

March 24, 2024

Via E-mail (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of Barings LLC (“Barings” or the “Company”) to inform you about the nature and circumstances of a recent cybersecurity incident.

Newport Group Inc. (“Newport”) recently notified Barings LLC (“Barings”) that personal information of Barings deferred compensation plan participants and beneficiaries may have been affected by a ransomware incident involving one of Newport’s sub-processors, Infosys McCamish Systems LLC (“IMS”). Newport serves as a third-party recordkeeper for certain deferred compensation plans sponsored by Barings. The incident is not the result of an issue with Barings systems or a breach of Barings’ environment. The personal information that may have been affected included data such as name, contact information (such as postal and email address, and phone number), date of birth, Social Security number, employee ID and employment status. Not all of this information may have been impacted for each affected Barings plan participant or beneficiary.

Promptly after receiving the notification, Barings began coordinating with Newport to determine whether the incident had affected personal information related to Barings plan participants or their beneficiaries. Barings understands that the sub-processor, IMS, conducted a forensic investigation with assistance from cybersecurity experts and is continuing to analyze affected data to determine whether personal information related to Barings plan participants or their beneficiaries was affected by the incident. Nevertheless, Barings is planning to notify 8 Maryland residents who may have been affected by this issue and provide recommendations and steps they can take as precautionary measures to help protect their personal information.

The Company also has arranged to provide individuals whose Social Security numbers were potentially affected with identity protection and credit monitoring services for two years at no

Office of the Attorney General
March 24, 2024
Page 2

cost to them. Attached to this letter is a sample of a notice Barings is providing in connection with this incident.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

A handwritten signature in blue ink that reads "Lisa J. Sotto". The signature is written in a cursive, flowing style.

Lisa J. Sotto

Enclosure



Return Mail Processing
PO Box 999
Suwanee, GA 30024

10 1 1435 *****SINGLP

SAMPLE A. SAMPLE - A

C/O [Extra1]

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



March 25, 2024

NOTICE OF DATA BREACH

Dear **Sample A. Sample**,

Newport Group, Inc. ("Newport") serves as a third-party recordkeeper for certain deferred compensation plans sponsored by Barings LLC ("Barings"). We are writing to notify you of an issue that may involve certain of your personal information associated with a Barings deferred compensation plan.

What Happened?

We recently learned that Infosys McCamish Systems ("IMS"), a service provider that Newport uses to process transactions related to Barings deferred compensation plans, experienced a cybersecurity issue that impacted their systems. We understand that, on October 29, 2023, an unauthorized third party accessed some of IMS's systems and obtained certain IMS customer data. This may have included certain personal information of Barings plan participants and their beneficiaries. To date, Newport does not have evidence that personal information associated with a Barings plan participant or beneficiary was specifically affected in connection with this event.

What Information Was Involved?

The personal information that may have been affected included data such as your name, contact information (such as postal and email address, and phone number), date of birth, Social Security number, employee ID and employment status. Not all of this information may have been impacted for each affected Barings plan participant or beneficiary.

What We Are Doing

Promptly after learning of the issue, we began coordinating with IMS to determine whether the incident had affected personal information related to Barings plan participants or their beneficiaries. We understand that IMS conducted a forensic investigation with assistance from cybersecurity experts and is continuing to analyze affected data to determine whether personal information related to Barings plan participants or their beneficiaries was affected by the incident.

What You Can Do

We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect yourself. Steps you can take include the following:

- Register for Credit Monitoring Services. We have arranged to offer identity protection and credit monitoring services to potentially affected Barings plan participants and their beneficiaries for two years at no cost to them through Experian IdentityWorks. The attached Reference Guide provides information on how to register.
- Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.
- Review the Attached Reference Guide. The attached Reference Guide provides additional information and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

Other Important Information

Based on our investigation, we have no evidence at this time that the affected information has been used for fraud or identity theft.

For More Information

If you have any questions regarding this issue, please call 800-230-3950. We are available to assist you Monday – Friday, 8:00 AM - 8:00 PM ET.

We regret that this issue may affect you and we hope this information is useful to you.

Reference Guide

We encourage affected individuals to take the following steps:

Register for Identity Protection and Credit Monitoring Services. We have arranged with Experian to provide identity protection and credit monitoring services for two years at no cost to you. This offer is available to you for two years from the date of enrollment and requires an action on your part. Additional information, terms of this service, self-help tips, and information about identity protection are located at www.ExperianIDWorks.com/restoration.

To enroll in this service, please follow the steps below:

1. Ensure that you enroll by June 30, 2024
2. Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
3. Provide your activation code: **ABCDEFGHI**

If you have questions about Experian or IdentityWorks, or if you would like an alternative to enrolling in IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332. As proof of eligibility for this service, you will need to provide the engagement number, which is B118342.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755
(800) 788-9898
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)727-3400
www.oag.dc.gov

