29395

uponor

<<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 Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing on behalf of Uponor North America to follow up on an incident that may have involved your personal information. This letter provides you with information about the nature of the incident and affected data, and immediate and additional measures Uponor has taken to guard against future unauthorized disclosure or misuse of your personal data.

What Happened?

On November 5, 2022, Uponor experienced a security incident which rendered some North American operations inoperable. Uponor immediately took steps to contain the incident and retained global cybersecurity professionals to conduct an extensive investigation of the incident. Based on that investigation, forensic evidence indicated that, just prior to the incident, there were exports of data to an external cloud storage platform by an unauthorized party. We initially believed these exports primarily affected Uponor business documents but later discovered that exports contained personnel files with information about current and former employees and their dependents or beneficiaries. In mid-February 2023, we learned the threat actor had begun to post the exported data on its internet site.

What Information Was Involved?

Potentially exposed records included the name, social security number, and date of birth of a current or former employee and their dependents or beneficiaries. We believe exposed current or former employee data also included basic payroll information such as a person's job title, benefits, paycheck information and deductions, but no banking information was impacted.

What We Are Doing

We take the security of your personal information seriously. Therefore, upon discovering the incident, Uponor immediately took its data centers offline and shut off all factory and internet connections to help contain the incident. We identified and removed malicious files, reset administrative and employee credentials, and rebuilt and recovered systems from known clean backups. We also enhanced our monitoring, logging, and detection capabilities, and retrained staff on cybersecurity.

We retained global security professionals to conduct an independent investigation and assist with our recovery efforts. After several weeks of investigation, they were able to produce a listing of affected directories, which our professionals and outside counsel then used to harvest and review restored files for potentially affected personal information.

Finally, to help relieve any concerns, we also secured the services of Allstate Identity Protection to provide identity monitoring for two years at no cost to you. Allstate is a global leader in identity protection, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your Allstate identity monitoring services include Tri-Bureau credit monitoring, an annual Tri-Bureau credit report and score, unlimited TransUnion reports and scores, TransUnion credit lock, assistance with credit freezes, Allstate Security Pro for real-time emerging threat alerts, Allstate Digital Footprint for privacy management, Dark Web Monitoring, 24/7 customer care, and up to $1 million in identity theft expense reimbursement.

What You Can Do

If you would like to activate your identity monitoring services, please follow the instructions in the section below titled *Activating Your Complimentary Identity Monitoring*. As always, please continue to be vigilant about the security of your personal accounts and monitor them for unauthorized activity. Please report any suspicious activity to appropriate law enforcement.

For More Information

Again, we take the security of your information seriously and regret any concerns or inconvenience this incident may have caused. Please review the enclosed attachment called *Preventing Identity Theft and Fraud* for more information about how to protect your personal data. If you have any questions, please contact us toll-free at 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Erica Amevo

Erica Amevo
Vice President of Human Resources

ACTIVATING YOUR COMPLIMENTARY IDENTITY MONITORING

Visit www.MyAIP.com/ProtectUponor to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Click on "enroll now" and enter Activation Code **<<Activation Code s_n>>** and your name. Then click "Next."

For more information about Allstate and your Identity Monitoring services, you can email Allstate at clientservices@aip.com. They are available 24 hours a day, 7 days a week, to ensure that you have help when you need it most. Additional information describing your services is included with this letter.

Allstate IDENTITY PROTECTION

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Allstate Identity Protection Pro +

Triple Bureau Annual Report and Score and Unlimited TransUnion Reports and Scores

Your current credit report is available for you to review. You have unlimited access to TransUnion credit reports and scores. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance when a new line of credit is applied for in your name. If you do not recognize the activity, you can call an Allstate Security Pro, who can help you determine if it indicates identity theft. With Allstate Identity Protection Pro +, you also have high-risk and financial transaction monitoring.

Dark Web Monitoring

When a breach occurs, we're consistently the first to detect victims' personal information on the dark web. We have access to cybercrime marketplaces in the most hidden parts of the internet, and we can alert you to compromised information weeks or even months before a breach is made public.

Social Media Monitoring

Social media monitoring keeps an eye out for signs of account takeover or potentially inappropriate comments within your social media accounts.

Real-time emerging threat alerts

Allstate Security Pro5M delivers real-time, personalized emerging threat and scam alerts. Additionally, Allstate Pro + allows access to Allstate's Digital Footprint, Allstate's unique tool for seeing and managing personal data.

$1 Million Identity Fraud Loss Reimbursement

Coverage includes up to $1 million in reimbursement for stolen funds, fraudulent 401(k) and HSA withdrawals, and expenses resulting from home title fraud and professional fraud.

Preventing 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. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office, or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and also to access some services that are free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this letter and at www.identitytheft.gov/#/Know-Your-Rights. For example, 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.

In addition, at no charge, you can have these credit bureaus place a short-term or an extended "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 a fraud alert 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. If you wish to place a fraud alert or have any questions regarding your credit report, please contact any one of the agencies listed below. Please note: no one is allowed to place a fraud alert on your credit report except you.

General contact information for each agency:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016-2000
1-866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

To add a fraud alert:

Equifax	(888) 202-4025, Option 6 or	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	(714) 830-7000, Option 2 or	https://www.experian.com/fraud/center.html
TransUnion	(800) 916-8800, Option 0 or	https://www.transunion.com/fraud-alerts

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit 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. Unlike a fraud alert, you must separately place a security freeze on your credit file at each bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-888-298-0045. P.O. Box 1057881, Atlanta, GA 30348-0241. www.equifax.com/personal/credit-report-services/credit-freeze;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016-2000. www.transunion.com/credit-freeze

The Federal Trade Commission also provides additional information about credit freezes here: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or another statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who

discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement or your state Attorney General as well.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov **or** www.ftc.gov

OTHER IMPORTANT INFORMATION

You may file a report with your local police or the police in the community where the identity theft took place. You are entitled to request a copy of your police report filed in that matter.

California residents:
Visit the California Attorney General's site (www.oag.ca.gov/idtheft) for additional information on protection against identity theft

Iowa residents:
You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

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

Maryland residents:
You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General, 200 St. Paul Place Baltimore, MD 21202; phone: 1-888-743-0023; www.marylandattorneygeneral.gov.

New Mexico residents:
The Fair Credit Reporting Act (FCRA) provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, be told if information in your credit file has been used against you, and seek damages from violators. You may have additional rights under the FCRA not summarized here, and identity theft victims and active duty military personnel have specific additional rights pursuant to the FCRA. You can review these rights by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York residents:
The Office of the Attorney General may be reached at The Capitol, Albany, NY 12224-0341; phone: 1-800-771-7755; ag.ny.gov.

North Carolina residents:
You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001; phone: 919-716-6400; ncdoj.gov.

Oregon residents:
You may obtain information about avoiding identity theft at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; phone: 1-877-877-9392; www.doj.state.or.us/.

Washington D.C. residents:
You may obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001; phone: 202-727-3400; https://oag.dc.gov/.

Colorado, Georgia, Maryland, Massachusetts, and New Jersey residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).