CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

June 3, 2021

Mr. Joseph Blount
Chief Executive Officer
Colonial Pipeline Company
1185 Sanctuary Parkway
Suite 100
Alpharetta, GA 30009

Dear Mr. Blount:

I am writing to request documents related to Colonial Pipeline's decision to pay a ransom to an Eastern European cybercrime group following a ransomware attack against the company on May 7, 2021, that led to the shutdown of 5,500 miles of pipelines supplying approximately 45% of fuel consumed on the East Coast.[1] The ransomware attack disrupted energy supplies across the region for days, driving gas prices to their highest levels in six and a half years.[2]

According to press reports, a Colonial Pipeline employee found a ransom note from hackers on a control-room computer at 5:30 a.m. on May 7, 2021.[3] Shortly thereafter, Colonial Pipeline shut down the entire 5,500-mile pipeline, engaged the services of cybersecurity firm FireEye Mandiant, and contacted various federal offices.[4]

After the ransomware attack, the FBI identified the hacking group Darkside, believed to be based in Russia or Eastern Europe, as being responsible for the attack.[5] On May 13, news reports indicated that Colonial Pipeline had paid nearly $5 million in ransom to Darkside.[6]

---

[1] *Ransomware Attack Leads to Shutdown of Major U.S. Pipeline System*, Washington Post (May 8, 2021) (online at www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/).

[2] *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall Street Journal (May 19, 2021) (online at www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636).

[3] *Id.*

[4] Briefing by Marie Mouchet, Vice President and Chief Information Officer, Colonial Pipeline, to Staff, Committee on Oversight and Reform and Committee on Homeland Security (May 17, 2021).

[5] *Russian Criminal Group Suspected in Colonial Pipeline Ransomware Attack*, NBC News (May 9, 2021) (online at www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793).

[6] *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*, Bloomberg (May 13, 2021) (online at www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom).

On May 17, executives from Colonial Pipeline met with staff of the Oversight Committee and the Committee on Homeland Security but refused to share any information related to the reported payment of ransom, including whether the company consulted with federal authorities before the ransom was paid.[7] However, you subsequently gave an interview to the *Wall Street Journal* in which you admitted that Colonial Pipeline paid $4.4 million to attackers and said you made this decision on the same day the attack was discovered.[8] In the interview, you stated that the decision "was the right thing to do for the country."[9]

I am troubled that the company declined to provide the Committees with any information regarding how and why you decided to pay the attackers, including whether federal agencies and law enforcement had any input on your decision. In addition, I am extremely concerned that the decision to pay international criminal actors sets a dangerous precedent that will put an even bigger target on the back of critical infrastructure going forward.

Congress needs detailed information about the ransom payment that Colonial Pipeline made to international criminal actors to legislate effectively on ransomware and cybersecurity in the United States. Although the Department of Homeland Security has recently issued a security directive designed to increase transparency and improve the cybersecurity posture of pipelines, that directive will not eliminate the pressing problem of ransomware, which affects numerous other industries and government entities.

For all these reasons, I request that you provide the following information and documents, regardless of whether they reside on personal or business accounts, to the Committee no later than June 17, 2021:

1. All documents and communications relating to the discovery of the May 7, 2021, ransomware attack;

2. All documents and communications relating to the ransom, including but not limited to the following:

    a. any communications with the attackers about the ransom payment or the receipt of the decryption key;

    b. any consultation or communications with outside experts or federal agencies regarding the identity of the cybercriminals and whether to pay ransom;

---

[7] Briefing by Marie Mouchet, Vice President and Chief Information Officer, Colonial Pipeline, to Staff, Committee on Oversight and Reform and Committee on Homeland Security (May 17, 2021).

[8] *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall Street Journal (May 19, 2021) (online at www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636).

[9] *Id.*

c. the purchase and transfer of Bitcoin and other cryptocurrencies and any intermediaries used in such transactions;

d. any sanctions screening regarding the ransom payment; and

e. any internal communications among employees of Colonial Pipeline regarding the ransom payment; and

3. All documents and communications relating to the decryption tool provided by the attackers, including the performance of the decryption tool and the company's decision to use its own tools to bring the pipelines back online.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

An attachment to this letter provides additional instructions for responding to this request. If you have any questions, please contact Committee staff at (202) 225-5051.

Sincerely,

Carolyn B. Maloney
Chairwoman

Enclosure

cc: The Honorable James Comer, Ranking Member

Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.

2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.

3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.

4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.

5. Documents produced in electronic format should be organized, identified, and indexed electronically.

6. Electronic document productions should be prepared according to the following standards:

    a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.

    b. Document numbers in the load file should match document Bates numbers and TIF file names.

    c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

    d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:

        BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.

8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.

9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.

10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.

11. The pendency of or potential for litigation shall not be a basis to withhold any information.

12. In accordance with 5 U.S.C.§ 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.

13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.

14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.

15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.

16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.

17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.

19. All documents shall be Bates-stamped sequentially and produced sequentially.

20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.

21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic

message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.

4. The term “including” shall be construed broadly to mean “including, but not limited to.”

5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.

6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.

7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.

8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.

9. The term “individual” means all natural persons and all persons or entities acting on their behalf.