Frost Brown Todd LLC
ATTORNEYS

Michael E. Nitardy
Member
859.817.5914 (t)
859.283.5902 (f)
mnitardy@fbtlaw.com

July 5, 2022

VIA OVERNIGHT MAIL

New Hampshire Attorney General's Office
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Incident

Dear Sir or Madam:

We represent Prysmian Cables and Systems USA, LLC d/b/a Prysmian Group located at 4 Tesseneer Road, Highland Heights, KY 41076. We are writing to notify your office of an incident that may affect the security of some personal information relating to approximately five of your residents.

Nature of the Data Event

As part of providing benefits to its employees, Prysmian has used Aon PLC ("Aon") as a broker for insurance services. On February 25, 2022, Aon identified a cyber incident that, upon investigation, impacted a limited number of its systems. According to Aon, it immediately retained leading cybersecurity firms to assist in responding and to help conduct a thorough investigation of the incident.

This May, Aon completed its investigation, and at that time, informed Prysmian of the incident. Since being informed of the incident, Prysmian has worked diligently to confirm the incident as reported to it by Aon and to confirm the identifies of the individuals impacted by the incident for notification purposes. Aon's investigation revealed that an unauthorized third party first accessed certain Aon systems beginning on or around December 29, 2020 through the use of a "zero-day" vulnerability. The access continued until February 25, 2022. Findings from Aon's investigation indicate the unauthorized third party temporarily obtained certain documents containing personal information from Aon systems during this period. Aon indicates that it 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. Aon has stated it has no reason to believe the information accessed as part of the incident has been misused.

What Information Was Involved?

Aon's review of the data determined some of the information obtained in the incident contained personal information, including name, social security number, email address, date of birth, and carrier and health plan level information. A total of 564 current or former Prysmian employees will be notified as a result of the incident.

Notice to Residents

After being notified of the incident and receiving information about the individuals potentially impacted by the incident, Prysmian conducted its own review of the information to confirm the individuals that should be notified as a result of the incident. In addition to notifying the appropriate authorities, on

July 5, 2022, Prysmian will send written notice of the event to the affected individuals. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit 1***.

Other Steps Taken and To Be Taken

Aon informed Prysmian that it immediately reported the incident to, and is working closely with, the FBI. Upon learning of the incident, Prysmian immediately took steps to investigate the event and to work with Aon in determining the notifications to be made. Through Aon, impacted individuals are also being provided access to complimentary credit monitoring services for 24 months, through Experian.

Prysmian is undertaking a review of its processes for sharing employee information with its vendors in order to assure the information's security. Additionally, Prysmian's notification to the affected individuals provides guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. The notification also provides individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, Prysmian does not waive any rights or defenses regarding the applicability of law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification, or other aspects of the data security event, please contact us at (859) 817-5914.

Very truly yours,

FROST BROWN TODD LLC

Michael E. Nitardy

Prysmian Group

Linking the Future

[First Name] [Last Name]
[Address #1]
[Address #2]
[City, State Zip Code]

June __, 2022

RE: Notice of Data Breach

Dear [INSERT NAME]:

Prysmian Group North America ("Prysmian") is writing to notify you of a recent event involving one of our third-party insurance benefits brokers that may involve some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened?

As part of providing benefits to our employees, Prysmian has used Aon PLC ("Aon") as a broker for insurance services. On February 25, 2022, Aon identified a cyber incident that, upon investigation, impacted a limited number of its systems. Once the incident was discovered, Aon immediately retained leading cybersecurity firms to assist in responding and to help conduct a thorough investigation of the incident.

This May, Aon completed its investigation, and at that time, informed us of the incident. Since being informed of the incident, we have worked diligently to confirm the incident as reported to us by Aon and to confirm the identifies of the individuals impacted by the incident for notification purposes. Aon's investigation revealed that an unauthorized third party accessed certain Aon systems at various times between December 29, 2020 and February 25, 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's review of the data determined some of the information obtained in the incident contained some of your personal information, including your name and one or more of the following: social security number, email address, date of birth, and benefit carrier and health plan level.

What We Are Doing.

The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event and to work with Aon in providing proper notifications. We are reviewing our processes for sharing employee information with our vendors to assure the information's security. In addition, Aon informed us that it immediately reported the incident to, and is working closely with, law enforcement authorities, including the FBI.

Prysmian Group North America
4 Tesseneer Dr,
Highland Heights KY 41076
Tel. +1 859-572-8000
na.prysmiangroup.com

Prysmian Group

Linking the Future

What You Can Do.

You can remain vigilant by monitoring your account statements and free credit reports for any indications of fraud or identity theft. Please review the enclosed "Steps You Can Take to Help Protect Your Information," which contains information on what you can do to safeguard against possible misuse of your information should feel it appropriate to do so.

As an added precaution, to help protect your personal information, you are being offered a complimentary 24 month membership of Experian's® IdentityWorks℠. 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: https://www.experianidworks.com/credit
- Provide your activation code: CODE

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.** Be prepared to provide engagement number 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 to inquire about the personal information we maintain about you, or if you have any questions or need additional information, please contact Ann Maier, NA Benefits and Retirement Sr. Manager, at 4 Tesseneer Drive, Highland Heights, KY 41076 or Ann.Maier@prysmiangroup.com.

Sincerely.

John Andrews
Vice President of Human Resources
Prysmian Group NA

Prysmian Group North America
4 Tesseneer Dr,
Highland Heights KY 41076
Tel. +1 859-572-8000
na.prysmiangroup.com

Prysmian Group

Linking the Future

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll In Credit Monitoring

Please see instructions above on how to enroll.

Monitor Your Accounts

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 one-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, 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.

Prysmian Group North America
4 Tesseneer Dr,
Highland Heights KY 41076
Tel. +1 859-572-8000
na.prysmiangroup.com

Prysmian Group

Linking the Future

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 2002, 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.

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 North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For *Oregon residents*, the Oregon Attorney general may be contacted at: 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and www.doj.state.or.us.

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 6 known Rhode Island residents impacted by this incident.

Prysmian Group North America
4 Tesseneer Dr,
Highland Heights KY 41076
Tel. +1 859-572-8000
na.prysmiangroup.com