IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

ADAM A MALIK and MALIK & ASSOCIATES, PLLC, Plaintiffs, v. U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, DAVID PEKOSKE, Acting Secretary of Homeland Security, and TROY MILLER, Senior Official Performing the Duties of the Commissioner of U.S. Customs and Border Protection, Defendants.	)	Case No. 4:21-cv-00088

ORIGINAL VERIFIED COMPLAINT FOR TEMPORARY RESTRAINING ORDER, PRELIMINARY INJUNCTION, PERMANENT INJUNCTION, & DECLARATORY JUDGMENT

ADAM A. MALIK ("Mr. Malik") and MALIK & ASSOCIATES, PLLC (the "Law Firm") (collectively, "Plaintiffs"), by and through undersigned counsel, respectfully files this Original Complaint against U.S. DEPARTMENT OF HOMELAND SECURITY ("DHS") and U.S. CUSTOMS AND BORDER PROTECTION ("CBP") (collectively, "Defendants") and show the Court as follows:

INTRODUCTION

1. Searches of law firm documents present special circumstances requiring particular care to preserve client confidences, especially for clients not connected with the search. Our criminal justice and immigration system depends on a robust adversarial process, protected through constitutional and statutory rights to counsel.

2. That process breaks down when the public perceives that confidential materials are at risk of disclosure to adversaries and the government. If clients and their lawyers believe that adversaries and the government may one day sift through their communications in searches involving unrelated matters, clients are less likely to be candid with their lawyers, and lawyers will hesitate before writing down what they need to write down.

3. Defendants committed and continue to commit a gross violation of these principles. Defendants, without a warrant and without reasonable suspicion that Plaintiffs' iPhone contains contraband or evidence of violation of the law, seized Plaintiffs' iPhone, which contains emails, notes, files, and voice mails and other communications of more than 2000 clients of Plaintiffs, as well as private information of Mr. Malik.

4. Plaintiffs have evidence that Defendants already have searched the contents of the iPhone and remotely stored digital information of Plaintiffs. Defendants deny that they already have made such a search and claim to be assembling a filter team to search the digital information. That filter team is composed of adversaries to many of the 2000 clients whose documents they will be searching. Defendants threaten to begin their search of the privileged documents as early as today, Monday, January 25, 2021.

5. This lawsuit challenges Defendants'

(1) Search and seizure of Plaintiffs' iPhone, including its digital contents;
(2) Continuing search and seizure of remotely stored digital information that was and likely still is being downloaded to the seized iPhone;
(3) CBP Directive 3340-049A" (the "Directive") upon which Defendants rely to justify the search and seizure;
(4) Failure to follow the Directive; and
(5) Use and formulation of Defendants' filter team. If this Court determines that the search and seizure is lawful, Plaintiffs ask the Court to create a protocol for the search and to appoint a Special Master to segregate privileged information.

JURISDICTION & VENUE

6. This Court has subject matter jurisdiction over the federal claims pursuant to 28 U.S.C. § 1331 because Plaintiffs challenge federal law and final agency action under the laws and Constitution of the United States.

7. This Court has authority to issue declaratory and injunctive relief under 28 U.S.C. § 2201 and § 2202, and Rules 57 and 65 of the Federal Rules of Civil Procedure, and the Court's inherent equitable powers.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this Division and District. Defendants seized Plaintiffs' iPhone at the Dallas-Fort Worth Airport, within Tarrant County, Texas.

9. All administrative remedies are exhausted. No administrative remedies exist for review of the claims made in this Complaint.

PARTIES

10. Mr. Malik is a U.S. citizen and an attorney admitted to the State Bar of Texas. He resides in Denton County, Texas. Prior to becoming an attorney, Mr. Malik was a DHS officer, having worked for both U.S. Immigration & Customs Enforcement and U.S. Citizenship & Immigration Services.

11. Malik & Associates, PLLC (the "Law Firm") is a Texas law firm and Mr. Malik is the managing member. The Law Firm was organized under Texas law on February 8, 2018 and continues to operate as a law firm.

12. DHS is a Department of the executive branch of the United States and is an "agency" within the meaning of 5 U.S.C. § 552(f)(1).

13. CBP is an agency within DHS. CBP is an "agency" within the meaning of 5 U.S.C. § 552(f)(1).

14. DAVID PEKOSKE is the Acting Secretary of Homeland Security. He oversees all functions of DHS and its agencies. He is sued only in his official capacity.

15. TROY MILLER is the Senior Official Performing the Duties of the Commissioner of CBP. He oversees all functions of CBP. He is sued only in his official capacity.

FACTUAL ALLEGATIONS

Plaintiffs' Law Practice Involves Matters Before and Against Defendants.

16. Plaintiffs primarily represent individuals in U.S. immigration and naturalization matters, including lawsuits against Defendants and in removal proceedings. When noncitizens are placed in removal proceedings before the U.S. Department of Justice, DHS is the adversary. When noncitizens seek an immigration benefit or naturalization they do so with DHS.

17. Plaintiffs represent the plaintiff in *Rahim v. Wolf et al*, 4:20-cv-03260 (S.D. Texas). DHS is a defendant in that proceeding.

18. Plaintiffs represent and advise clients who are located throughout the United States and abroad. Mr. Malik travels nationally and internationally in the representation of his clients.

19. While many of Plaintiffs' clients have no criminal history, some of the clients have significant legal troubles. Plaintiffs represent one client in removal proceedings whom DHS has accused of engaging in terrorist activities. Plaintiffs represent various clients who have been alleged to have committed significant offenses. Some seek Plaintiffs' guidance in crafting plea

agreements necessary to meet the Sixth Amendment requirements of effective assistance of counsel as described in *Padilla v. Commonwealth of Kentucky*, 559 U.S. 356 (2010). Other clients have committed significant offenses and have not yet been criminally charged. Other clients are victims of domestic violence who are hiding themselves or their cases from abusers.

20. The nature of Mr. Malik's practice causes him frequently to be outside his office to see clients and potential clients. He uses an iPhone to communicate with his clients and potential clients, save notes and recordings of client communications and legal research, record legal strategy, and access client files and documents. The iPhone is owned by the Law Firm and is provided to Mr. Malik for his professional and personal use.

21. The nature of Mr. Malik's law practice requires that Mr. Malik always have access to his client files and communications, regardless whether he is within the U.S. or abroad.

The Information Contained on the iPhone and Accessible Through the iPhone.

22. Mr. Malik has a possessory interest in the iPhone. He also has a reasonable expectation of privacy in all digital information stored on the iPhone and in all digital information that is stored remotely, and which is accessible through the iPhone.

23. The iPhone and the applications and software installed on the iPhone contain digital information that is protected by attorney/client privilege and attorney work product privilege. All attorney/client privileged and attorney work product privileged information of Plaintiffs are referred to in this Complaint as "Privileged Information."

24. The attorney work product privilege component of the Privileged Information includes fact work product and opinion work product.

25. Residing on the iPhone is Privileged Information of more than 2000 individuals and organizations who have consulted with Plaintiffs for legal advice and/or who have hired Plaintiffs to provide them legal representation.

26. The iPhone and the applications and software installed on the iPhone also contain highly sensitive information concerning Mr. Malik's personal, confidential, and anonymous communications and associations. For example, such information includes medical reports of physicians addressing Mr. Malik's recent medical examinations and current health. Such information also includes Mr. Malik's expressive information, such as his personal thoughts and opinions. All such information described in this paragraph is referred to herein as "Private Information."

27. The iPhone and the applications and software installed on the iPhone may be used to access and retrieve Privileged Information and Private Information that is stored remotely on servers throughout the United States.

28. Certain applications and software on the iPhone are configured to automatically download digital information from remote servers to the iPhone when the iPhone is connected to the internet or to a communications network. The iPhone, for example, contains Microsoft Outlook, which is an email and calendaring application. Plaintiffs also maintain copies of Outlook on other computers and mobile devices with the same Outlook account. Plaintiffs' installations of Outlook synchronize information on all computers and devices. When Mr. Malik sends or receives an email or his secretary calendars an appointment, information about that email and appointment immediately are downloaded to the iPhone when the iPhone is connected to the internet. Mr. Malik regularly uses Microsoft Outlook to send, receive, and store Privileged

Information and Private Information. In fact, undersigned counsel has exchanged confidential emails with Mr. Malik about this lawsuit.

29. As a second example, the iPhone contains an application called WhatsApp Messenger which is maintained by WhatsApp, Inc., a subsidiary of Facebook, Inc. WhatsApp Messenger allows users to send and receive text messages, voice messages, video messages, images, and documents when the iPhone is connected to the internet or a communications network. Those messages, images, and documents are saved on the servers of WhatsApp, Inc. and downloaded to the iPhone when connected. Those messages, images, and documents automatically are downloaded to the iPhone when the iPhone is connected to the internet or a communications network.

30. WhatsApp Messenger also permits the sending of a user's location. Plaintiffs and their clients regularly use WhatsApp Messenger to send, receive, and store Privileged Information and Private Information. Privileged and Private Information is contained in both WhatsApp Messenger and on the servers of WhatsApp, Inc.

31. As a third example, the iPhone is configured to regularly download messages consisting of text, audio, video, images, and documents from the servers of AT&T to the iPhone when the iPhone is connected to the internet or a communication network. Clients of Plaintiffs and others regularly send Privileged Information and Private Information to Mr. Malik by this type of message.

32. As a fourth example, the iPhone receives voice mail messages and allows for accessing voice mail messages. Clients of Plaintiffs and others regularly send Privileged Information and Private Information to Mr. Malik by this type of voice message. Those voice

mail messages are accessible through the iPhone when the iPhone is connected to the internet or a communications network.

The Seizure of the iPhone by Defendants.

33. To facilitate his extensive travel, Mr. Malik applied for and received membership in CBP's Global Entry Trusted Traveler Program ("Global Entry"). DHS approved him for Global Entry on or about November 2014 and approved his renewal in 2019.

34. To receive membership in Global Entry, Mr. Malik passed a layer of extremely thorough security checks conducted by DHS. Mr. Malik passed a DHS conducted background check against criminal, law enforcement, customs, immigration, agriculture, and terrorist indices, a process that includes fingerprinting. He also passed an in-person interview with a DHS security officer.

35. On January 3, 2021, Mr. Malik returned to the United States from a trip to Costa Rica. During that trip he contacted clients and worked on the *Rahim* case and other legal matters in which DHS is an adversary. He worked from his iPhone. His iPhone contains Privileged Information of those cases.

36. Mr. Malik attempted to reenter the United States at the Dallas-Fort Worth Airport, located in Tarrant County, Texas, using a Global Entry kiosk. He was rejected entry at the kiosk and was passed to secondary inspection.

37. In secondary inspection, a CBP officer informed Mr. Malik that he was selected at random for review of eligibility for Global Entry. Upon information and belief, the statement of the CBP officer was false. Upon information and belief, the name of the CBP officer who made this statement is Aaron Sullivan ("Officer Sullivan").

38. Officer Sullivan, another employee of DHS, and one more unidentified employee of DHS separately interrogated Mr. Malik about his personal life, parents, and his personal U.S. immigration history.

39. The officers also extensively interrogated Mr. Malik about his law practice. Specifically, Defendants interrogated Mr. Malik about legal representation he had provided and continues to provide to certain clients, cases that he had taken on, and the identity of certain past and current clients of Mr. Malik.

40. Mr. Malik freely answered all questions about his personal life but refused to answer questions about his clients that required his revealing Privileged Information.

41. During interrogation, Officer Sullivan displayed anger to Mr. Malik when Mr. Malik would not reveal Privileged Information. In response to Mr. Malik's assertion of privilege, Officer Sullivan asked Mr. Malik to place the iPhone on the table. Mr. Malik placed the iPhone on the table.

42. Officer Sullivan asked Mr. Malik to unlock the iPhone so that the digital contents could be inspected.

43. Mr. Malik explained to Officer Sullivan that the iPhone contains extensive Privileged Information and allows for the accessing of Privileged Information that is stored remotely. Mr. Malik told Officer Sullivan that he cannot consent to the search of the iPhone.

44. Mr. Malik is prohibited by Tex. Disciplinary R. Prof. Conduct 1.05 from consenting to the search and seizure of Privileged Information. He brings this lawsuit, in part, to comply with his professional responsibilities as a member of the State Bar of Texas. Plaintiffs also bring this lawsuit to protect current and former clients from violations of their rights.

45. In response to Mr. Malik's assertion of privilege, Officer Sullivan informed Mr. Malik that DHS was seizing the iPhone and that the digital contents would be searched. Officer Sullivan did not disconnect the iPhone from the internet or the communications network. He failed to take action that would protect the iPhone from accessing the internet or a communications network. Officer Sullivan ordered Mr. Malik to leave the deferred inspection area without the iPhone while the iPhone still was connected to the internet and a communications network.

46. Neither Officer Sullivan nor any other employee of Defendants asked Mr. Malik to disable connectivity of the iPhone to the internet or to any network. Had Officer Sullivan or any employee of Defendants offered to permit Mr. Malik to place the iPhone in airplane mode upon or after seizure of the iPhone, Mr. Malik would have done so immediately.

47. Neither Officer Sullivan nor Defendants were warranted by national security, law enforcement, officer safety, or other operational consideration to disable connectivity of the iPhone to the internet or to any network.

Defendants' Rules & Policies for Search of Mobile Devices at the Border.

48. Defendants' seized the iPhone pursuant to the Directive. A true and accurate copy of the Directive is attached as Exhibit A. The Directive applies to the search and seizure of the Privileged Information and Private Information. The Directive creates two types of searches—"basic" and "advanced"—neither of which must be supported by a warrant, probable cause, or even a reasonable suspicion that the devices contains contraband or evidence of a violation of law.

49. A basic search allows a CBP officer to review and analyze all digital contents of the iPhone without suspicion and without a warrant. Directive § 5.1.3. An advanced search

allows the iPhone to be connected to "external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." Directive § 5.1.4.

50. The Directive authorizes the CBP officer to perform an advanced search if he has either "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or where "there is a national security concern." Directive § 5.1.4.

51. The Directive fails to define "reasonable suspicion" or "national security concern." These terms are vague and capacious.

52. The Directive does not require that the "reasonable suspicion" be related to (1) the electronic device, (2) the contents of the mobile device, (3) the information to be searched, or (3) the traveler's return to the United States or to his activities abroad.

53. Rather, the Directive authorizes CBP officers to use an external device to review, copy, and analyze the content of an electronic device based only on suspicion that the owner of the device is violating any CBP-administered law, regardless whether CBP reasonably suspects that the device or the information to be searched contains evidence of the violation.

54. While the Directive recommends that CBP officers obtain supervisor approval before conducting a search, officers need only obtain such approval if it is "practicable." Directive § 5.1.5.

55. The Directive gives CBP officers power, absent any individualized suspicion, to seize electronic devices and information copied from them "for a brief, reasonable period of time to perform a thorough border search." This period "ordinarily should not exceed five (5) days" but can be extended for undefined "extenuating circumstances." Directive § 5.4.1.

56. The Directive provides that electronic devices will be returned and data will be deleted only "if, after reviewing information, there exists no probable cause to seize the device or information." Directive § 5.4.1.2.

57. As a result, Defendants permanently may detain an electronic device and its data without a warrant. The probable cause necessary to permanently detain devices or information can be generated through the initial searches and seizures performed without any individualized suspicion, absent any review by a neutral magistrate.

58. Defendants are authorized to retain "information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of record notice," even absent any individualized suspicion. Directive § 5.5.1.2.

59. Without individualized suspicion, the CBP officer is authorized to transfer electronic devices and information thereon to other government agencies for a variety of purposes.

60. For example, without individualized suspicion, "[o]fficers may convey electronic devices or copies of information contained therein to seek technical assistance" so as to allow access to the device or its information. Directive § 5.4.2.1. Officers may also convey devices or information to "subject matter experts" in other federal agencies "when there is a national security concern or . . . reasonable suspicion." Directive § 5.4.2.2.

61. Individuals need not be notified when their devices or information are transmitted to other agencies. Directive § 5.4.2.5.

62. The Directive provides inadequate and vague guidance on how CBP officers should handle privileged and sensitive material. It contemplates that CBP officers may

"encounter[] information they identify as, or that is asserted to be, protected by attorney-client privilege or attorney work product doctrine." Directive § 5.2.1.

63. The Directive provides no meaningful direction on how officers should handle that information. Rather, the Directive vaguely instructs officers to "ensure the segregation of any privileged material" so that it is "handled appropriately while also ensuring that CBP accomplishes its critical border security mission." Directive § 5.2.1.2.

64. The Directive's guidance on "[o]ther possibly sensitive information" is even vaguer. "[M]edical records and work-related information carried by journalists . . . shall be handled in accordance with any applicable federal law and CBP policy." § 5.2.2.

65. The Directive contemplates that privileged or sensitive information may be shared with other federal agencies so long as those agencies "have mechanisms in place to protect appropriately such information." Directive § 5.2.4.

66. The Directive requires that "[t]he Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information." Directive § 5.2.1.1.

67. The Directive fails to adequately address the handling and make-up of the filter team.

Defendants Violated the Directive in the Search & Seizure of the iPhone.

68. Defendants violated the Directive in the handling of the iPhone, Privileged Information, and Personal Information.

69. Officer Sullivan and Defendants violated Directive § 5.1.2 by failing to ask Mr. Malik to disable connectivity of the iPhone to a network. Officer Sullivan and Defendants violated Directive § 5.1.2 by failing to timely disable connectivity of the iPhone to a network.

70. Defendants violated and will violate Directive § 5.1.4 by conducting an advanced search without reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern.

71. Officer Sullivan violated Directive § 5.2.1 by failing to seek clarification from Mr. Malik of the information described in that section.

72. Defendants violated Directive § 5.2.1.1 by failing to timely seek clarification from Mr. Malik of the information described in that section.

73. Defendants violated Directive § 5.2.1.2 by searching the digital contents of the iPhone prior to segregation of privileged material by a filter team.

74. Defendants violated Directive § 5.1.2 by intentionally using the iPhone to access information that is solely stored remotely.

75. Defendants violated Directive § 5.4.1 by failing to detain the iPhone for a brief, reasonable period of time. Defendants have detained the iPhone for twenty-two days and still are in possession of the iPhone.

76. Defendants' violation of the Directive has caused the search and seizure of the iPhone to be an unreasonable search and seizure in violation of the First and Fourth Amendments.

Defendants Allowed the iPhone to Download Privileged Information and Private Information After Seizure of the iPhone.

77. After Defendants seized the iPhone, Defendants allowed the iPhone to be connected to the internet and a communications network.

78. On January 4, 2021, Mr. Malik received notification from Flypsi, Inc. that a request was made to obtain a verification code to access Mr. Malik's FLYP account. A true and accurate copy of that notification is attached as Exhibit B.

79. FLYP is a call, text, and voicemail system and application installed on the iPhone that Mr. Malik uses to communicate with his clients. That service stores Privileged Information and Private Information on the servers of Flypsi, Inc. and on the iPhone.

80. The verification code was necessary to access the FLYP application residing on the iPhone and to access, through the iPhone, Mr. Malik's FLYP account and Privileged Information and Private Information on the servers of Flypsi, Inc.

81. On January 4, 2021, at the time that the verification code was requested of Flypsi, Inc., DHS and CBP were in sole possession of the iPhone, the iPhone was unlocked, and the iPhone was connected to the internet or a communications network.

82. Defendants accessed Mr. Malik's FLYP account without a warrant. Defendants accessed, searched, and seized Privileged Information and Private Information residing on the servers of Flypsi, Inc. without a warrant.

83. By permitting the iPhone to be connected to the internet or to a communications network after the iPhone's seizure, Defendants seized Privileged and Private Information that was automatically downloaded to the iPhone from remote servers, such as but not limited to the servers of Microsoft, Inc. and WhatsApp, Inc. For example, emails or portions of emails and appointments with notations about the subject matter of the appointments were downloaded from the servers of Microsoft, Inc. to the iPhone during its seizure.

84. Defendants have seized, searched, and reviewed Privileged Information and Private Information residing on the iPhone in violation of the Directive and the U.S. Constitution.

85. Defendants have seized, searched, and reviewed Privileged Information and Private Information residing on servers throughout the United States in violation of the Directive and the U.S. Constitution.

86. The period of time that Defendants have seized the iPhone is unreasonable under the law and not in compliance with the Directive.

87. By unreasonably delaying the return of the iPhone, Defendants permit the iPhone to scoop up Privileged Information and Private Information that Defendants will search and seize. Defendants' actions are the equivalent of pen register and trap and trace devices and used in violation of 18 U.S.C. § 3121.

Defendants Intend to Search and Read Privileged Information.

88. On January 6, 2021, Plaintiffs notified DHS's attorney in *Rahim* that DHS had seized Privileged Information in that case. DHS's attorney did not respond to Plaintiffs.

89. On January 15, 2021, CBP notified Plaintiffs by email that it was going to conduct a search of the iPhone and that CBP was "in the process of identifying a filter team in accordance with CBP Directive 3340-049A" A true and accurate copy of that email is attached as Exhibit C.

90. CBP invited Plaintiffs to "identify the name(s) of any individual(s) or entities who you contend would fall under the umbrella of the attorney-client privilege for the scope of this search."

91. Plaintiffs are prohibited from identifying such names because the identification for most, if not all the individuals, are connected inextricably with the privileged and confidential purpose for which the clients sought legal advice.

92. Part of the Privileged Information contained on the iPhone and on the remote servers is identifiable only by a telephone number of the client. Telephone numbers of the clients are privileged and confidential and will lead to exposure of Privileged Information.

93. Because Plaintiffs' clients include adversaries of Defendants in both immigration removal proceedings and US district court proceedings, Defendants reading Privileged Information creates an inherent and unreasonable conflict.

94. CBP's proposed filter team as implemented and as articulated in the Directive, creates the appearance of and potential for improprieties. The Directive authorizes CBP officers to rummage through attorney-client communications. The use of the filter team in these circumstances will chill the free flow of information between clients and lawyers.

95. CBP's proposed filter team as implemented and as articulated in the Directive is incompatible with protections of the attorney-client privilege and the work-product doctrines.

96. CBP's proposed filter team as implemented and as articulated in the Directive will lead to the improper disclosure of attorney-client privileged information and attorney work product information in violation of the rights of privilege and in violation of rights protected by the Fourth Amendment and the Sixth Amendment.

Plaintiffs and Their Clients Have Been and Will Continue to be Harmed by Defendants.

97. By seizing the iPhone and its contents, searching the digital contents of the iPhone, using the iPhone to access remotely stored Privileged and Private Information, permitting the downloading of Privileged Information and Private Information to the iPhone after

its seizure, Defendants have acted unreasonably, in violation of the Directive, and have caused irreparable and proximate harm to Plaintiffs and to their clients. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of Mr. Malik's constitutional rights and the constitutional rights of Plaintiffs' clients. Defendants will continue to violate Mr. Malik's constitutional rights and the constitutional rights of Plaintiffs' clients unless enjoined from doing so by this Court.

98. As early as Monday, January 25, 2021, Defendants will search the digital contents of the iPhone. See the email of the Assistant US Attorney, a true and accurate copy of which is attached as Exhibit D. That search will include a search of Privileged Information and Private Information downloaded to the iPhone after its seizure, and Defendants will search and seize Privileged Information and Private Information that is stored remotely but accessed through the iPhone.

99. The impending search and seizure of Privileged Information and Private Information is unreasonable, will cause irreparable and proximate harm to Plaintiffs and to Plaintiffs' clients, and will violate Mr. Malik's constitutional rights and the constitutional rights of Plaintiffs' clients.

100. To enforce their rights, Plaintiffs were required to hire an attorney and are entitled to reasonable attorney fees and costs of court.

CLAIMS FOR RELIEF

COUNT I - FIRST AMENDMENT (UNLAWFUL SEARCH & SEIZURE OF IPHONE)

101. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

102. Defendants violated the First Amendment by searching and seizing the iPhone containing expressive content, associational information, and personal information, absent reasonable suspicion to believe that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws.

103. Defendants violated the First Amendment by searching and seizing the iPhone containing expressive content, associational information, and personal information, absent probable cause to believe that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws.

104. Defendants violated the First Amendment by searching and seizing the iPhone containing expressive content, associational information, and personal information, absent a warrant supported by probable cause that the iPhone contains contraband or evidence of a violation of law, and without particularly describing the information to be searched.

COUNT II - FIRST AMENDMENT
(UNLAWFUL SEARCH OF INFORMATION ON SERVERS)

105. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

106. Defendants violated the First Amendment by searching and seizing Mr. Malik's digital information that was not on the iPhone at the time of the seizure but residing on servers throughout the United States and which contain expressive content, associational information, and private information, absent reasonable suspicion to believe that the information is evidence of a violation of criminal, immigration, or customs laws.

107. Defendants violated the First Amendment by searching and seizing Mr. Malik's digital information that was not on the iPhone at the time of the seizure but residing on servers throughout the United States and which contains expressive content, associational information,

and personal information, absent probable cause to believe that the information is evidence of a violation of criminal, immigration, or customs laws.

108. Defendants violated the First Amendment by searching and seizing Mr. Malik's digital information that was not on the iPhone at the time of the seizure but residing on servers throughout the United States and which contain expressive content, associational information, and personal information, absent a warrant supported by probable cause that the information is evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

COUNT III - FOURTH AMENDMENT
(UNLAWFUL SEARCH & SEIZURE OF IPHONE)

109. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

110. Defendants violated the Fourth Amendment by searching and seizing the iPhone and digital content containing expressive content, associational information, and personal information, absent reasonable suspicion that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws.

111. Defendants violated the Fourth Amendment by searching and seizing the iPhone and digital content containing expressive content, associational information, and personal information, absent probable cause to believe that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws.

112. Defendants violated the Fourth Amendment by searching and seizing the iPhone and digital content absent a warrant supported by probable cause that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

113. Defendants' search and seizure was unreasonable at the inception, and in scope, duration, and intrusiveness and in violation of the Fourth Amendment.

COUNT IV - FOURTH AMENDMENT
(UNLAWFUL SEARCH OF INFORMATION ON SERVERS)

114. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

115. Defendants violated the Fourth Amendment by searching and seizing the Privileged Information and Private Information residing on remote servers, absent reasonable suspicion that the information on the remote servers contains contraband or evidence of a violation of criminal, immigration, or customs laws.

116. Defendants violated the Fourth Amendment by searching and seizing the Privileged Information and Private Information residing on remote servers, absent probable cause to believe that the information on the remote servers contains contraband or evidence of a violation of criminal, immigration, or customs laws.

117. Defendants violated the Fourth Amendment by searching and seizing the Privileged Information and Private Information residing on remote servers, absent a warrant supported by probable cause that the information on the remote servers contains contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

118. Defendants' search and seizure of information residing on remote servers was unreasonable at the inception, and in scope, duration, and intrusiveness and in violation of the Fourth Amendment.

//

COUNT V - FOURTH AMENDMENT
(UNLAWFUL SEARCH & SEIZURE OF INFORMATION NOT ON THE IPHONE AT THE TIME OF THE SEIZURE)

119. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

120. Defendants violated the Fourth Amendment by searching and seizing the Privileged Information and Private Information that did not reside on the iPhone at the time of the seizure but that was downloaded to the iPhone after the iPhone's seizure, absent reasonable suspicion that the downloaded information contains contraband or evidence of a violation of criminal, immigration, or customs laws.

121. Defendants violated the Fourth Amendment by searching and seizing the Privileged Information and Private Information that did not reside on the iPhone at the time of the seizure but that was downloaded to the iPhone after the iPhone's seizure, absent probable cause to believe that the downloaded information contains contraband or evidence of a violation of criminal, immigration, or customs laws.

122. Defendants violated the Fourth Amendment by searching and seizing the Privileged Information and Private Information that did not reside on the iPhone at the time of the seizure but that was downloaded to the iPhone after the iPhone's seizure, absent a warrant supported by probable cause that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

123. Defendants' search and seizure of the downloaded information was unreasonable at the inception, and in scope, duration, and intrusiveness and in violation of the Fourth Amendment.

COUNT VI - FOURTH AMENDMENT
(UNLAWFUL SEIZURE OF IPHONE)

124. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

125. Defendants violated the Fourth Amendment by seizing the iPhone for the purpose of effectuating a search of that device after Mr. Malik had left the border, absent a warrant, probable cause, or reasonable suspicion that the iPhone contains contraband or evidence of a violation of criminal, immigration, or customs laws.

126. Defendants' seizure of the iPhone for the purpose of effectuating a search of that device after Mr. Malik had left the border was unreasonable at the inception, and in scope, duration, and intrusiveness, and in violation of the Fourth Amendment.

COUNT VII – UNLAWFUL SEARCH AND SEIZURE UNDER THE DIRECTIVE

127. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

128. The search and seizure of the iPhone and digital information that is stored remotely and accessible through the iPhone is unlawful because it was and is done in violation of the Directive.

COUNT VIII - ADMINISTRATIVE PROCEDURE ACT, 5 U.S.C. § 706
(AGENCY DIRECTIVE)

129. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

130. The Directive is a "final agency action" subject to judicial review under the Administrative Procedure Act, 5 U.S.C. § 704.

131. The Directive impermissibly permits CBP to conduct searches and seizures that violate the First and Fourth Amendments or that otherwise are not accordance with the law.

132. The Directive's rules regarding the use of a filter team fail to adequately protect attorney-client privileged information, work product privileged information, and other personal and confidential information of the traveler.

133. The Directive violates the Administrative Procedure Act because it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

134. The Directive violates the Administrative Procedure Act because it is "contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

COUNT IX - APPOINTMENT OF SPECIAL MASTER

135. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

136. Should the Court rule that a search may be made of the Privileged Information, this Court, pursuant to Fed. R. Civ. P. 53, and its inherent powers, has the authority to order that the search of the iPhone, including the Privileged Information and Private Information be conducted by a Special Master and under the supervision of this Court or a Magistrate Judge pursuant to protocols reviewed by the parties and approved by this Court or a Magistrate Judge.

137. The protocols should permit Plaintiffs to have a duplicate copy of the digital information to be searched prior to any search, permit Plaintiffs to contest any findings by a Special Master that a particular matter is not privileged by *in camera* review of this Court or a Magistrate Judge, and prohibit Defendants from reviewing any such digital information until first approved by this Court or a Magistrate Judge.

138. Defendants should be required to bear the entire cost of the Special Master.

COUNT X - TEMPORARY RESTRAINING ORDER

139. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

140. Plaintiffs have a substantial likelihood of success on the merits of this case. Immediate and irreparable injury, loss, or damage will result to Plaintiffs and their clients before Defendants may be heard in opposition unless this Court issues a temporary restraining order prohibiting Defendants from (1) searching the digital contents of the iPhone and using the iPhone to search digital information of Plaintiffs, (2) providing the iPhone or its digital contents to any other governmental agency, and (3) connecting the iPhone to the internet or to a communications network.

141. The threatened injury outweighs any harm that the temporary restraining order might cause Defendants. The temporary restraining order is in the public interest. The temporary restraining order will preserve the status quo until Defendants may be heard in opposition.

142. Additionally, pursuant to 5 U.S.C. § 705 issuance of injunctive relief sought in this case is necessary and appropriate to prevent irreparable injury, to preserve the Court's jurisdiction, and to preserve the status quo pending a final decision.

COUNT XI - PRELIMINARY INJUNCTION

143. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

144. Plaintiffs are entitled to a preliminary injunction if they show (1) a substantial likelihood that they will prevail on the merits of their claims, (2) a substantial threat that they will suffer an irreparable injury if the injunction is not granted, (3) their threatened injury

outweighs the threatened harm to Defendants, and (4) the public interest will not be disserved if the preliminary injunction is granted.

145. Plaintiffs have a substantial likelihood of success on the merits of this case. Immediate and irreparable injury, loss, or damage will result to Plaintiffs and their clients prior to judgment unless this Court issues an order prohibiting Defendants from (1) searching the digital contents of the iPhone and using the iPhone to search digital information of Plaintiffs, (2) providing the iPhone or its digital contents to any other governmental agency, and (3) connecting the iPhone to the internet or to a communications network.

146. The threatened injury outweighs any harm that the preliminary injunction might cause the Defendants and the injunctive order is in the public interest. The preliminary injunction will preserve the status quo until a final decision on the merits of this case.

147. Additionally, pursuant to 5 U.S.C. § 705 issuance of injunctive relief sought in this case is necessary and appropriate to prevent irreparable injury, to preserve the Court's jurisdiction, and to preserve the status quo until a final decision on the merits of this case.

COUNT XII - PERMANENT INJUNCTION

148. The allegations contained in paragraphs 1 through 100 of this Complaint are incorporated by reference as if fully set out herein.

149. Plaintiffs and their clients have suffered and will continue to suffer irreparable injury unless this Court issues a permanent injunction that orders Defendants to (1) Refrain from searching the digital information residing on the iPhone, (2) Refrain from accessing digital information of Plaintiffs through the iPhone, (3) Return the iPhone to Plaintiffs, (4) Inform Plaintiffs of the manner of any search of the iPhone that already has been conducted, (5) Refrain from providing the iPhone or its contents to any other governmental agency and inform Plaintiffs

of the name of any agency that has handled the iPhone or its contents, (6) Securely destroy all copies of digital information that Defendants obtained from the iPhone or by accessing the iPhone and inform Plaintiffs of the manner of the destruction.

150. There are no adequate remedies at law to prevent the irreparable injury to Plaintiff and their clients. Plaintiffs and their clients already have suffered an irreparable injury. Considering the balance of the hardships between the parties, a remedy in equity is warranted. The public interest would not be disserved by a permanent injunction.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs ask for the following relief as to all counts:

a. Declare that Defendants violated the rights of Mr. Malik under the First Amendment of the U.S. Constitution as articulated in Counts I and II.

b. Declare that Defendants violated the rights of Mr. Malik and Plaintiffs' clients under the Fourth Amendment of the U.S. Constitution as articulated in Counts III through VI.

c. Declare that the search and seizure of the iPhone and digital information that is stored remotely and accessible through the iPhone is unlawful because it was done in violation of the Directive as articulated in Count VII.

d. Declare that the Directive violates the Administrative Procedure Act as articulated in Count VIII, vacate all or part of the Directive, enjoin enforcement of all or part of the Directive against Plaintiffs, and enjoin enforcement of all or part of the Directive.

e. Should the Court determine that the iPhone may be searched, appoint a Special Master and determine the appropriate protocols as articulated in Count IX.

f. Issue a temporary restraining order as articulated in Count X.

g. Issue a preliminary injunction as articulated in Count XI.

h. Issue a permanent injunction as articulated in Count XII.

i. Award Plaintiffs reasonable attorneys' fees and costs.

j. Grant such other or further relief as the Court deems proper.

Respectfully submitted,

ROY PETTY & ASSOCIATES, PLLC

/s/ Roy Petty

Roy Petty
Texas Bar No. 24043870
PO Box 561063
Dallas, TX 75356
Tel. 214.905.1420
Fax 214.905.2010
roy@roypetty.com
ATTORNEY FOR PLAINTIFF

VERIFICATION

I, Adam A. Malik, am a Plaintiff named in this action. I state that I have read the contents of this Original Verified Complaint for Temporary Restraining Order, Preliminary Injunction, Permanent Injunction, & Declaratory Judgment, and the exhibits submitted in support thereof, and I certify, for myself and on behalf of Malik & Associates, PLLC that the statements and claims made are true and correct to my knowledge, except as to those statements made on information and belief, and as to those, I believe them to be true.

January 25, 2021

Adam A. Malik, individually,
and as Managing Member of
Malik & Associates, PLLC

Date

SUBSCRIBED AND SWORN to before me this 25th day of January 2021.

Notary Public

ISABEL VICTORIA CARMONA
Notary Public, State of Texas
Comm. Expires 01-22-2025
Notary ID 12106669