

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. Dino E. Robusto
Chief Executive Officer
CNA Financial Corporation
151 North Franklin Street
Chicago, IL 60606

Dear Mr. Robusto:

I am writing to request documents related to CNA Financial Corporation's decision to pay a \$40 million ransom to a cybercrime group following a ransomware attack against the company on March 21, 2021.¹ Press reports indicate that the attack against your company—one of the largest insurance companies in the United States and a major cyber insurance provider—encrypted 15,000 company devices and led to widespread network disruption.² The attackers reportedly accessed and stole company data, though the extent of the theft and the identity of the attackers have not been reported in detail.³ CNA's systems were not fully restored until May 12, nearly two months after the initial attack.⁴

Recently, *Bloomberg* reported that CNA paid \$40 million in ransom in April 2021 to regain control of its systems. According to the article, CNA paid hackers approximately two weeks after “a trove of company data was stolen” and CNA executives were locked out of the company's systems. It is unclear why it still took months to restore the company's systems following payment of the ransom. A spokesperson for your company stated that CNA had “followed all laws, regulations, and published guidance, including [Office of Foreign Asset

¹ *CNA Financial Hit by Cyberattack*, Security Magazine (Mar. 25, 2021) (online at www.securitymagazine.com/articles/94895-cna-financial-hit-by-cyberattack).

² *CNA Central, CNA Surety Now Back Online; Work on Other Portals Continues*, Insurance Journal (Apr. 6, 2021) (online at www.insurancejournal.com/news/national/2021/04/06/608685.htm).

³ *CNA Financial Paid \$40 Million in Ransom After March Cyberattack*, Bloomberg (May 20, 2021) (online at www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack).

⁴ CNA Financial Corporation, *Security Incident Update* (May 12, 2021) (online at www.cna.com/web/wcm/connect/96a7c7dd-96d1-41cc-8a0c-25604bfc2898/Security-Incident-Update-5-12-21.pdf?MOD=AJPERES).

Control]'s 2020 ransomware guidance.” However, the company has not commented on the ransom.⁵

I am concerned that the decision to pay the cybercriminal actors sets a dangerous precedent that will put an even bigger target on the backs of companies at risk for ransomware attacks going forward. CNA’s payment of a ransom to cybercriminals is the latest example of a company paying millions of dollars in ransom without any public disclosure. Congress needs detailed information about ransom payments that companies like CNA made to cybercriminal actors to legislate effectively on ransomware and cybersecurity in the United States.

For these reasons, I request that you provide the following information and documents, regardless of whether they reside on personal or business systems or accounts, to the Committee by June 17, 2021:

1. All documents and communications relating to the discovery of the March 21, 2021, ransomware attack against CNA;
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 any decryption tool;
 - b. any consultation or communications with outside experts or federal agencies regarding the identity of the cybercriminals and the issue of whether to pay ransom;
 - c. the transfer of funds or cryptocurrencies to the attackers, their representatives, or accounts or cryptocurrency wallets under their control, and any intermediaries used in such transactions;
 - d. any sanctions screening regarding the ransom payment, including verification of the identity of the recipient of any payment; and
 - e. any internal communications among employees of CNA regarding the ransom payment; and
3. Documents sufficient to show, in fiscal years 2020 and 2021:
 - a. the aggregate number of claims relating to a ransomware attack, data breach incident, or other information security incident by holders of insurance policies issued or brokered by CNA or its affiliates;

⁵ *CNA Financial Paid \$40 Million in Ransom After March Cyberattack*, Bloomberg (May 20, 2021) (online at www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack).

- b. the aggregate total dollar amount paid on the claims described in request 3.a; and
- c. the highest dollar amount paid on any single claim described in request 3.a.

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
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.