NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

July 8, 2021

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Legal Notice of Information Security Incident*

Dear Sir or Madam:

I am writing on behalf of my client, CNA Financial Corporation ("CNA"), to inform you that CNA sustained a sophisticated ransomware attack that may have involved the personal information of 205 New Hampshire residents. As further explained below, while CNA is providing notification to impacted individuals, CNA's investigation concluded there is no reason to suspect any information has or will be misused and that there is no risk of harm to individuals arising from the incident.

On March 21, 2021, CNA discovered it was the victim of a sophisticated ransomware attack (the "Incident"). CNA immediately began implementing containment steps, launched an investigation, and engaged third-party cybersecurity experts to assist (the "Forensic Team"). CNA also immediately reported the Incident to federal law enforcement and has been supporting their investigation ever since.

CNA's investigation determined that the Threat Actor first gained access to an employee's workstation on March 5, 2021 with a fake browser update that executed after the employee visited a legitimate website. Although the employee did not have elevated privileges, the Threat Actor obtained credentials through additional malicious activity. With elevated privileges, the Threat Actor moved laterally within the environment to conduct reconnaissance and establish persistence onto certain systems within the environment. Between March 5 and March 20, 2021, the threat actor conducted reconnaissance within CNA's IT environment using legitimate tools and legitimate credentials to avoid detection and to establish persistence. On March 20 and into March 21, 2021, the Threat Actor disabled monitoring and security tools; destroyed and disabled certain CNA back-ups; and deployed ransomware onto certain systems within the environment, leading CNA to proactively disconnect systems globally as an immediate containment measure.

Prior to deploying the ransomware, the Threat Actor copied, compressed and staged unstructured data obtained from file shares found on three CNA virtual servers; and used MEGAsync, a legitimate tool, to copy some of that unstructured data ("Exported Data") from the CNA

environment directly into the threat actor's cloud-based account (the "Mega Account") hosted by Mega NZ Limited ("Mega").

Fortunately, CNA's forensic experts, in coordination with the FBI, were able to confirm the Exported Data moved directly from the CNA environment into the threat actor's Mega Account, without any evidence of it being viewed or otherwise shared. The Exported Data was secured in encrypted form in the Mega Account by the Threat Actor, such that no one, not even Mega, could access the data without the decryption key. Working with the FBI and the Cloud-Storage Platform provider, CNA was able to take control of the account and quickly recover CNA's data. In addition, Mega supplied information related to the Threat Actor's account, which indicated there is no evidence that the CNA data in the Threat Actor's account was shared outside the Threat Actor's account. CNA's forensic investigation confirms that the Exported Data recovered by CNA is the full set of data copied out of the environment. With respect to data encrypted by the malware, the data was merely encrypted and saved locally to CNA systems and there was no ability for the malware to exfiltrate/copy encrypted data from the environment.

Furthermore, threat intelligence and the nature of the attack strongly suggest that the attacker's goal was simply to hold CNA's data hostage for extortion purposes, rather than sell or misuse it. Importantly, CNA has been conducting dark web scans and searches for CNA-related information, and CNA has not located any copies of the Exported Data and while CNA will continue such searches, does not anticipate finding any CNA data in connection with this attack. Lastly, there is affirmative evidence that CNA was not targeted by the Threat Actor for any of its data, and instead was a crime of opportunity based on the initial attack vector and subsequent theft of the Exported Data.

Taking into account all of the facts and circumstances delineated above, CNA determined that there is no evidence that the Threat Actor viewed, retained or shared the Exported Data and, thus, no risk of harm to individuals arising from the incident. Although CNA believes that notification to individuals is not required by applicable law, CNA plans to notify individuals whose personal information was contained in the Exported Data.

The overwhelming majority (greater than 90%) of the individuals being notified are employees, former employees, and their dependents. In addition, some claimants and policyholders will also be notified. The affected data includes name and Social Security number. In a smaller number of cases, individuals also had their date of birth, benefit enrollment and/or medical information affected.

CNA will begin notifying affected residents by First Class mail on July 9, 2021 and will be offering 24 months of complimentary credit monitoring and fraud protection services. A copy of the notice letter is attached. CNA is also providing a toll-free hotline for the individuals to call with any questions regarding the Incident.

To help prevent a similar occurrence in the future, CNA has implemented numerous measures to enhance the security of its networks, systems, and data, including for example:

- Deploying additional endpoint detection and response tools to systems across the environment;
- Enhancing network restrictions;

- Accelerating its existing project to implement an advanced privilege access management solution; and
- Engaging a new managed security service provider, in addition to the managed Security Operations Center that was in place prior to the Incident.

In addition, CNA is currently working with external cybersecurity experts to evaluate additional opportunities to further enhance CNA's information security program, including aspects of people, processes, and tools, in an effort to continuously improve CNA's security posture in the months and years ahead.

If you have any questions or need further information regarding this Incident, please do not hesitate to contact me.

Respectfully submitted,

Chris Cwalina

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 9, 2021

G5946-L01-0000001 T00001 P001 ********SCH 5-DIGIT 32808
SAMPLE A. SAMPLE - L01 US EMPLOYEE NO PHI
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

CNA Financial Corporation ("CNA") was recently the target of a sophisticated ransomware attack. We have no evidence that any of your personal information has or will be misused, but we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on proactive steps you may consider taking to help protect your information.

What Happened

On March 21, 2021, CNA discovered that it sustained a sophisticated ransomware attack. Once the incident was discovered, CNA immediately retained leading cybersecurity firms to assist in responding and help conduct a thorough investigation of the incident.

The investigation revealed that the threat actor accessed certain CNA systems at various times from March 5, 2021 to March 21, 2021. During this time period, the threat actor copied a limited amount information before deploying the ransomware. However, CNA was able to quickly recover that information and there was no indication that the data was viewed, retained or shared. Therefore, we have no reason to suspect your information has or will be misused.

What Information Was Involved

Having recovered the information, we have now completed our review of that information and have determined it contained some of your personal information including your name and Social Security number.

What We Are Doing

CNA immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. Additionally, to help prevent a similar occurrence in the future, we implemented numerous additional measures designed to enhance the security of our network, systems, and data.

What You Can Do

Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

As an added precaution, to help protect your personal information, we are offering a complimentary 24 month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **October 9, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 671-0412 by **October 9, 2021.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact us.

Sincerely,

Garrett Williams
Chief Compliance Officer

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.