DLA Piper LLP (US)
444 West Lake Street
Suite 900
Chicago, Illinois 60606-0089
www.dlapiper.com

Matthew Satchwell
matthew.satchwell@us.dlapiper.com
T 312.368.2111

July 8, 2022

VIA EMAIL: Idtheft@oag.state.md.us

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

Re: Security Incident Notification

Dear Attorney General Frosh:

We are providing notice on behalf of Ardagh Group ("Ardagh"), pursuant to Md. Code Com. Law §§ 14-3501 et seq., about an incident involving three (3) Maryland residents.

On May 2, 2021, Ardagh discovered that criminal actors encrypted portions of its network environment in Europe and the United States in a ransomware attack. Upon discovery of the incident, Ardagh took the impacted systems offline and launched an investigation with the assistance of leading cybersecurity experts. The unauthorized activity related to the ransomware incident occurred between April 23, 2021 and May 19, 2021.

In October 2021, Ardagh learned that a ransomware group posted links to data that it claimed to have stolen from Ardagh systems on a dark web site. In the ensuing time period, Ardagh has worked with outside cybersecurity experts to obtain copies of the posted data and to analyze its contents, specifically with the aim of identifying whether personal information was impacted. The servers used to post the data on the dark web have been offline since on or about November 16, 2021. The files containing Ardagh data are no longer available for download and may remain so. When the servers were online, they were unreliable and slow, which prolonged Ardagh's efforts to obtain a copy of the data even with the assistance of cybersecurity experts.

On June 22, 2022, Ardagh determined that personal information for three (3) Maryland residents was contained within the data files posted on the dark web site. Overall, Ardagh's analysis of the posted data to date has revealed very limited amounts of personal information interspersed throughout the large data set posted online, making the personal information difficult to locate even with Ardagh's knowledge of the dataset and powerful technological search tools. Aside from the act of posting the data on the dark web site, Ardagh's investigation has not revealed any evidence that this resident's data has been otherwise misused. Ardagh is undertaking ongoing monitoring of the dark web to identify if such attempts are made.

For most individuals, their names and Social Security Numbers were involved. For a small subset of individuals, the types of affected data varied by individual, but may have included one or more of the following data types: name, Social Security Number, driver's license number, passport number, other governmental identification number, birth certificate, financial account number, or work-related injury information.

In response to this incident, Ardagh immediately launched an investigation with the assistance of leading cybersecurity experts to secure each impacted system and has continued to monitor for suspicious activity. Ardagh also continues to enhance its security controls where appropriate and trains its workforce regarding cybersecurity issues. We are also regularly monitoring the dark web to identify any data taken from or relating to Ardagh.

Ardagh mailed written notice to the potentially affected Maryland residents on July 5, 2022, offering a 12-month subscription to IdentityWorks℠ credit monitoring and identity restoration services at no cost, through Experian. The IdentityWorks℠ services include: 12 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Enclosed is a copy of the text of this notification.

If you should have any questions or if we can provide further assistance to the Maryland residents affected by this incident, please feel free to contact me at (312) 368-2111 or matthew.satchwell@us.dlapiper.com.

Respectfully submitted,
DLA Piper LLP (US)

Matthew D Satchwell

Matthew Satchwell

An Attorney for Ardagh Group

Enclosure

ArdaghGroup

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

July 5, 2022

i0488-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY
qppssppprspppqpqsprssqrrqqprsrppppsrsqrqqsqrsrpqsqqppssppsssqrsqp

RE: Notice of Data [Extra1]

Dear Sample A. Sample:

We write to share important information with you about a data security incident that may have impacted your personal information. In an abundance of caution, we are providing you with this notice so that you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so. We regret that this incident occurred and take the security of your personal information seriously.

What Happened? We have conducted an investigation, with the assistance of leading cybersecurity experts, into a criminal cyberattack that targeted our systems. On May 2, 2021, Ardagh discovered that criminal actors encrypted portions of our network environment in Europe and the United States in a ransomware attack. Based on our investigation, we understand that the potential unauthorized activity occurred between April 23, 2021 and May 19, 2021.

In October 2021, we learned that a ransomware group posted links to data that it claimed to have stolen from Ardagh systems on a dark web site, which appears on a portion of the Internet that is only accessible by means of special software and knowledge. In the ensuing time period, Ardagh has worked with outside cybersecurity experts to obtain copies of the posted data and to analyze its contents, specifically with the aim of identifying whether personal information was impacted.

On June 22, 2022, we determined that your personal information was contained within the data files posted on the dark web site. Aside from the act of posting the data on the dark web site, our investigation has not revealed any evidence that your data has been otherwise misused. We are undertaking ongoing monitoring of the dark web to identify if such attempts are made.

There are some additional facts that we can provide to help you assess any risk to your information. First, the servers used to post the data on the dark web have been offline since on or about November 16, 2021. Thus, at this time, the files containing Ardagh data are no longer available for download and may remain so. Second, when the servers were online, they were unreliable and slow, which prolonged Ardagh's efforts to obtain a copy of the data even with the assistance of cybersecurity experts. Third, this dark web site was posted in an area of the internet that can only be accessed with specialized knowledge and software, making it unlikely that any personal data relating to you was readily accessible by the general public. Finally, very limited amounts of personal information were interspersed throughout the data set posted online, making the personal information difficult to locate even with Ardagh's knowledge of the dataset and powerful technological search tools.

Nonetheless, Ardagh takes this matter extremely seriously and wants to ensure that any risk to your information is being properly addressed.

What Information Was Involved? For most individuals, their names and Social Security Numbers were involved. For a small subset of individuals, the types of affected data varied by individual, but may have included one or more of the following data types: name, Social Security Number, driver's license number, passport number, other governmental identification number, birth certificate, financial account number, or work-related injury information.

What We Are Doing. Ardagh regularly reviews and updates the measures it takes to protect your personal information. We strive to continually improve our data security and maintain a secure environment for confidential and personal information.

In response to this incident, Ardagh immediately launched an investigation with the assistance of leading cybersecurity experts to secure each impacted system and has continued to monitor for suspicious activity. Ardagh also continues to enhance its security controls where appropriate and trains its workforce regarding cybersecurity issues. We are also regularly monitoring the dark web to identify any data taken from or relating to Ardagh.

As an added precaution, we are providing you with access to a complimentary ##-month membership of Experian's® IdentityWorksSM. 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**: **September 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

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 1-877-890-9332 by September 30, 2022. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR Coverage_Length-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 agents 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. 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 (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 this Identity Restoration support is available to you for Coverage_Length 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. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-833-737-0006.

Sincerely,

Joshua Markus
General Counsel Ardagh North America

Steps You Can Take to Protect Against Identity Theft and Fraud

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
800-349-9960	888-397-3742	888-909-8872

Websites:
www.equifax.com/personal/credit-report-services/credit-freeze
www.experian.com/freeze/center.html
www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of Birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.

District of Columbia 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
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
https://oag.dc.gov/

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

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

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 agencies 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 a 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

0000001

Act. You can 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.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.