UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

EDWARD BUTOWSKY, Plaintiff, v. DAVID FOLKENFLIK, et al., Defendants.	Civil Action No. 4:18-cv-00442-ALM-CMC

NON-PARTY DEMOCRATIC NATIONAL COMMITTEE'S RESPONSES AND OBJECTIONS TO SUBPOENA TO PRODUCE DOCUMENTS

Pursuant to Rule 45 and 26(b) of the Federal Rules of Civil Procedure, non-party Democratic National Committee ("DNC"), through its undersigned counsel, hereby submits its Responses and Objections to the Subpoena to Produce Documents (the "Subpoena"), issued in the above captioned action, from Plaintiff Edward Butowsky, as follows:

GENERAL OBJECTIONS

The following objections are based on the information and documents currently available to the DNC. The DNC reserves the right to alter, supplement, amend, or otherwise modify its objections based on later recollections, the recollections of persons presently unidentified or unavailable, or the discovery of additional documents or information.

1. The DNC objects to the Subpoena pursuant to Rule 45(d)(3)(A)(iii) of the Federal Rules of Civil Procedure because it seeks documents and materials protected by the attorney work product doctrine, the attorney-client privilege, a joint or common interest privilege, or any other privilege recognized by law, to which no exception or waiver applies.

2. The DNC objects to the Subpoena because it seeks documents and materials

protected by the associational privilege guaranteed by the First Amendment to the United States Constitution.

3. The DNC objects to the Subpoena to the extent it calls for disclosure of the DNC's confidential or proprietary business information, trade secrets, or commercially sensitive information.

4. The DNC objects to the Subpoena to the extent it calls for disclosure of information pertaining to the investigative activities of the Federal Bureau of Investigation, the Metropolitan Police Department, the U.S. Department of Justice, members of Congress, Congressional personnel, or any other governmental entity or personnel, that may implicate the government's interests in maintaining the confidentiality of its investigative activities.

5. The DNC objects to the Subpoena to the extent it calls for any individual's personal and private information that may be protected by such individual's right to privacy under the U.S. Constitution and/or any State constitution.

6. The DNC objects to the Subpoena under Rule 26 of the Federal Rules of Civil Procedure, because the burdens of producing the requested information would significantly outweigh the benefits of any such production. Specifically, the Subpoena seeks confidential documents and materials that would threaten the safety and security of the DNC if disclosed. The documents and materials sought assess the DNC's security vulnerabilities, provide information regarding the DNC's information technology and cyber security systems, and provide details outlining how a successful hack of the DNC could be orchestrated. If disclosed, such information could be used by individuals with malicious intent to harm the DNC, namely, by compromising or otherwise hacking into the DNC's information technology systems.

7. The DNC objects to the Subpoena to the extent that it purports to impose

obligations on the DNC greater than what the Federal Rules of Civil Procedure and other applicable laws require.

8. The DNC objects to the Subpoena to the extent that it seeks materials that are not within the DNC's possession, custody, or control.

9. The DNC objects to the Subpoena to the extent that it seeks discovery of information from sources that are not reasonably accessible in light of the burdens or costs required to identify, locate, restore, review, and produce whatever responsive information may be found.

10. The DNC objects to the Subpoena to the extent that it seeks documents that are not relevant to the claims and defenses asserted in the underlying action and are not likely to lead to the discovery of admissible evidence in the underlying action.

11. The DNC objects to the Subpoena's introductory description and definition of the "2016 Data Breach" as vague, overbroad, and burdensome. The definition and description of the "2016 Data Breach" fails to accurately describe the facts and circumstances of the infiltration of the DNC and subsequent events.

12. The DNC objects to Subpoena on the basis that the subpoena is in violation of the geographical limitation set forth in Fed. R. Civ. P. 45(c) and is therefore invalid.

13. The DNC further objects on the basis that this subpoena fails to avoid imposing an undue burden or expense on the DNC under Fed. R. Civ. P. 45(d)(1) because the Court has not yet issued a final ruling on Defendants' Motion to Dismiss, ECF No. 25. *See* ECF Nos. 58, 63-64. Thus, the Court may determine that this case should not proceed or issue a ruling that narrows the matters in dispute. It is inappropriate and unduly burdensome to proceed with third-party discovery until such time as the Court issues a final adjudication on the motion.

14. The DNC objects to the Subpoena on the basis that it seeks information that is

equally or more easily available to the parties through party discovery.

15. The DNC also objects on the basis that there is no protective order in place in this action and the Subpoena requests highly confidential and sensitive information.

16. The DNC reserves the right to seek all appropriate remedies and sanctions resulting from the Defendants' presentation of unnecessary and improper discovery requests, including, but not limited to, related costs and counsel fees incurred by the DNC in responding to the Subpoena pursuant to applicable legal authorities.

17. By responding to the Subpoena, the DNC does not in any way waive or intend to waive any objection as to the relevance or admissibility of any document produced in response to the Subpoena. Nor do the Objections set forth herein in any way admit or imply the existence or nonexistence of the documents requested.

18. Each of these General Objections is hereby specifically incorporated into each set of the Specific Objections and Responses, set forth below.

1. Produce unredacted copies of all reports (and draft reports) that CrowdStrike, Inc. (hereinafter "CrowdStrike") prepared or submitted regarding the 2016 Data Breach (or any other breaches of DNC servers during 2016).

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 1 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine. The DNC further objects on the basis that any of the CrowdStrike's reports or draft reports that have not been made publicly available are protected by the applicable privileges as CrowdStrike was retained by the DNC's counsel to conduct an investigation to assist in the provision of legal advice to the DNC.

The DNC also objects to Request Number 1 on the ground that it infringes on the DNC's

associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 1 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 1 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 1.

2. Produce mirror image(s) of the disks that were breached during the 2016 Data Breach (or any other security breaches of DNC servers during 2016) as of the time those breach(es) was/were first detected by CrowdStrike and/or the DNC system administrator.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to this Request on the basis that this Request essentially seeks all documents and

information of the DNC and is facially overbroad. The DNC further objects to the term "disks" as undefined and vague and ambiguous in the context of the cyberattack on the DNC systems. The DNC further objects to Request Number 2 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine. The DNC also objects to Request Number 2 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 2 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 2 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 2.

3. Produce all documents, communications, records or other evidence regarding the 2016 Data Breach (or any other security breaches of DNC servers during 2016) that were exchanged between (1) the DNC, and (2) government investigators *(e.g.,* the FBI or Metropolitan Police Department), the U.S. Department of Justice, members of Congress, Congressional personnel, or CrowdStrike or its representatives.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 3 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, the law enforcement investigatory privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 3 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 3 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security

protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 3 is overbroad, unduly burdensome, and seeks information that is not relevant to any claims or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 3.

4. For the period from January 1, 2016 until July 10, 2016, produce user access logs for each of the disks identified in Paragraph 2.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 4 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine. The DNC further objects to the term "disks" as undefined and vague and ambiguous in the context of the cyberattack on the DNC systems.

The DNC also objects as the production of "user access logs" during that period would reflect potentially thousands of users who have nothing to do with any of the issues in this case. The DNC also objects to Request Number 4 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and

tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 4 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 4 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 4.

5. For the period from January 1, 2016 to July 10, 2016, produce records indicating all occasions (time and date) that Seth Rich downloaded or saved onto any device (e.g., flash drive, data disc, etc.) more than 10 GB of data from Democratic National Committee servers, as well as records reflecting the exact amount of data greater than 10 GB that Seth Rich downloaded.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 5 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 5 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election*

Comm'n, 333 F.3d 168, 177-78 (D.C. Cir. 2003).

Additionally, the DNC objects to Request Number 5 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 5 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 5.

6. For the period from January 1, 2016 to July 10, 2016, produce records indicating all other occasions (time and date) that more than 10 GB of data were downloaded or saved from Democratic National Committee servers onto any device (e.g., flash drive, data disc, etc.), as well as records reflecting (1) the exact amount of data greater than 10 GB that was downloaded and (2) the person or persons responsible for each such download.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC also objects to Request Number 6 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could

also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 6 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 6 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 6.

7. Produce for inspection the actual servers that were breached as part of the 2016 Data Breach. If the servers were destroyed or if data relevant to the breach was altered, removed or destroyed, produce records reflecting the same. *Note: If the servers cannot be produced in Texas (e.g., because they are still in use elsewhere), then the Plaintiff's experts are willing to inspect them at a mutually agreeable location.*

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC objects to this Request on the basis that this Request essentially seeks all documents and information of the DNC and is facially overbroad. The DNC further objects to Request Number 7 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, the law enforcement investigatory privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 7 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political

information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 7 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 7 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

The DNC further objects, as set forth in General Objection No. 12 incorporated herein, that this Request specifically requests production beyond the geographical limitation required by Fed. R. Civ. P. 45(c) and is therefore invalid.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 7.

8. For the 120 days preceding Seth Rich's death, produce all texts, emails and/or instant messages exchanged among/between Seth Rich and any other person or persons. Also produce all texts, emails and/or instant messages that referenced Seth Rich during that time period.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 8 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 8 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 8 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. This Request would require the DNC to search through thousands of emails, texts and/or IM which have nothing to do

with this case. Thus, the DNC also objects to the extent Request Number 8 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 8.

9. Produce, records or communications identifying all individuals and/or entitles (government or otherwise) who were allowed to examine the DNC servers (or mirror images of those servers) after the 2016 Data Breach or after any other security breaches of DNC servers during 2016.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 9 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, the law enforcement investigatory privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 9 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 9 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 9 is overbroad, unduly burdensome, seeks information not relevant to any claim or defense in this matter and unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 9.

10. Produce all documents, records, or communications setting the parameters of what information CrowdStrike was or was not allowed to share with government agencies or representatives (*e.g.*, FBI, Metropolitan Police, Congressional investigators, etc.) regarding the unauthorized release of data from Democratic National Committee servers. If, for example, an email forbade CrowdStrike (or its representatives) from sharing certain information from the FBI, that email should be produced.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 10 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, the law enforcement investigatory privilege, and the common or joint interest doctrine. The DNC further objects on the basis that any of the CrowdStrike's reports or draft reports that have not been made publicly available are protected by the applicable privileges as CrowdStrike was retained by the DNC's counsel to conduct an investigation to assist in the provision of legal advice to the DNC.

The DNC also objects to Request Number 10 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political

information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 10 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 10 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 10.

11. Produce all metadata (*e.g.*, download speeds, file markings, etc.) indicating whether the 2016 Data Breach was the result of (1) outside forces *(e.g.,* Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who entered DNC facilities and downloaded the data onto a storage device.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 11 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 11 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 11 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 11 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 11.

12. Produce all documents, communications, records or other evidence (including written reports) suggesting that someone other than Russian hackers may have been responsible for the 2016 Data Breach.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC

further objects to Request Number 12 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine

The DNC also objects to Request Number 12 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 12 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 12 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request

Number 12.

13. Produce all documents, communications, records or other evidence (including written reports) suggesting that Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, and/or Rao Abbas improperly accessed data, improperly removed data, or otherwise compromised the security of the DNC's computer systems.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 13 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 13 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 13 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also

objects to the extent Request Number 13 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 13.

14. Produce. all documents, communications, records or other evidence (including written reports) indicating what role, if any, that Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, and/or Rao Abbas held with respect to the DNC and/or its information systems (e.g., employment status and title; contractor status; or subcontractor status) during 2016.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 14 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine.

The DNC also objects to Request Number 14 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 14 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 14 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 14.

15. Produce all documents, communications, records or other evidence indicating whether the DNC had terminated Seth Rich or was planning to terminate Seth Rich as of the date of his death.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 15 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine. The DNC also objects to Request Number 15 as it requests confidential employee information. The DNC also objects to the extent Request Number 15 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 15.

16. Produce a copy of Seth Rich's final paycheck (after deposit) or records indicating the bank and account into which his final earnings were deposited.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 16 because it seeks documents and materials protected by the

attorney work product doctrine, the attorney client privilege, and the common or joint interest doctrine. The DNC also objects to Request Number 16 as it requests confidential employee information. The DNC also objects to the extent Request Number 16 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 16.

17. A July 18, 2018 *Washington Post* article (https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons campaign/?noredirect=on&utm_term=alfd9f9dba2a) lists several alleged dates that Russian hackers tried to compromise DNC servers:

> **March 15, 2016**. Russian hackers allegedly begin trying to identify vulnerabilities in the network of the Democratic National Committee.
> **April 18, 2016.** Hackers allegedly gain access to the DNC network using credentials stolen from a Democratic Congressional Campaign Committee ("DCCC") employee. By June, they've allegedly compromised 33 computers, using the same relay system as for the DCCC
> **April 22, 2016**. Hackers allegedly compress and steal several gigabytes of opposition research material.
> **May 2016.** Both the DCCC and DNC become aware that their networks have been compromised.
> **May 25 - June 1, 2016**. Hackers allegedly access the DNC's Microsoft Exchange server and steal thousands of emails.
>
> Produce all evidence (*e.g.*, user logs) that corroborates or refutes the *Washington Post's* allegations above regarding the activities of Russian hackers.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 17 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, law enforcement investigatory privilege and the common or joint interest doctrine.

The DNC also objects to Request Number 17 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution,

because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 17 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 17 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request Number 17.

18. If any item or thing requested by this subpoena was destroyed, produce documents, communications, records or other evidence indicating as much.

RESPONSE: The DNC incorporates its General Objections set forth above. The DNC further objects to Request Number 18 because it seeks documents and materials protected by the attorney work product doctrine, the attorney client privilege, and the common or joint interest

doctrine. The DNC further objects to this Request on the basis that it is vague and ambiguous as to time period, encompasses documents and things subject to a general retention policy, and would require an extensive and burdensome review of the DNC's systems.

The DNC also objects to Request Number 18 on the ground that it infringes on the DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. *See e.g. Am. Fed'n of Labor & Cong. of Indus. Organizations v. Fed. Election Comm'n,* 333 F.3d 168, 177-78 (D.C. Cir. 2003). Moreover, in the event the DNC were subject to yet another hack, the illegal exfiltration and subsequent release of such documents would reveal the DNC's political activities, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity.

Additionally, the DNC objects to Request Number 18 because under Rule 26 of the Federal Rules of Civil Procedure, the burdens of producing the requested information—including the grave risk to the safety and security of the DNC, its information technology, and cyber security protocols—would significantly outweigh the benefits of any such production. The DNC also objects to the extent Request Number 18 is overbroad, unduly burdensome, and seeks information that is not relevant to any claim or defense in this matter and that is unlikely to lead to the discovery of admissible evidence.

Pursuant to its Objections, the DNC will not produce documents in response to Request

Number 18.

Dated: July 22, 2019

Respectfully submitted,

DEMOCRATIC NATIONAL COMMITTEE

By: /s/ Graham Wilson

Graham Wilson
John Geise
Perkins Coie LLP
700 13th St NW, Suite 600
Washington, DC 20005-3960
202.654.6200
gwilson@perkinscoie.com
jgeise@perkinscoie.com

Debra R. Bernard
Perkins Coie LLP
131 South Dearborn Street, Suite 1700
Chicago, IL 60603-5559
312.324.8400
dbernard@perkinscoie.com

CERTIFICATE OF SERVICE

I hereby certify that on July 22, 2019, a copy of the foregoing was served via U.S. Mail and Email to the following attorney of record:

Ty Clevenger
P.O. Box 20753
Brooklyn, NY 11202
tyclevenger@yahoo.com
979-985-5289

Date: 7/22/19 Signed: [signature]