21696

Appendix A
Company Letterhead

[First Name] [Last Name]
[Address Line 1] [Address Line 2]
[City] [State] [Zip]

[Date]

NOTICE OF DATA DISCLOSURE INCIDENT

Dear [First Name],

We are writing to let you know about a data disclosure incident which affected Assured Investment Management LLC ("AssuredIM") and its affiliate, Assured Investment Management (London) LLP ("AssuredIM London"), that involved your personal information.

WHAT HAPPENED?

AssuredIM London entered into an Office License Agreement with The Argyll Club Ltd. ("Argyll Club") for office space located at Octagon Point London for the period from March 23, 2020 to April 22, 2021. On April 21, 2021, AssuredIM's IT security team detected personal information in an email sent from Argyll Club to an Executive Assistant at AssuredIM London (the "Argyll Email"). The file attached to the email contained the name, date of birth, marital status, gender, ethnic group, social security number, home address, home phone, cell phone, office phone, work email, and personal email of 164 current and former employees of AssuredIM and AssuredIM London.

Following an internal investigation (which commenced promptly after receipt of the Argyll Email), AssuredIM's Senior HCM Business Partner contacted Argyll Club's Customer Relations Supervisor, on May 26, 2021 to inquire about the origin of the file attachment. Argyll Club responded on May 27, 2021, indicating that the original file containing the personal information was sent via email to Argyll Club by former management of the AssuredIM London office. AssuredIM's IT security team verified from internal email logs that the original file attachment was sent to Argyll Club on April 2, 2020 and again on April 7, 2020. The file was sent in response to a request from Argyll Club for the name, job title, business email, office phone, and cell phone of the AssuredIM London employees for use in procuring security passes allowing access to the London office building. The file contained 2 worksheets, one of which contained the limited information requested, and a second one, that was included inadvertently, that contained the more detailed list of personal information, regarding employees of AssuredIM and AssuredIM London. Argyll Club has represented to AssuredIM that all copies of the file containing your personal information (i) have been deleted and are no longer on their system; and (ii) were not shared with any third party, downloaded or printed.

WHAT INFORMATION WAS INVOLVED?

Based on our review of the file attachments, the data inadvertently shared with Argyll Club includes your name, date of birth, social security number, gender, home address, office phone, and work email. For certain employees, the data also included ethnic group, home phone, cell phone, and personal email.

WHAT WE ARE DOING?

We value your privacy and deeply regret that this incident occurred. We have conducted a thorough review of the potentially affected records and systems and are notifying you so that you can take steps to protect your information. We will notify you if we discover any significant developments. We have further implemented additional security measures and employee training designed to prevent a recurrence of such an attack. Our IT security team is working diligently to ensure the incident is properly addressed and to guard against future data exposures.

WHAT YOU CAN DO?

Please review the Steps You Can Take to Protect Your Information which is attached to this letter as Appendix A for additional information, including how to sign up to receive credit monitoring and identity theft protection services that we are offering at no charge to you.

For more information on identity theft, you can also visit the following websites:

Massachusetts Office of the Attorney General, Division of Criminal Justice at: https://www.mass.gov/protecting-yourself-if-your-identity-is-stolen.

Federal Trade Commission at: www.ftc.gov/bcp/edu/microsites/idtheft/

FOR MORE INFORMATION

For further information and assistance, please contact Dave Ray, Chief Compliance Officer, Assured Investment Management (212-905-5630 or dray@assuredim.com) Monday through Friday from 9am to 5pm EST.

Very truly yours,

Appendix A

Steps You Can Take to Protect Your Information

PROTECTION AGAINST ADDITIONAL FRAUDULENT ACTIVITY

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You have the right to obtain a copy of the Police Report(s) filed, if any, regarding the incident that resulted in disclosure of your personal information.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/index.action or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To

place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com.

- **Sign Up for Credit Monitoring and Identity Theft Protection Services**

We have engaged Allstate Identify Protection to provide you with credit monitoring and identity theft protection services for eighteen (18) months, at no cost to you. Please see the attached informational documents describing the services. You may access the website below to enroll for services. To take advantage of this offer, you must enroll within thirty (30) days from receipt of this letter. Once enrolled, Allstate Identity Protection will provide the services directly to you, subject to Allstate Identity Protection's Terms & Conditions, Privacy Policy and other applicable terms and disclosures (see links below provided by Allstate) and will bill AssuredIM for the cost of the services.

- Website: www.myaip.com/assuredguaranty
- Customer Service Number: (800) 789-2720
- Privacy Policy
- Terms & Conditions
- CCPA Policy

- **Review Additional Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877- ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

- **Consider a Credit Security Freeze**

In Massachusetts, you have the right to put a security freeze on your credit file free of charge. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, cell phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee to place, lift, or remove the security freeze. For more information on how to place a security freeze on credit reports in Massachusetts, please visit the Massachusetts Office of the Attorney General's brief available at: https://www.mass.gov/service-details/freeze-your-credit.