



Baker & McKenzie LLP

300 East Randolph Street, Suite 5000  
Chicago, IL 60601  
United States

Tel: +1 312 861 8000  
Fax: +1 312 861 2899  
www.bakermckenzie.com

**Asia Pacific**

Bangkok  
Beijing  
Hanoi  
Ho Chi Minh City  
Hong Kong  
Jakarta\*  
Kuala Lumpur\*  
Manila\*  
Melbourne  
Seoul  
Shanghai  
Singapore  
Sydney  
Taipei  
Tokyo

**Europe, Middle East  
& Africa**

Abu Dhabi  
Almaty  
Amsterdam  
Antwerp  
Bahrain  
Baku  
Barcelona  
Berlin  
Brussels  
Budapest  
Cairo  
Casablanca  
Doha  
Dubai  
Dusseldorf  
Frankfurt/Main  
Geneva  
Istanbul  
Johannesburg  
Kyiv  
London  
Luxembourg  
Madrid  
Milan  
Moscow  
Munich  
Paris  
Prague  
Riyadh  
Rome  
St. Petersburg  
Stockholm  
Vienna  
Warsaw  
Zurich

**Latin America**

Bogota  
Brasilia\*  
Buenos Aires  
Caracas  
Guadalajara  
Juarez  
Lima  
Mexico City  
Monterrey  
Porto Alegre\*  
Rio de Janeiro\*  
Santiago  
Sao Paulo\*  
Tijuana  
Valencia

**North America**

Chicago  
Dallas  
Houston  
Miami  
New York  
Palo Alto  
San Francisco

August 21, 2023

**VIA EMAIL**

New Hampshire Attorney General  
attorneygeneral@doj.nh.gov

**RE: Data Breach Reporting**

Dear New Hampshire Attorney General:

I am writing on behalf of Avient Corporation (“Avient”) to notify you of a data incident. On April 9, 2023, Avient detected and responded to a suspected security event and ransomware infection within its network infrastructure. Upon learning of this incident, Avient immediately initiated an investigation to determine the scope of the incident. The investigation determined that compromised credentials were used to access Avient's Citrix environment. While in the environment, the unauthorized actor successfully transferred less than one (1) terabyte of data out of the Avient environment. The exfiltrated data included low-volume and limited personal information of current and prior Avient employees and contingent workers. In addition, Avient determined that there was no permanent loss of relevant personal data during the incident.

Avient is taking steps to protect the affected individuals following this incident. Following a thorough investigation with the assistance of its third-party partners, Avient confirmed that personal information relating to approximately 1,406 individuals worldwide was included in the files that were taken by the threat actor, approximately 1 of whom is a New Hampshire resident. The potentially-impacted personal information for some individuals included

Avient is providing notice to all potentially-affected individuals. Notice to these individuals who are residents of New Hampshire will be sent on or about August 22, 2023 by postal mail. A copy of this notice is attached. These individuals are also being provided of credit monitoring services through Kroll, at no cost to them.

Please feel free to contact me with any questions at  
or

Best regards,

Brian Hengesbaugh



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

### **Notice of Data Breach**

Dear <<First\_Name>> <<Last\_Name>>,

Avient Corporation, formerly known as PolyOne ("Avient") understands the importance of protecting information and your privacy is important to us. We recently had a cyber security incident that has affected some of your personal information. This notice explains the incident, measures we have taken, and steps you can take as well.

#### **WHAT HAPPENED**

On or around April 9, 2023, Avient experienced a disruption to its IT systems which was determined to be caused by a cyber security incident that impacted some of our servers and workstations. As soon as we became aware of the incident, we immediately took steps to protect potentially impacted individuals and our systems. We initiated an investigation to determine the scope of the incident and to confirm the restoration of the security and integrity of the servers and workstations. We also immediately engaged leading third-party cybersecurity forensics firms.

#### **WHAT INFORMATION WAS INVOLVED**

On or about July 6, 2023, we determined that certain personal information about you was stored on the impacted servers. This includes information such as <<b2b\_text\_1 ("your" data elements)>>. At this point, we do not believe that your information has been used to commit identity theft, although we encourage you to remain vigilant regarding protection from such potential risks, including by considering the identity monitoring services we offer below.

#### **WHAT WE ARE DOING**

We worked quickly and diligently to investigate and contain the incident, and to prevent this type of incident in the future. In response to this incident, we voluntarily and temporarily restricted access to select systems as a precautionary measure until we confirmed they were safe to use. We increased our data security measures through implementation of additional security monitoring tools, ensuring associate password resets, and implementing additional multi-factor authentication measures on specific systems. To further protect personal information, we have plans to implement additional data security measures and additional training of associates for continued awareness of these types of incidents. We continue to work closely with our external industry-leading service providers to implement additional incremental security measures to protect our systems, and to help us defend against this type of unlawful activity in the future.

As a precautionary measure, we have purchased identity monitoring services for you through Kroll, a leading data breach resolution services expert. This complimentary membership to Kroll's credit and identity monitoring services is completely free to you and will not affect your credit score. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s\_n>>

**WHAT YOU CAN DO**

We encourage you to enroll in the identity monitoring services. If you choose to enroll, this service will be available to you for two years (24 months) from the date of enrollment.

In addition, we encourage you to be especially aware of email, telephone, and postal mail scams that ask for your personal or sensitive information. Avient will never contact you in any way, including by email, asking for your social security number, payroll banking information, or any other sensitive information about you. If you are ever asked for this information, you can be confident Avient is not the entity asking. Avient encourages you to remain vigilant, review your account statements, and monitor your credit reports closely.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. If you have additional questions, please call our dedicated call center directly at (866) 676-6018 between 8:00 am and 5:30 pm CT, Monday through Friday, excluding major US holidays.

Sincerely,

Kristen Gajewski  
Chief Human Resources Officer  
Avient Corporation



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ADDITIONAL STEPS YOU CAN TAKE

Avient is providing the following additional information for those U.S. residents who wish to consider it:

- **[For Connecticut residents]:** the Connecticut Attorney General may be contacted at: 165 Capitol Avenue, Hartford, CT 06106; 860-808-5318; and [Attorney.General@ct.gov](mailto:Attorney.General@ct.gov).
- **[For District of Columbia residents]:** the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).
- **[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.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).
- **[For Massachusetts residents]:** the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)
- **[For New York state residents]:** the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.
- **[For North Carolina residents]:** the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566- 7226.

You may wish to visit the website of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.

You may have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free 877-322-8228.

You can request information regarding “fraud alerts” and “security freezes” from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can 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. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may 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. A “security freeze” generally prohibits the credit reporting agency from releasing your credit report or any information from it without your

written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: (1) *name*; (2) *Social Security number*; (3) *date of birth*; (4) *current address*; (5) *addresses over the past five years*; (6) *proof of current address*; (7) *copy of government identification*; and (8) *any police/investigative report or complaint*. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

- Experian: 888-397-3742; <https://www.experian.com/help/>; P.O. Box 9554, Allen, TX 75013
- Equifax: 800-525-6285; <https://www.equifax.com/personal/credit-report-services/>; P.O. Box 105788, Atlanta, GA 30348
- TransUnion: 800-680-7289; <https://www.transunion.com/credit-help/>; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

Please note that although Avient is offering to provide the Kroll Identity product at no charge to you for 24 months, the consumer reporting agencies listed above may require fees for their services.