Morgan Lewis

RECEIVED

JUN 28 2021

CONSUMER PROTECTION

Ezra D. Church
Partner
215.963.5710
ezra.church@morganlewis.com

VIA FIRST CLASS MAIL

June 25, 2021

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notification of Information Security Incident Involving 130 New Hampshire Residents*

Dear Office of the Attorney General:

This Firm represents Brenntag North America, Inc. ("Brenntag") in connection with a recent information security incident which involved a ransomware attack.

As soon as we learned of the incident on April 28, 2021, out of an abundance of caution, Brenntag disconnected affected systems from the network to contain the threat. In addition, third-party cybersecurity forensic experts were immediately engaged to help investigate and law enforcement and CISA were informed. Since learning of this situation, Brenntag has been taking steps to further protect and strengthen the security of its systems.

Our investigation confirmed that Brenntag systems were accessed without authorization starting on April 26, 2021, and/or that some information was taken from our system. On May 27, 2021, we first confirmed that some personal information was present in the information removed from Brenntag's network by the threat actor. Based on the evidence to date, we believe the impact of this incident was limited, and Brenntag has not received any reports of improper use of the affected individuals' personal information. Brenntag's investigation concluded that information taken from its system by the threat actor likely contained personal information of 130 New Hampshire residents, potentially including name, address, date of birth, social security number, select medical information, and/or driver's license number. Brenntag is notifying all 130 residents and offering a one-year complimentary subscription of Experian's credit monitoring services.

Further information about what Brenntag has done and what it is recommending to the individuals in question can be found in the enclosed notification letter that Brenntag sent on June 25, 2021, via U.S. Mail to the New Hampshire residents whose personal information was likely contained in the information taken by the threat actor.

If you have any questions, please feel free to contact me.

Sincerely,

/s/ Ezra D. Church

Ezra D. Church

ConnectingChemistry

BRENNTAG

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

June 25, 2021

G5559-L03-0000002 T00001 P001 *****AUTO**MIXED AADC 159
SAMPLE A. SAMPLE - L03 US&CANADA
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Re: Notice of Information Security Incident

Dear Sample A. Sample:

At Brenntag North America, Inc., we take the privacy and security of your personal information very seriously. We are writing to tell you about a recent information security incident that may have exposed some of your personal information. While we have no reason to believe that this information has been used for any fraudulent purpose as a result of this incident, we are sharing details about what happened, what information was involved, what we are doing to address it, the steps you can take, and resources that we are making available to you.

What Happened?

On April 28, 2021, we became aware of an information security incident impacting certain of our computer systems. As soon as we learned of the incident, out of an abundance of caution, we disconnected affected systems from the network to contain the threat. In addition, third-party cybersecurity forensic experts were immediately engaged to help investigate and law enforcement was informed. Since learning of this situation, we have been taking steps to further protect and strengthen the security of our systems.

Our investigation confirmed that Brenntag systems were accessed without authorization starting on April 26, 2021, and/or that some information was taken from our system. There is no evidence that any information was misused for fraudulent purposes as a result of this incident.

What Information Was Involved?

We have confirmed that the information taken may include your social security number, date of birth, driver's license number, and select medical information.

What We Are Doing

As soon as we discovered the incident, we took the steps previously described. We have also taken steps to increase the security of our systems and will continue to evaluate other measures to strengthen our cybersecurity defenses. In addition, we are offering information in the reference guide below about steps you can take to help protect your personal information. We are also making resources available to you. We have established a dedicated call center to provide information and direct you to resources that are available.

To help protect your identity, we are offering a complimentary EXTRA1 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, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

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 (833) 796-8640 by **September 30, 2021**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXTRA1 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.

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 (833) 796-8640. 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 EXTRA1 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.

What You Can Do

We recommend that you review the guidance provided in the enclosed reference guide about how to help protect your information. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports. If you find any transactions you do not recognize, contact the business or institution issuing the statement. We also recommend that you enroll in the complimentary credit monitoring that we are offering.

* 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.

For More Information

If you have questions or need assistance, please call (833) 796-8640 Monday thru Friday from 6 a.m. to 8 p.m. and Saturday and Sunday from 8 a.m. to 5 p.m. PST.

* * *

Please know that we take this matter very seriously and we apologize for any concern and inconvenience this may cause you.

Sincerely,

Scott Leibowitz
Regional President
Brenntag Essentials North America

Lars Schneider
Regional President
Brenntag Specialties Americas

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place 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 a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

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, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- 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 learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.