[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

From: Brake, Kacy <Kacy.Brake@GAPAC.com>
Sent: Friday, February 5, 2021 11:24 AM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: Notice of Data Security Incident

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

February 5, 2021

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Dear Attorney General MacDonald:

Pursuant to New Hampshire Section 359-C:19, we are writing to notify you of a breach of security/an unauthorized access or use of personal information involving 2 New Hampshire residents.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Koch Industries, Inc. and its affiliates ("Koch") recently became aware of email phishing activity that reached Koch employees' inbox. Several of those employees' credentials were compromised. By leveraging the compromised credentials, an unauthorized party gained access to these employees' email mailbox for a limited period of time. Based on our investigation, this unauthorized access occurred on January 8, 2021 until at the latest January 12, 2021. The personal information involved in the issue was names and social security numbers. Upon detecting the unauthorized access, Koch Cybersecurity quickly expelled the unauthorized party from further accessing the compromised mailboxes on the Koch network, and ensured the bad actor could not continue to reenter our environment via the attack method used.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The breach involved 2 New Hampshire residents who will be notified via U.S. Mail on February 8, 2021. A copy of the notice is attached.

STEPS TAKEN RELATING TO THE INCIDENT

Koch has arranged for identity protection and credit monitoring services to those impacted for one year at no cost through Experian's® IdentityWorksSM. This product provides identity detection and resolution of identity theft.
As part of our ongoing efforts to help prevent something like this from happening in the future, Koch has taken several steps, including:

- Resetting all affected passwords
- Forced re-authentication of all affected user accounts
- Reconfirming triggers for multi-factor authentication
- New security alerts around legacy email protocols

Please do not hesitate to contact me if you have any questions

Sincerely,

Kacy Brake
Associate General Counsel - Global Privacy

Koch Companies Public Sector
133 Peachtree Street
Atlanta, Georgia 30303
(404) 652-4508
kacy.brake@gapac.com

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

February 8, 2021

G1958-L01-0000001 T00001 P001 **********MIXED AADC 159
SAMPLE A SAMPLE - L01
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A Sample,

Koch Industries, Inc. and its affiliates ("Koch") take the protection and proper use of your personal information very seriously. We are therefore contacting you to explain a recent incident that involves certain personal information and to provide you with steps you can take to protect yourself.

What Happened

Koch, like many companies today, is a target of phishing emails. Despite best efforts at identifying and preventing these emails from reaching employee inboxes, cybercriminals in this space are sophisticated. We recently became aware of email phishing activity that reached Koch employees' inbox, and several of those employees' credentials were compromised. By leveraging the compromised credentials, an unauthorized party gained access to these employees' email mailbox for a limited period of time.

Upon detecting the unauthorized access, Koch Cybersecurity quickly expelled the unauthorized party from further accessing the compromised mailboxes on the Koch network. However, prior to locking out the unauthorized party, the unauthorized party removed a copy of the compromised employees' email mailbox, which included file(s) that contained your personal information. Based on our investigation, this unauthorized accessed occurred on January 8, 2021 until at the latest January 12, 2021.

What Information Was Involved

The information that was taken, and that the unauthorized party may have viewed, contained your name [Extra1] The employees whose email mailbox was compromised are in HR and Payment Processing related roles and, as such, have access to such information as part of their job responsibilities.

What We Are Doing

We are notifying you so that you can take action to protect yourself. Ensuring the safety of our [Extra2] is of the utmost importance to us. As part of our ongoing efforts to help prevent something like this from happening in the future, Koch has implemented several changes, including:

- Resetting all affected passwords
- Forced re-authentication of all affected user accounts
- Reviewed email configuration and blocked legacy email protocols where not explicitly required
- Reconfirming that connections to email boxes trigger multi-factor authentication
- New security alerts around legacy email protocols

What You Can Do

We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect yourself. Steps you can take include the following:

- Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

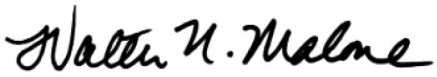
- Register for Credit Monitoring Services. We have arranged to offer identity protection and credit monitoring services to you for **one year** at no cost to you. The attached Reference Guide provides additional information about enrollment.

- Review the Attached Reference Guide. The attached Reference Guide provides information on registration for identity protection services and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We sincerely apologize for this incident at Koch and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us directly at: (316) 828-4616 or privacyoffice@kochind.com.

Sincerely,



Walt Malone
Vice President Human Resources
Koch Industries, Inc.

4111 E 37th St N
Wichita, KS 67220
PO Box 2256
Wichita, KS 67201-2256

Reference Guide

We encourage affected individuals to take the following steps:

Register for Identity Protection and Credit Monitoring Services. To help protect your identity, we are offering a complimentary one-year 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**: **4/30/2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **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 toll-free at **877-890-9332** by **4/30/2021**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

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 **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 one year 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.

* 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.

4111 E 37th St N
Wichita, KS 67220
PO Box 2256
Wichita, KS 67201-2256

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- 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 contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing 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 the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/internet/resource-center

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us