November 10, 2021

BY U.S. MAIL

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

To Whom It May Concern:

Atlantic Specialty Insurance Company, on its own behalf and on behalf of its subsidiaries OBI National Insurance Company and OBI America Insurance Company ("ASIC" or the "Company"), pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(B), provides this notice of a cybersecurity incident that occurred at ASIC's former vendor, Gallagher Bassett Services, Inc., a subsidiary of Arthur J. Gallagher & Co (together, "Gallagher"), between June 3, 2020 and September 26, 2020 (the "Gallagher Security Incident" or the "Incident"). The ASIC companies are insurance companies that use the marketing brand Intact Insurance Specialty Solutions to offer a broad range of specialty insurance products through independent agencies, regional and national brokers, wholesalers and managing general agencies, targeted to specific customer groups or industry segments. Gallagher's principal place of business is located at 2850 W. Golf Rd., Rolling Meadows, IL 60008.

On October 19, 2021, ASIC became aware that a number of U.S. individuals associated with ASIC may have been impacted in the Gallagher Security Incident. This includes 7 individuals residing in New Hampshire. The types of personal information that may have been accessed for these individuals included names, addresses, and Social Security numbers.

From July 1, 2009 to August 12, 2020, ASIC, through its direct parent, OneBeacon Insurance Group, LLC (now known as Intact Insurance Group USA LLC), retained Gallagher to provide various claims administration related services, pursuant to which ASIC shared certain information belonging to its insured's claimants with Gallagher as part of its normal business operations. As part of its vendor risk management, ASIC periodically assessed Gallagher's information security program, and requested and reviewed its SOC 1 audits. ASIC obligated Gallagher, by contract, to maintain appropriate physical, administrative and technical safeguards to prevent the unauthorized use or disclosure of personal information. Gallagher was also obligated by contract to notify ASIC as soon as practical of unauthorized access to unencrypted PII with respect to the services provided under the agreement.

ASIC first became aware of the Gallagher Security Incident shortly after it occurred in September 2020. It was not, however, until June 29, 2021, that Gallagher first informed ASIC that (1) certain personal information stored on Gallagher's internal

systems may have been affected, and (2) ASIC may have been one of Gallagher's many clients whose customers' data may have been affected. Following that notification, ASIC made repeated requests to Gallagher for additional information about its potentially impacted customers, and on October 19, 2021, Gallagher first confirmed that ASIC insured's claimants in the U.S. were affected and provided information on the number of ASIC's insured's claimants who may have been affected in the Incident and their state of residency. After receiving this new information, ASIC first determined that it would be required to notify your office about this Incident.

Upon receiving the list of potentially affected individual claimants from Gallagher, ASIC began diligently evaluating the list to confirm that they are associated with ASIC and evaluate its breach notification obligations. Gallagher stated in the Notice that it was not aware of any actual or attempted misuse of the affected data and ASIC has received no reports of identity theft or fraud from potentially affected individuals. ASIC does not believe it was targeted in the Incident affecting Gallagher's systems.

According to Gallagher and its external counsel, all of the potentially affected individuals have already been notified pursuant to applicable state laws via U.S. mail between August 17, 2021 and October 7, 2021. Additionally, according to the Notice, Gallagher has provided 24 months of free identity theft and credit monitoring services through Kroll to all of the potentially affected individuals.

Gallagher has represented to ASIC that, in response to the Incident, it enacted Gallagher's incident response plan and isolated impacted Gallagher systems, initiated business continuity plans, retained cybersecurity legal counsel, engaged with cybersecurity and forensic experts, deployed and monitored endpoint detection and response software, rotated passwords, and added additional email controls, among other improvements. Gallagher also stated it notified law enforcement of the Incident.

Although ASIC's systems were not impacted by Gallagher's Security Incident, ASIC is reviewing the relevant sections of its WISP, including the Incident Response Plan sub-section, for opportunities for improvement, and will make adjustments and updates as appropriate. ASIC is also assessing whether employees need additional training on overseeing vendor cybersecurity compliance and incident response.

ASIC takes the protection of personal information very seriously and is committed to answering any questions your office may have. Please do not hesitate to contact me at kbarrow@intactinsurance.com or 952-852-0478.

***

This letter contains ASIC's confidential and proprietary information, including concerning its security practices. In accordance with N.H. Rev. Stat. § 91-A:5(IV), N.H. Rev. Stat. § 91-A:5(XI), and/or other applicable laws and regulations, ASIC

requests that confidential treatment be provided to this letter and to any notes, memoranda, or other records created by or at the direction of the Office of the Attorney General, its officers, or staff members that reflect, refer to, or relate to this letter (the "Confidential Materials"). ASIC also requests that Confidential Materials be kept in a non-public file and that only staff of your Office have access to them. Should your Office receive any request for the Confidential Materials pursuant to N.H. Rev. Stat. § 91-A:4 or otherwise, ASIC requests that the undersigned be immediately notified of such request and be furnished a copy of all written materials pertaining to such request (including but not limited to the request and any determination relating thereto) and that ASIC be given an opportunity to object in advance to any such disclosure.

Should your Office be inclined to grant such a public records request, ASIC requests that it be given at least 10 business days' advance notice of any such decision to enable it to pursue any remedies that may be available to it. In such event, ASIC requests that you telephone and email me at 952-852-0478 or kbarrow@intactinsurance.com.

Sincerely,

Kara L.B. Barrow
Associate General Counsel, Corporate Legal

Enclosure

Gallagher

Insurance | Risk Management | Consulting

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Arthur J. Gallagher & Co. ("Gallagher") is an insurance broker and claims service provider offering services to its clients and business partners, and writes to notify you of an incident that may affect the privacy of some of your information. While we are unaware of any actual or attempted misuse of your information relating to this incident, we want to provide you with details regarding the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On September 26, 2020, Gallagher detected a ransomware event impacting our internal systems. We promptly took all our systems offline, including those at Gallagher Bassett, as a precautionary measure, initiated response protocols, launched an investigation with the assistance of third-party cybersecurity and forensic specialists, implemented our business continuity plans to minimize disruption to our customers, and ensured the ongoing security of our systems. We worked with the cybersecurity and forensic specialists to determine what may have happened and what information may have been affected. Our investigation determined that an unknown party accessed or acquired data contained within certain segments of our network between June 3, 2020 and September 26, 2020. While the investigation was able to confirm that certain systems were accessed, it was unable to confirm what information within those systems was actually accessed. Therefore, in an abundance of caution, Gallagher conducted an extensive review of the entire contents of the impacted systems. On May 24, 2021, Gallagher's investigation confirmed that the impacted data included information relating to certain individuals. Gallagher continued to work through June 23, 2021 to confirm the accuracy of the information so we could begin notifications to our business partners and to obtain address information for impacted individuals to provide accurate notice to impacted parties.

What Information Was Involved? Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification in an abundance of caution because certain information relating to you was accessed or acquired during this event. The impacted information relating to you includes your <<b2b_text_2(DataElements)>><<b2b_text_4(DataElementsCont)>>.

What Are We Doing. The privacy and security of information are among one of our highest priorities and Gallagher has strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to protect the privacy and security of client, partner, and employee information. We also reviewed existing security policies and implemented additional measures and enhanced security tools to further protect information in our systems. We also implemented additional safeguards and are providing additional training to our employees on data privacy and security. We reported this incident to law enforcement and regulatory authorities, as required by law.

In addition to providing notice of this event to you, we are also providing you access, at no cost, to identity and credit monitoring services for twenty-four (24) months through Kroll. Information and instructions on how to activate these complimentary services can be found in the "Steps You Can Take to Help Protect Your Information" attached to this letter.

What Can You Do. While Gallagher is unaware of any actual or attempted misuse of any information as a result of this incident, we nonetheless encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You may review the information contained in the attached "Steps You Can Take to Help Protect Your Information." You may also activate your access to the Kroll identity and credit monitoring services we are making available to you. There is no charge to you for the cost of these services; however, you will need to follow the instructions below in "Activate Identity Monitoring" section to activate your enrollment in this service.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-731-3320 (toll free), Monday through Friday (excluding U.S. holidays), 8:00 a.m. to 5:30 p.m., Central Time.

We sincerely regret any inconvenience this incident may cause you. Protecting information entrusted to Gallagher is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Arthur J. Gallagher & Co.

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **ajg.kroll.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_3(ActivationDeadline)>> to activate your identity monitoring services.

Your Identity Monitoring Services Include:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data – for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Accounts, Financial, and Medical Billing Statements

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement. Arthur J. Gallagher & Co. is located at 2850 W. Golf Rd., Rolling Meadows, IL 60008.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov. *For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. *For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. *For New York residents,* the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/. *For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-5-NO-SCAM, 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. *For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are # Rhode Island residents impacted by this incident.