May 26, 2022

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

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

Tel +1 202 662 0200
Fax +1 202 662 4643

Via email: consumer@ag.iowa.gov

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: *Legal Notice of Information Cyber Event*

Dear Sir or Madam:

I am writing on behalf of my client, Aon Corporation PLC ("Aon"), to inform you that Aon was the target of a cyber event that may have involved the personal information of 147 Iowa residents. We are continuing to receive direction regarding notice from our clients, and we will provide a supplemental notice when the total number of impacted residents changes. As further explained below, while Aon is providing notification to impacted individuals, Aon's investigation concluded there is no reason to suspect any information has or will be misused and Aon, with the support of its investigation team, has concluded there is no risk of harm to individuals arising from the event. Nonetheless, at this time Aon is providing notice to 147 individuals in Iowa.

On February 25, 2022, Aon identified a cyber event that, upon investigation, impacted a limited number of systems (the "event"). Aon immediately launched an investigation and engaged third-party advisors, incident response professionals and counsel. Aon also reported the event to federal law enforcement and has been supporting their investigation ever since. At the same time, in an abundance of caution, Aon also chose to disclose this event in an 8-K filing on February 25. Notwithstanding these actions, the event did not have a significant impact on Aon's operations, and no Aon systems were encrypted, disabled, or taken off-line in any way.

Aon's investigation determined that an unauthorized third party first gained access to Aon's environment on December 29, 2020, via a "Zero Day" vulnerability. A Zero Day vulnerability is an undisclosed vulnerability, meaning Aon had no opportunity to know about, let alone remediate, the vulnerability exploited to launch the cyber event. This vulnerability [**CVE-2021-27852**] was eventually published by CheckBox Survey Inc., in May 2021.

While the unauthorized third party added a backdoor at this time, it was not until December 2021 that the unauthorized third party began to move laterally in Aon's network, ultimately stole data, and extorted the company on February 25, 2022.

The unauthorized third party copied, compressed and staged unstructured data obtained from certain SharePoint sites and Outlook Mailboxes (the "Temporarily Obtained Data"). Using forensic data Aon was able to confirm what data was exported. In addition, Aon was able to obtain information from the unauthorized third party to corroborate its forensic findings. With this information, Aon has a high degree of confidence that it was able to review all Exported Data to determine notification obligations.

Based on forensic facts and other evidence, Aon has concluded that the Temporarily Obtained Data is no longer at risk. First, threat intelligence and the nature of the attack strongly suggest that the unauthorized third party's goal was simply to hold Aon's data hostage for extortion purposes, rather than sell or misuse it. Second, Aon reached a settlement with the unauthorized third party in exchange for the deletion of the Temporarily Obtained Data. The unauthorized third party provided strong evidence that matches our forensic evidence indicating the Temporarily Obtained Data has in fact been deleted and no longer resides in the unauthorized third party's possession. Federal law enforcement's experience with this unauthorized third party supports our belief that the unauthorized third party has in fact deleted the information and a copy does not exist.

Third, Aon continues to conduct dark web monitoring and searches for the Temporarily Obtained Data and has found no instances of it being sold. While Aon plans to continue these searches, it does not anticipate finding any Temporarily Obtained Data in connection with this event.

Fourth, the Temporarily Obtained Data was entirely unstructured information either from SharePoint sites or email. While some personal information was included in the documents, it would take the unauthorized third party significant resources to extract and use that information. Indeed, the process of reconfiguring, reviewing and identifying personal information in the Temporarily Obtained Data took a large team of experts weeks to accomplish. It is highly unlikely that any unauthorized third party would invest the same resources to find and pull together these disparate pieces of personal information to ultimately identify and/or target individuals.

Moreover, with respect to the review, Aon confirmed that only a limited set of documents even contained personal information – less than 1 percent – a remarkably low percentage, compared with other cases. This is because personal data was segmented and, in many circumstances, either deidentified, masked or otherwise unidentifiable. The low instance of personal data found in the Temporarily Obtained Data is due in large part to Aon's company-wide data minimization efforts.

Taking into account all of the facts and circumstances of this event, Aon determined that there is no risk of harm to individuals arising from the event. Although Aon believes that notification to individuals is not required because there is no risk, Aon plans to notify individuals whose personal information was contained in the Temporarily Obtained Data.

The majority of individuals who will receive notice are associated with or employed by entities that receive professional services from Aon, including insurance brokerage and consulting. The affected data includes name, driver's license number, Social Security number and in a smaller number of cases, benefit enrollment and/or medical information.

Aon will begin notifying affected residents by First Class mail on May 27, 2022 and will be offering 24 months of complimentary credit monitoring and fraud protection services to impacted individuals. A copy of the notice letter is attached. Aon is also providing a toll-free hotline for the individuals to call with any questions regarding the event.

Aon has taken steps to contain this event by putting enhanced controls in place that are designed to further strengthen existing safeguards. Those steps include but are not limited to:

- Engaging external security experts to investigate the event;
- Enhancing security, including upgrading and expanding internal and external multi-factor authentication (MFA);
- Reviewing and updating account permissions;
- Resetting user passwords firm-wide; and
- Enhancing security by deploying CrowdStrike Falcon, a leading Endpoint Protection Platform.

Furthermore, Aon engaged with other third-party advisors, incident response professionals – including leading forensic experts at CrowdStrike – counsel, as well as law enforcement, to supplement our investigation and further secure our environment.

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

Respectfully submitted,

Chris Cwalina

Return Mail Processing
PO Box 999
Suwanee, GA 30024

128 1 27904 **********SNGLP
SAMPLE A. SAMPLE - LV01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

May 27, 2022

RE: Notice of Data Breach

Dear Sample A. Sample:

Aon PLC ("Aon") was recently the target of a cyber event that the firm identified impacted a limited number of Aon systems. 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 February 25, 2022, Aon identified a cyber incident that, upon investigation, impacted a limited number of systems. Once the incident was discovered, Aon immediately retained leading cybersecurity firms to assist in responding and help conduct a thorough investigation of the incident.

The investigation revealed that an unauthorized third party accessed certain Aon systems at various times between December 29, 2020 – February 26, 2022. Findings from the investigation indicate the unauthorized third party temporarily obtained certain documents containing personal information from Aon systems during this period. Aon has taken steps to confirm that the unauthorized third party no longer has access to the data and Aon has no indication the unauthorized third party further copied, retained, or shared any of the data. We have no reason to suspect your information has or will be misused.

What Information Was Involved?

Aon reviewed the data that was obtained and determined it contained some of your personal information, including your name and one or more of the following: Social Security number, driver's license number, and, in a small number of cases, benefit enrollment information.

What We Are Doing.

Aon immediately reported the incident to, and is working closely with, law enforcement authorities, including the FBI. Additionally, to prevent a similar occurrence in the future, we implemented numerous measures designed to enhance the security of our network, systems, and data. Aon will continue to evaluate additional steps that may be taken to further enhance the firm's security environment.

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 security freeze on your credit file.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** August 31, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 575-2853 by August 31, 2022. Be prepared to provide engagement number B053207 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 call **(833) 575-2853**, Monday through Friday, between 9 a.m. to 11 p.m. Eastern Time, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern Time.

Sincerely,

Brad Bryant

Brad Bryant
Global Chief Privacy Officer

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 vvvvw.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, 1-860-8085318, 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, 1-888-7430023.

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 / 1800-697- 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.