box 5104
Spring Hill, FL 34611
Telephone: 5082830145

Employee: od02162

Ship Date: 01/18/2016

SKU	Description	Price	Recipient Information
	First Class Mail	\$2.24	Mr A Lee Bentley III Esq
	Insured Value Fee:	\$0.00	United States Attorney
	Delivery Confirmation	\$0.00	Middle District of Florida
	Signature Confirmation	\$0.00	400 North Tampa Street Suite 3200
	Insured Value: \$ 0.00		Tampa, FL, 33602, US
	Contents: Other : Docs		
Tracking #:			
9400110200793854883457 Weight: 0.20 LBS Dim: 12.00 in. x 8.00 in. x 1.00 in.			
Delivery Date: 1/20/2016 * Weight entered manually			

Total \$2.24

- I understand that Office Depot is not liable for packages improperly packed.
- I understand that Office Depot will not ship any hazardous materials, as designated by the Department of Transportation, or any other materials restricted by UPS or US Post Office rules. Please see an Office Depot associate if you have any item in question.
- I represent that my description of the materials I am shipping is accurate.
- Packing guidelines and Restricted Items are available at the Copy & Print Depot counter.
- I have declared a value for my package and paid for Insurance if optioned.
- To ensure your packages are shipped your receipt must be validated by a cashier at the time of purchase. The validated copy will be retained by the cashier.
- Please retain this receipt as proof of shipment in the event a claim needs to be filed with UPS or USPS.
- USPS claims are to be made by the shipper directly to a local USPS office or through their website www.usps.com
- UPS claims for lost or damaged parcels are to be made at the same Office Depot location the parcels were shipped from.

Customer Signature

**IMPORTANT INFORMATION REGARDING
PACKING SHIPPING PROGRAM**

UPS - Your package can be tracked online at www.ups.com
USPS - Your package can be tracked online at www.usps.com only if you purchased this additional service.



Store:

Office Depot Store 02162
 Copy and Print
 13173 CORTEZ BLVD
 BROOKSVILLE, FL 34613
 3525927966

Employee: od02162

Customer Information:

Pro Se Litigant
 Umesh Heendeniya
 P O Box 5104
 Spring Hill, FL 34611
 Telephone: 5082630145

Ship Date: 01/19/2016

SKU	Description	Price	Recipient Information
 0016482600002244	First Class Mail	\$2.24	New York State Office of Mental He.
	Insured Value Fee:	\$0.00	
	Delivery Confirmation	\$0.00	44 Holland Avenue
	Signature Confirmation	\$0.00	
	Insured Value: \$ 0.00		Albany, NY, 12229, US
	Contents: Other : Docs		
	Tracking #:		
	9400110200830013430029	Weight: 0.20 LBS Dim: 9.00 in. x 4.00 in. x 1.00 in.	
	Delivery Date: 1/27/2016	* Weight entered manually	

Total \$2.24

- I understand that Office Depot is not liable for packages improperly packed.
- I understand that Office Depot will not ship any hazardous materials, as designated by the Department of Transportation, or any other materials restricted by UPS or US Post Office rules. Please see an Office Depot associate if you have any item in question.
- I represent that my description of the materials I am shipping is accurate.
- Packing guidelines and Restricted Items are available at the Copy & Print Depot counter.
- I have declared a value for my package and paid for insurance if optioned.
- To ensure your packages are shipped your receipt must be validated by a cashier at the time of purchase. The validated copy will be retained by the cashier.
- Please retain this receipt as proof of shipment in the event a claim needs to be filed with UPS or USPS.
- USPS claims are to be made by the shipper directly to a local USPS office or through their website www.usps.com
- UPS claims for lost or damaged parcels are to be made at the same Office Depot location the parcels were shipped from.

Customer Signature

**IMPORTANT INFORMATION REGARDING
 PACKING SHIPPING PROGRAM**

UPS - Your package can be tracked online at www.ups.com
 USPS - Your package can be tracked online at www.usps.com only if you purchased this additional service.

EXHIBIT 2

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
January 12, 2016

Honorable Loretta E. Lynch
Attorney General of the United States of America
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Re: Request for Reasonable Disability Accommodation Pursuant to Title II, III, and V of the Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and Other Applicable Federal and State Laws, in Order for Me to Exercise my Second Amendment Rights.

Dear Madam:

I am submitting this letter and attached 16 (sixteen) pages of documents to you so that you're put on notice that I'm requesting reasonable disability accommodations from you pursuant to Title II, III, and V of The Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws, in order for me to lawfully exercise my fundamental constitutional right to The Second Amendment rights (per District of Columbia v. Heller, 554 U.S. 570 (2008) and McDonald v. Chicago, 561 U.S. 742 (2010)).

I'm requesting reasonable disability accommodations from you in regards to my Second Amendment rights because I have documented mental and physical disabilities. Thus, I have attached copies of 13 (thirteen) pages of letters and medical reports from my past and current primary-care physicians (PCPs), psychiatrists, and surgeons, as exhibit "A" to this letter, attesting to the diagnosis of my disabilities.

My mental illness diagnosis is-- and has been for more than 8 years-- type-2 manic depression (type-2 bipolar disorder) and post-traumatic stress disorder (PTSD) for which I take daily medications under the guidance of a psychiatrist. I have never had a psychotic or delusional episode in my life, and never been diagnosed by any of my treating physicians as having had one. Nor have I ever been found to have been insane by any medical or legal authority.

I also have significant physical limitations in my right knee which has undergone 2 knee surgeries in 1995 and 1999 respectively, and has significant cartilage damage and resultant pain; a twice-injured, herniated disc injury in my lower back; type-2 diabetes; hyper cholesterol condition; and neuropathy. I take several daily medications for these physical disabilities.

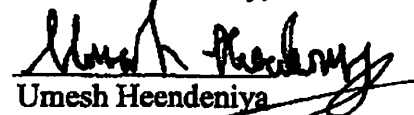
I also have to put you on notice that I have filed a civil rights and medical malpractice lawsuit in the Federal District Court for the Northern District of New York (Syracuse) against you and several other defendants, as part of my attempt to lawfully exercise my fundamental,

constitutional right to The Second Amendment. I have attached a copy of the 3-page docket sheet of the lawsuit to this letter, as exhibit "B." The lawsuit also names as defendants, St. Joseph's Hospital Health Center (henceforth "SJHHC") and several health care providers and staff members, who unlawfully, involuntarily admitted me into SJHHC's psychiatric unit on April 12, 2013 and kept me there for 5 (five) days before releasing me on April 17, 2013.

The SJHHC personnel were aware at that time that I was unemployed and indigent, and thus qualified for free legal representation from the New York state Mental Hygiene Legal Services (henceforth "NY MHLS"). I was never notified by anyone, nor given any paperwork throughout my 5-day, unlawful and involuntary stay at SJHHC informing me that I had the legal right to challenge my unlawful, involuntary admission and treatment in SJHHC's psychiatric unit using the free legal services offered by the NY MHLS. I had never been involuntarily or voluntarily admitted into any psychiatric facility, as an in-patient or as an out-patient, prior to April 12, 2013, and have not been involuntarily admitted into any psychiatric facility, as an in-patient or as an out-patient, since then.

Therefore, I ask you to kindly allow me to exercise my Second Amendment rights (i.e., purchase firearms and ammunition for lawful self-defense and target shooting purposes, possess them in my person, and keep them at home) by being granted reasonable disability accommodations, pursuant to Title II, III, and V of The Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws. Please let me know on or before January 26, 2016, whether you will grant me the above requested reasonable disability accommodations, by either writing to me or emailing me (both addresses are given below). If I don't hear back from you on or before January 26, 2016, I will assume that you thereby are informing and communicating to me that you will not grant me the requested reasonable disability accommodations in order for me to exercise my Second Amendment rights.

Sincerely,



Umesh Heendeniya

P. O. Box 5104

Spring Hill, FL-34611

(508)-263-0145

heendeniyavsjoephshospitalny@gmail.com

EXHIBIT 3

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
January 12, 2016

Honorable Eric T. Schneiderman
New York State Attorney General
Office of the Attorney General
Second Floor, Justice Building, Empire State Plaza
Albany, NY-12224

Re: Request for Reasonable Disability Accommodation Pursuant to Title II, III, and V of the Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and Other Applicable Federal and State Laws, in Order for Me to Exercise my Second Amendment Rights.

Dear Sir:

I am submitting this letter and attached 16 (sixteen) pages of documents to you so that you're put on notice that I'm requesting reasonable disability accommodations from you pursuant to Title II, III, and V of The Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws, in order for me to lawfully exercise my fundamental constitutional right to The Second Amendment rights (*per District of Columbia v. Heller*, 554 U.S. 570 (2008) and *McDonald v. Chicago*, 561 U.S. 742 (2010)).

I'm requesting reasonable disability accommodations from you in regards to my Second Amendment rights because I have documented mental and physical disabilities. Thus, I have attached copies of 13 (thirteen) pages of letters and medical reports from my past and current primary-care physicians (PCPs), psychiatrists, and surgeons, as exhibit "A" to this letter, attesting to the diagnosis of my disabilities.

My mental illness diagnosis is-- and has been for more than 8 years-- type-2 manic depression (type-2 bipolar disorder) and post-traumatic stress disorder (PTSD) for which I take daily medications under the guidance of a psychiatrist. I have never had a psychotic or delusional episode in my life, and never been diagnosed by any of my treating physicians as having had one. Nor have I ever been found to have been insane by any medical or legal authority.

I also have significant physical limitations in my right knee which has undergone 2 knee surgeries in 1995 and 1999 respectively, and has significant cartilage damage and resultant pain; a twice-injured, herniated disc injury in my lower back; type-2 diabetes; hyper cholesterol condition; and neuropathy. I take several daily medications for these physical disabilities.

I also have to put you on notice that I have filed a civil rights and medical malpractice lawsuit in the Federal District Court for the Northern District of New York (Syracuse) against

you and several other defendants, as part of my attempt to lawfully exercise my fundamental, constitutional right to The Second Amendment. I have attached a copy of the 3-page docket sheet of the lawsuit to this letter, as exhibit "B." The lawsuit also names as defendants, St. Joseph's Hospital Health Center (henceforth "SJHHC") and several health care providers and staff members, who unlawfully, involuntarily admitted me into SJHHC's psychiatric unit on April 12, 2013 and kept me there for 5 (five) days before releasing me on April 17, 2013.

The SJHHC personnel were aware at that time that I was unemployed and indigent, and thus qualified for free legal representation from the New York state Mental Hygiene Legal Services (henceforth "NY MHLS"). I was never notified by anyone, nor given any paperwork throughout my 5-day, unlawful and involuntary stay at SJHHC informing me that I had the legal right to challenge my unlawful, involuntary admission and treatment in SJHHC's psychiatric unit using the free legal services offered by the NY MHLS. I had never been involuntarily or voluntarily admitted into any psychiatric facility, as an in-patient or as an out-patient, prior to April 12, 2013, and have not been involuntarily admitted into any psychiatric facility, as an in-patient or as an out-patient, since then.

Therefore, I ask you to kindly allow me to exercise my Second Amendment rights (i.e., purchase firearms and ammunition for lawful self-defense and target shooting purposes, possess them in my person, and keep them at home) by being granted reasonable disability accommodations, pursuant to Title II, III, and V of The Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws. Please let me know on or before January 26, 2016, whether you will grant me the above requested reasonable disability accommodations, by either writing to me or emailing me (both addresses are given below). If I don't hear back from you on or before January 26, 2016, I will assume that you thereby are informing and communicating to me that you will not grant me the requested reasonable disability accommodations in order for me to exercise my Second Amendment rights.

Sincerely,



Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-263-0145

heendeniyavsjoephshospitalny@gmail.com

EXHIBIT A-2

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**

UMESH HEENDENIYA,

Plaintiff,

Civil Action No. 5:15-CV-01238-GTS-TWD

v.

Honorable Glenn T. Suddaby

Honorable Therese Wiley Dancks

ST. JOSEPH'S HOSPITAL HEALTH CENTER;

ROGER GARY LEVINE, MD; LISA MARIE

O'CONNOR, MD; GEORGE O. TREMITI, MD;

HORATIUS ROMAN, MD; JOANNE MARY

FRENCH, RN; WENDY BRISCOE, RN; SUSAN

LYNN CATE, LMFT; ROSALINE SPUNELKA, RN:

ROBERT MICHAEL CONSTANTINE, MD;

MITCHELL BRUCE FELDMAN, MD; CYNTHIA A.

RYBAK, NP; KATHRYN HOWE RUSCITTO,

PRESIDENT and CEO; LOWELL A. SEIFTER, JD,

SENIOR VP and GENERAL COUNSEL; MERED

PRICE, VP of FINANCIAL SERVICES and CFO;

DEBORAH WELCH, VP; GAEL GILBERT, RN,

DIRECTOR; SJHHC DOES 1-5 INCLUSIVE:

Defendants.

Plaintiff Heendeniya's Affidavit Attesting That the 18 Federal and NY State Persons and Entities Informed Him That They Will Not Grant or Provide Him the Reasonable Disability Accommodations That He Had Requested per Title II, III, and V of The ADA, Section 504 of The Rehabilitation Act, and Other Applicable Federal and State Laws, in Order for Him to Purchase and Possess Firearms and Ammunition.

STATE OF FLORIDA

)

) SS

COUNTY OF HERNANDO

;

Umesh Heendeniya, being duly sworn, deposes and says:

1. On January 16, 2016, I wrote and mailed essentially identical 20 (twenty) page letters, each containing 2 (two) exhibits, to 17 (seventeen) federal and New York state persons and governmental entities. Then on January 19, 2016, I wrote essentially the identical 20 page letter containing the same 2 exhibits to a New York state government entity.
2. Each of the set of above cited exhibits that were mailed to the 18 (eighteen) federal and New York state persons and governmental entities (henceforth the “18 receivers” or “receivers”) were identical. The first exhibit was 13 (thirteen) pages in length, and the second exhibit was 3 (three) pages in length.

3. I used the U.S. Postal Service to mail the above cited letters, and each envelope to the 18 receivers had a unique postal tracking number associated with it.
4. I wrote these 20-page letters containing the 2 exhibits in order to request reasonable disability accommodations from the 18 receivers, per Title II, III, and V of The Americans with Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws, in order for me to purchase and possess firearms and ammunition and thereby exercise my Second Amendment rights.
5. At the end of each of the letters written to the 18 receivers, I wrote: "Please let me know on or before January 26, 2016, whether you will grant me the above requested reasonable disability accommodations, by either writing to me or emailing me (both addresses are given below). If I don't hear back from you on or before January 26, 2016, I will assume that you thereby are informing and communicating to me that you will not grant me the requested reasonable disability accommodations in order for me to exercise my Second Amendment rights."
6. The names of the 18 receivers that I wrote requesting reasonable disability accommodations in order for me to exercise my Second Amendment rights are: (i) Honorable Loretta E. Lynch; (ii) Honorable Eric T. Schneiderman; (iii) James B. Comey, Jr., Esq.; (iv) Thomas E. Brandon; (v) A. Lee Bentley, III. Esq.; (vi) Paul Wysopal; (vii) Regina Lombardo; (viii) Dr. Ann Marie T. Sullivan; (ix) Joshua Pepper, Esq.; (x) Michael C. Green; (xi) United States Department of Justice; (xii) Federal Bureau of Investigation; (xiii) Bureau of Alcohol, Tobacco, Firearms and Explosives; (xiv) National Instant Background Check System; (xv) FBI Criminal Justice Information Services Division; (xvi) New York State Office of Mental

Health; (xvii) New York State Division of Criminal Justice Services; (xviii) New York State Office of Mental Health - NICS Appeals Office.

7. Using the web tracking tool offered by the U.S. Postal Service at https://tools.usps.com/go/TrackConfirmAction_input, I checked for the successful delivery of the letters to the 18 receivers named above in ¶ 6.
8. By January 21, 2016, using the web tracking tool identified above in ¶ 7, I verified that most of the 18 receivers had received my 20-page letters that requested reasonable disability accommodations from them.
9. However, the tracking information for three of the defendants in this lawsuit-- Hon. Loretta E. Lynch, Hon. Eric T. Schneiderman, and FBI director James B. Comey, Jr.-- didn't show for certain that they or their office had received my letters.
10. Prior to this, I have sent many letters and correspondence using U.S. Postal Service, and many times have paid extra money for including postal tracking numbers in order to track and verify successful delivery of the correspondence.
11. Hence, I knew from prior experience that even though sometimes, the tracking information for a mailed correspondence obtained by typing the corresponding tracking number into the web tracking tool at https://tools.usps.com/go/TrackConfirmAction_input will show that the correspondence had not reached the destination yet, in fact the package had been successfully delivered, and the discrepancy was because the tracking information shown on the USPS website was incorrect.
12. Therefore, I was confident that Hon. Lynch, Hon. Schneiderman, and director Comey had received my letters, but nevertheless, in an abundance of caution, I decided to send them a copy of the 20-page letters utilizing USPS tracking, one more time (as a backup).

13. Thus, on January 21, 2016, I mailed Hon. Lynch, Hon. Schneiderman, and director Comey copies of the 20-page letters *via* certified postal mail. On the front of each of the three 9"x12" manila envelopes, below the recipients' address information, I wrote "URGENT LEGAL MAIL" in large, black, uppercase letters using a "sharpie marker."
14. On January 26, 2016, I went to my P. O. Box number 5104 at the Spring Hill post office at approx. 8PM and checked my mail to see whether any of the 18 receivers had written back to me. There was no correspondence from any of them in my post box.
15. On January 26, 2016, after returning home from checking my P. O. Box, I checked my Gmail email account to see whether any of the 18 receivers had written back to me. There was no correspondence from any of them in my Gmail email inbox in response to my reasonable disability request.
16. A true and correct copy of the 22-page tracking information screenshots for each of the tracking numbers assigned to each of the letters that were mailed to the aforementioned 18 receivers, obtained from the https://tools.usps.com/go/TrackConfirmAction_input website, is annexed hereto as Exhibit 1.
17. Based on what I had written at the end of each letter that I had sent to the 18 receivers (see ¶ 5 above) and not having received any correspondence from them at either my P.O. Box number 5104 or at my email address heendeniyavsjoephshospitalny@gmail.com on or before January 26th, I can attest that the 18 receivers were communicating clearly to me that they were not going to grant me reasonable disability accommodations, pursuant to Title II, III, and V of The Americans With Disabilities Act (ADA), Section 504 of The Rehabilitation Act, and other applicable federal and state laws, in order for me to lawfully exercise my fundamental constitutional rights to The Second Amendment rights (i.e., purchase firearms

and ammunition for lawful self-defense and target shooting purposes, possess them on my person, and keep them at my home).

18. Therefore, I intend to add two additional claims (i.e., 2 additional causes of action) to the instant legal action when I prepare and file the "First Amended Complaint." The 1st additional claim will be against all 18 receivers for violating Title II, III, and V of The Americans With Disabilities Act (ADA) with regard to my Second Amendment rights. The 2nd additional claim will also be against the 18 receivers for violating Section 504 of The Rehabilitation Act with regard to my Second Amendment rights.

This concludes my affidavit.


Umesh Heendaniya

Sworn to before me this 27 th day of January, 2016.



Notary Public



EXHIBIT 1

Bureau of Alcohol, Tobacco, Firearms, and Explosives (The BATFE)

usps.com
 PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

USPS Tracking



Have questions? We're here to help.



Get Easy Tracking Updates
 Sign up for My USPS.

Tracking Number: 9400110200793853014524

Delivered

On Time

Expected Delivery Day: Tuesday, January 19, 2016

Product & Tracking Information

Postal Product:
 First-Class Package Service

Features:
 USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 19, 2016 , 8:46 am	Delivered, In/At Mailbox	WASHINGTON, DC 20002

Your item was delivered in or at the mailbox at 8:46 am on January 19, 2016 in WASHINGTON, DC 20002.

January 19, 2016 , 5:39 am	Arrived at Post Office	WASHINGTON, DC 20066
January 18, 2016 , 4:53 pm	Arrived at USPS Destination Facility	WASHINGTON, DC 20066
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:27 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Available Actions

Text Updates

Email Updates

Mr. Joshua Pepper, Esq. (NY State Office of Mental Health)

tools.usps.com/go/TrackConfirmAction.action?tRef=fullpage&ttc=1&text28777=&tlLabels=9400110200828883224077

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results < > Options

Sign up for My USPS.

Tracking Number: 9400110200828883224077



Updated Delivery Day: Saturday, January 23, 2016

Product & Tracking Information

Postal Product: First-Class Package Service
Features: USPS Tracking™

Available Actions

- Text Updates
- Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 23, 2016 , 8:17 am	Delivered, Individual Picked Up at Postal Facility	ALBANY, NY 12208
Your item was picked up at a postal facility at 8:17 am on January 23, 2016 in ALBANY, NY 12208.		
January 23, 2016 , 8:09 am	Arrived at Post Office	ALBANY, NY 12206
January 20, 2016 , 5:09 am	Departed USPS Destination Facility	ALBANY, NY 12288
January 18, 2016 , 10:48 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:22 pm	Shipping Label Created	BROOKSVILLE, FL 34613

United States Department of Justice (U.S. DOJ)

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results < > Options v

USPS Tracking®



Have questions? We're here to help.



Get Easy Tracking Updates
Sign up for My USPS.

Tracking Number: 9400110200828883225678



Updated Delivery Day: Saturday, January 23, 2016

In-Transit

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 22, 2016, 12:59 pm	Sorting Complete	WASHINGTON, DC 20530

All sorting has been completed at the delivery unit for today's deliveries at 12:59 pm on January 22, 2016 in WASHINGTON, DC 20530.

January 22, 2016, 10:43 am	Arrived at Post Office	WASHINGTON, DC 20018
January 18, 2016, 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016, 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016, 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016, 1:26 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Available Actions

Text Updates

Email Updates

Delivery Instructions

Mr. Thomas E. Brandon (Acting Director of The BATFE)

tools.usps.com/go/TrackConfirmAction.action?Ref=fullpage&tlc=1&text2S/77=&tlabels=9400110200828883228228

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

USPS Tracking

Have questions? We're here to help.

Get Easy Tracking Updates
Sign up for My USPS.

Tracking Number: 9400110200828883228228



On Time
Expected Delivery Day: Tuesday, January 19, 2016

Product & Tracking Information

Postal Product: First-Class Package Service
Features: USPS Tracking™

Available Actions

- Text Updates
- Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 19, 2016 , 8:46 am	Delivered, In/At Mailbox	WASHINGTON, DC 20002
Your item was delivered in or at the mailbox at 8:46 am on January 19, 2016 in WASHINGTON, DC 20002		
January 19, 2016 , 5:39 am	Arrived at Post Office	WASHINGTON, DC 20066
January 18, 2016 , 4:53 pm	Arrived at USPS Destination Facility	WASHINGTON, DC 20066
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:30 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Mr. Michael C. Green (NY State Division of Criminal Justice Services)

Full page: 9400110200828883229980

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate



Get Easy Tracking Updates ,
Sign up for My USPS.

Tracking Number: 9400110200828883229980

**Delivered**

Updated Delivery Day: Wednesday, January 20, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

Available Actions

Text Updates


Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 20, 2016 , 8:38 am	Delivered, Individual Picked Up at Postal Facility	ALBANY, NY 12210

Your item was picked up at a postal facility at 8:38 am on January 20, 2016 in ALBANY, NY 12210.

January 20, 2016 , 8:09 am	Arrived at Post Office	ALBANY, NY 12207
January 20, 2016 , 5:07 am	Departed USPS Destination Facility	ALBANY, NY 12288
January 18, 2016 , 10:48 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:34 pm	Shipping Label Created	BROOKSVILLE, FL 34613

 tools.usps.com/go/TrackConfirmAction.action?ref=fullpage&tlc=1&ext=28771=&Labels=9400110200629885166526



Get Easy Tracking Updates ,
Sign up for My USPS.

Delivered

Product & Tracking Information

Features:
USPS Tracking™

Available Actions

Text Updates

Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 20, 2016 , 8:38 am	Delivered, Individual Picked Up at Postal Facility	ALBANY, NY 12210
Your item was picked up at a postal facility at 8:38 am on January 20, 2016 in ALBANY, NY 12210.		
January 20, 2016 , 8:09 am	Arrived at Post Office	ALBANY, NY 12207
January 20, 2016 , 5:07 am	Departed USPS Destination Facility	ALBANY, NY 12288
January 18, 2016 , 10:48 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:23 pm	Shipping Label Created	BROOKSVILLE, FL 34613

NICS Appeals Office - OMH Central Files (NY State Office of Mental Health)

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results



Options ▾



Sign up for My USPS.

Tracking Number: 9400110200829883167203



Delivered

Updated Delivery Day: Saturday, January 23, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™


Available Actions

Text Updates

Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 23, 2016 , 8:17 am	Delivered, Individual Picked Up at Postal Facility	ALBANY, NY 12208
Your item was picked up at a postal facility at 8:17 am on January 23, 2016 in ALBANY, NY 12208.		
January 23, 2016 , 8:09 am	Arrived at Post Office	ALBANY, NY 12206
January 20, 2016 , 5:09 am	Departed USPS Destination Facility	ALBANY, NY 12288
January 18, 2016 , 10:48 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:24 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Mr. James B. Comey, Jr. (Director of The FBI)

 tools.usps.com/go/TrackConfirmAction.action?ttRef=fullpage&ttLc=1&text28777=&ttLabels=9400110200829883170678

PACER  YouTube  The Guardian  Yahoo Email  Yahoo  Google  SunTrust  Chase  Google Scholar  Suicide Rates by  SecurityTube  2A Cases  2CT Intermediate

No results < > Options v

USPS Tracking®



Have questions? We're here to help.



Get Easy Tracking Updates
Sign up for My USPS.

Tracking Number: 9400110200829883170678



Updated Delivery Day: Saturday, January 23, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 22, 2016 , 10:56 am	Available for Pickup	WASHINGTON, DC 20535

Your item arrived at the WASHINGTON, DC 20535 post office at 10:56 am on January 22, 2016 and is ready for pickup.

January 22, 2016 , 10:31 am	Arrived at Post Office	WASHINGTON, DC 20018
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:32 pm	Shipping Label Created	BROOKSVILLE, FL 34613

In-Transit

Available Actions

Text Updates

Email Updates



Dr. Ann Marie Sullivan (NY State Office of Mental Health)

Full page URL: <https://www.usps.com/track/track?tracknum=9400110200829883171668>

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

USPS Tracking®**Customer Service ›**

Have questions? We're here to help.

**Get Easy Tracking Updates ›**

Sign up for My USPS.

Tracking Number: 9400110200829883171668

**Delivered**

Updated Delivery Day: Wednesday, January 20, 2016

Product & Tracking InformationPostal Product:
First-Class Package ServiceFeatures:
USPS Tracking™**Available Actions**

Text Updates

Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 20, 2016 , 7:42 am	Delivered, Individual Picked Up at Postal Facility	ALBANY, NY 12208

Your item was picked up at a postal facility at 7:42 am on January 20, 2016 in ALBANY, NY 12208.

January 20, 2016 , 7:41 am	Arrived at Post Office	ALBANY, NY 12206
January 18, 2016 , 10:48 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:34 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Federal Bureau of Investigation (The FBI)

tools.usps.com/go/TrackConfirmAction.action?ttRef=fullpage&tlc=1&text28777=&tlLabels=9400110200881883077524

PACER YouTube The Guardian Yahoo! Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results < > Options

USPS Tracking®



Have questions? We're here to help.



Get Easy Tracking Updates
Sign up for My USPS.

Tracking Number: 9400110200881883077524



Updated Delivery Day: Saturday, January 23, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 22, 2016 , 10:56 am	Available for Pickup	WASHINGTON, DC 20535

Your item arrived at the WASHINGTON, DC 20535 post office at 10:56 am on January 22, 2016 and is ready for pickup.

January 22, 2016 , 10:31 am	Arrived at Post Office	WASHINGTON, DC 20018
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:27 pm	Shipping Label Created	BROOKSVILLE, FL 34613

In-Transit

Available Actions

- Text Updates
- Email Updates

[id=106-10894894&from=7577&&label=s:9400110200881883078602](#)

Customer service >
Have questions? We're here to help.

**Get Easy Tracking Updates ,
Sign up for My USPS.**

Delivered

Expected Delivery Day: Tuesday, January 19, 2016

Available Actions

Features:
USPS Tracking™

5

1

January 19, 2016 , 7:37 am	Out for Delivery	TAMPA, FL 33609
January 19, 2016 , 7:27 am	Sorting Complete	TAMPA, FL 33609
January 19, 2016 , 6:52 am	Arrived at Post Office	TAMPA, FL 33607
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:30 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Honorable Loretta E. Lynch (Attorney General of The United States)

www.usps.com/go/trackConfirm.action?track=fullpage&tlc=1&stext22777=&stLabels=9400110200881883079962

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results < > Options

USPS Tracking®



Customer Service
Have questions? We're here to help.



Get Easy Tracking Updates
Sign up for My USPS.

Tracking Number: 9400110200881883079962



Updated Delivery Day: Saturday, January 23, 2016

In-Transit

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 22, 2016 , 12:59 pm	Sorting Complete	WASHINGTON, DC 20530

All sorting has been completed at the delivery unit for today's deliveries at 12:59 pm on January 22, 2016 in WASHINGTON, DC 20530

January 22, 2016 , 10:43 am	Arrived at Post Office	WASHINGTON, DC 20018
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:32 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Available Actions

- Text Updates
- Email Updates
- Delivery Instructions

National Instant Background Check System (NICS)

tools.usps.com/go/TrackConfirmAction.action?iRef=fullpage&tlc=1&text28777=&tlLabels=9400110200881883080173

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results

Options

USPS Tracking®



Have questions? We're here to help.



Get Easy Tracking Updates ›
Sign up for My USPS.

Tracking Number: 9400110200881883080173



In-Transit

Updated Delivery Day: Saturday, January 23, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

DATE & TIME

January 22, 2016 , 10:56
am

STATUS OF ITEM

Available for Pickup

LOCATION

WASHINGTON, DC 20535

Your item arrived at the WASHINGTON, DC 20535 post office at 10:56 am on January 22, 2016 and is ready for pickup.

January 22, 2016 , 10:31 am	Arrived at Post Office	WASHINGTON, DC 20018
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:33 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Available Actions

Text Updates

Email Updates

Honorable Eric T. Schneiderman (Attorney General of The State of New York)

tools.usps.com/go/TrackConfirmAction.action?iRef=fullpage&rtLc=1&text28777=&tlLabels=9400110200881883086274

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results



Options

Get Easy Tracking Updates ,
Sign up for My USPS.

Tracking Number: 9400110200881883086274

In-Transit,
Delayed

Product & Tracking Information

Postal Product:
First-Class Package ServiceFeatures:
USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 20, 2016 , 3:05 am	Departed USPS Destination Facility	ALBANY, NY 12288
The package is delayed and will not be delivered by the expected delivery date. An updated delivery date will be provided when available. Your item departed our USPS destination facility in ALBANY, NY 12288 on January 20, 2016 at 3:05 am. The item is currently in transit to the destination.		
January 18, 2016 , 10:50 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:44 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Available Actions

Text Updates

Email Updates

Delivery Instructions

Mr. A. Lee Bentley, III, Esq. (United States Attorney - Middle District of Florida)

usps.com

PACER

YouTube

The Guardian

Yahoo Email

Yahoo

Google

SunTrust

Chase

Google Scholar

Suicide Rates by

SecurityTube

2A Cases

2CT Intermediate

USPS Tracking®**Customer Service**
Have questions? We're here to help.**Get Easy Tracking Updates**
Sign up for My USPS.

Tracking Number: 9400110200883921387091

**Delivered**

On Time

Expected Delivery Day: Tuesday, January 19, 2016

Product & Tracking InformationPostal Product:
First-Class Package ServiceFeatures:
USPS Tracking™**Available Actions**

Text Updates

Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 19, 2016 , 9:53 am	Delivered, In/At Mailbox	TAMPA, FL 33602

Your item was delivered in or at the mailbox at 9:53 am on January 19, 2016 in TAMPA, FL 33602

January 19, 2016 , 8:07 am	Out for Delivery	TAMPA, FL 33602
January 19, 2016 , 7:57 am	Sorting Complete	TAMPA, FL 33602
January 18, 2016 , 11:10 am	Arrived at Post Office	TAMPA, FL 33605
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:28 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Ms. Regina Lombardo (BATFE Special Agent in Charge, Tampa, FL)

tools.usps.com/go/TrackConfirmAction.action?ref=fullpage&tlc=1&text28777=&Labels=9400110200883921387428

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

Get Easy Tracking Updates ,
Sign up for My USPS.

Tracking Number: 9400110200883921387428



Delivered

On Time

Expected Delivery Day: Tuesday, January 19, 2016

Product & Tracking InformationPostal Product:
First-Class Package ServiceFeatures:
USPS Tracking™**Available Actions**

Text Updates

Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 19, 2016 , 4:11 pm	Delivered, Front Desk/Reception	TAMPA, FL 33602

Your item was delivered to the front desk or reception area at 4:11 pm on January 19, 2016 in TAMPA, FL 33602.

January 19, 2016 , 8:07 am	Out for Delivery	TAMPA, FL 33602
January 19, 2016 , 7:57 am	Sorting Complete	TAMPA, FL 33602
January 18, 2016 , 11:10 am	Arrived at Post Office	TAMPA, FL 33605
January 18, 2016 , 1:22 am	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 1:29 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Federal Bureau of Investigation - Criminal Justice Information Services Division

tools.usps.com/go/TrackConfirmAction.action?trRef=fullpage&tlc=1&text28777=8&tlLabels=9400110200829883139026

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

USPS Tracking



Have questions? We're here to help.



Get Easy Tracking Updates
Sign up for My USPS.

Tracking Number: 9400110200829883139026



Delivered

Updated Delivery Day: Wednesday, January 20, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

Available Actions

Text Updates

Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 20, 2016 , 9:56 am	Delivered	CLARKSBURG, WV 26306

Your item was delivered at 9:56 am on January 20, 2016 in CLARKSBURG, WV 26306.

January 20, 2016 , 9:18 am	Arrived at Post Office	CLARKSBURG, WV 26301
January 19, 2016 , 7:56 pm	Departed USPS Facility	CHARLESTON, WV 25350
January 18, 2016 , 11:34 am	Arrived at USPS Destination Facility	CHARLESTON, WV 25350
January 16, 2016 , 10:04 pm	Departed USPS Facility	TAMPA, FL 33630
January 16, 2016 , 10:03 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 16, 2016 , 2:40 pm	Picked Up	BROOKSVILLE, FL 34613
January 16, 2016 , 12:37 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Mr. A. Lee Bentley, III, Esq. (United States Attorney - Middle District of Florida)

tools.usps.com/go/TrackConfirmAction.action?iRet=fullpage&atl=1&text28777=&labels=9400110200793854883457

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

Get Easy Tracking Updates Sign up for My USPS.

Tracking Number: 9400110200793854883457



Updated Delivery Day: Wednesday, January 20, 2016

Product & Tracking Information

Postal Product: First-Class Package Service Features: USPS Tracking™

Available Actions

- Text Updates
- Email Updates

DATE & TIME	STATUS OF ITEM	LOCATION
January 20, 2016 , 9:05 am	Delivered, In/At Mailbox	TAMPA, FL 33602
Your item was delivered in or at the mailbox at 9:05 am on January 20, 2016 in TAMPA, FL 33602.		
January 20, 2016 , 7:17 am	Out for Delivery	TAMPA, FL 33602
January 20, 2016 , 7:07 am	Sorting Complete	TAMPA, FL 33602
January 20, 2016 , 6:51 am	Arrived at Post Office	TAMPA, FL 33605
January 19, 2016 , 10:55 pm	Departed USPS Facility	TAMPA, FL 33605
January 19, 2016 , 9:00 pm	Arrived at USPS Facility	TAMPA, FL 33605
January 19, 2016 , 4:49 pm	Picked Up	BROOKSVILLE, FL 34613
January 19, 2016	Pre-Shipment Info Sent to USPS	
January 18, 2016 , 5:26 pm	Shipping Label Created	BROOKSVILLE, FL 34613

New York State Office of Mental Health

tools.usps.com/go/TrackConfirmAction.action?iRef=fullpage&tlc=1&ext=128777=&extLabels=9400110200830013430029

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

Quick Tools

Mail & Ship

Track & Manage

Postal Store

Business

International

USPS Tracking®



Customer Service ›
Have questions? We're here to help.



Get Easy Tracking Updates ›
Sign up for My USPS.

Tracking Number: 9400110200830013430029



Delivered

Updated Delivery Day: Thursday, January 21, 2016

Product & Tracking Information

Postal Product:
First-Class Package Service

Features:
USPS Tracking™

DATE & TIME	STATUS OF ITEM	LOCATION
January 21, 2016 , 9:14 am	Delivered, In/At Mailbox	ALBANY, NY 12208

Your item was delivered in or at the mailbox at 9:14 am on January 21, 2016 in ALBANY, NY 12208.

January 21, 2016 , 7:37 am	Arrived at Post Office	ALBANY, NY 12206
January 21, 2016 , 3:52 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 19, 2016 , 9:00 pm	Arrived at USPS Origin Facility	TAMPA, FL 33605
January 19, 2016 , 4:48 pm	Picked Up	BROOKSVILLE, FL 34613
January 19, 2016 , 2:18 pm	Shipping Label Created	BROOKSVILLE, FL 34613

Available Actions

Text Updates

Email Updates

Honorable Loretta E. Lynch (Attorney General of The United States) – mailed on Jan. 21, 2016

tools.usps.com/go/TrackConfirmAction.action?tlRef=fullpage&tlLc=1&text28777=&tlLabels=70150640000020444115

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results < > Options v

Quick Tools v

Mail & Ship

Track & Manage

Postal Store

Business

International

USPS Tracking®

Customer Service ›
Have questions? We're here to help.

Get Easy Tracking Updates ›
Sign up for My USPS.

Tracking Number: 70150640000020444115

Expected Delivery Day: Monday, January 25, 2016 ›

In-Transit

Product & Tracking Information

Postal Product:
First-Class Mail®

Features:
Certified Mail™

DATE & TIME	STATUS OF ITEM	LOCATION
January 22, 2016 , 1:24 am	Departed USPS Facility	TAMPA, FL 33630
Your item departed our USPS facility in TAMPA, FL 33630 on January 22, 2016 at 1:24 am. The item is currently in transit to the destination.		
January 21, 2016 , 10:17 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 21, 2016 , 6:02 pm	Departed Post Office	BROOKSVILLE, FL 34601
January 21, 2016 , 5:02 pm	Acceptance	BROOKSVILLE, FL 34601

Available Actions

- Text Updates
- Email Updates

[illegible]

No results < > Options ▾

 Delivered

Expected Delivery Day: Monday, January 25, 2016

Available Actions

Features:
Certified MailTM

Email Updates

Your item was delivered at 9:09 am on January 25, 2016 in ALBANY, NY 12224

January 25, 2016 , 8:14 am	Out for Delivery	ALBANY, NY 12224
January 25, 2016 , 8:04 am	Sorting Complete	ALBANY, NY 12224
January 25, 2016 , 4:19 am	Arrived at Unit	ALBANY, NY 12288
January 25, 2016 , 12:10 am	Departed USPS Destination Facility	ALBANY, NY 12288
January 23, 2016 , 7:50 am	Arrived at USPS Destination Facility	ALBANY, NY 12288
January 22, 2016 , 1:24 am	Departed USPS Facility	TAMPA, FL 33630
January 21, 2016 , 10:17 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 21, 2016 , 6:02 pm	Departed Post Office	BROOKSVILLE, FL 34601
January 21, 2016 , 5:02 pm	Acceptance	BROOKSVILLE, FL 34601

Mr. James B. Comey, Jr. (Director of The FBI) – mailed on Jan. 21, 2016

tools.usps.com/go/TrackConfirmAction.action?Ref=fullpage&tlc=1&text123777=&tlLabels=70150640000020444122

PACER YouTube The Guardian Yahoo Email Yahoo Google SunTrust Chase Google Scholar Suicide Rates by SecurityTube 2A Cases 2CT Intermediate

No results < > Options v

English Customer Service USPS Mobile



70150640000020444122

Quick Tools

Mail & Ship

Track & Manage

Postal Store

Business

International

USPS Tracking®



Customer Service ›
Have questions? We're here to help.



Get Easy Tracking Updates ›
Sign up for My USPS.

Tracking Number: 70150640000020444122



Expected Delivery Day: Monday, January 25, 2016 ›

In-Transit

Product & Tracking Information

Postal Product:
First-Class Mail®

Features:
Certified Mail™

DATE & TIME	STATUS OF ITEM	LOCATION
January 22, 2016, 1:24 am	Departed USPS Facility	TAMPA, FL 33630

Your item departed our USPS facility in TAMPA, FL 33630 on January 22, 2016 at 1:24 am. The item is currently in transit to the destination.

January 21, 2016, 10:17 pm	Arrived at USPS Origin Facility	TAMPA, FL 33630
January 21, 2016, 6:02 pm	Departed Post Office	BROOKSVILLE, FL 34601
January 21, 2016, 5:03 pm	Acceptance	BROOKSVILLE, FL 34601

Available Actions

Text Updates

Email Updates


[FAQs >](#)
[Track Another Package +](#)
Tracking Number: 70040750000303211304

[Remove X](#)

Your item was delivered to an individual at the address at 3:08 pm on March 2, 2020 in TAMPA, FL 33609.

✓ Delivered

March 2, 2020 at 3:08 pm
Delivered, Left with Individual
TAMPA, FL 33609

[Get Updates ✓](#)

[Text & Email Updates](#)

Tracking History

March 2, 2020, 3:08 pm

Delivered, Left with Individual
TAMPA, FL 33609

Your item was delivered to an individual at the address at 3:08 pm on March 2, 2020 in TAMPA, FL 33609.

March 2, 2020, 9:12 am

Out for Delivery
TAMPA, FL 33609

U.S. Postal Service™	
CERTIFIED MAIL™ RECEIPT	
(Domestic Mail Only; No Insurance Coverage Provided)	
For delivery information visit our website at www.usps.com	
TAMPA, FL 33609	
OFFICIAL USE	
Postage	\$3.55
Certified Fee	\$0.00
Return Receipt Fee (Endorsement Required)	\$0.00
Restricted Delivery Fee (Endorsement Required)	\$0.00
	\$7.50
Total Postage & Fees	\$11.05
Sent To <u>Michael McPherson</u>	
Street, Apt. No., or PO Box No. <u>FBI SAC</u>	
City, State, ZIP+4 <u>Tampa, FL-33609</u>	
PS Form 3800, June 2002	
See Reverse for Instructions	

7004 0750 0003 0321 1304

TAMPA, FL 33609
FEB 2 2020
Postmark
H02
USPS

02/29/2020

March 2, 2020, 9:01 am

Arrived at Unit

TAMPA, FL 33607

March 1, 2020, 3:11 am

Arrived at USPS Regional Facility

YBOR CITY FL DISTRIBUTION CENTER

February 29, 2020, 9:29 pm

Departed Post Office

TAMPA, FL 33630

February 29, 2020, 7:23 pm

USPS in possession of item

TAMPA, FL 33630

Product Information

Feedback
✓

See Less ^

Can't find what you're looking for?

Go to our FAQs section to find answers to your tracking questions.

FAQs