

Office of the Attorney General of Maryland
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Dear Sir or Madam:

We represent North Pacific Paper Company, 3001 Industrial Way, P.O. Box 2069, Longview, WA 98632 ("NORPAC"). Pursuant to Md. Code, Com. Law § 14-3504, we write to notify you of an incident that affects the security of information relating to one (1) Maryland resident. At this point, we are not aware of any harm arising from the incident. By providing this notice, NORPAC does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Our review indicates that on or around September 28, 2022, NORPAC experienced a cyberattack on its network. Upon discovering the attack on September 29, 2022, the company took immediate action, engaging external experts to address the incident and deploying enhanced 24x7 monitoring and detection technologies to its network environment.

It appears that data belonging to one NORPAC employee in Maryland was exfiltrated from NORPAC's network. The impacted data contained names, birthdates, driver's license numbers, social security numbers, and medical information.

Given the nature of the incident, NORPAC employees were almost immediately aware of it, and notice is being mailed to the affected Maryland resident concurrently with this letter.

Based on our ongoing analysis and investigation, NORPAC believes that the risk of harm to the affected individuals is low. Nonetheless, and out of an abundance of caution, NORPAC is providing notice of the incident and one year of credit monitoring to affected employees. Enclosed you will find a sample of the notice letters.

NORPAC is implementing additional safeguards to ensure information in its control is appropriately protected.

For further information, please do not hesitate to contact me.

Sincerely,



Timothy A. Newman
timothy.newman@haynesboone.com
Direct Dial 214-651-5029

Haynes and Boone, LLP

2323 Victory Avenue | Suite 700 | Dallas, TX 75219
T: 214.651.5000 | haynesboone.com

October 18, 2022

[Name]
[Address]

Notice of Data Security Incident

Dear [Name]:

We deeply value the relationship we have with our employees, and we are writing to make you aware of an incident that may have impacted your personal information. At this point, we are unaware of any harm arising from the incident.

1. What happened and what information was involved:

Our review indicates that on or around September 28, 2022, we experienced a cyberattack on our network. Upon discovering the attack on September 29, 2022, we took immediate action, engaging external experts to address the incident and deploying enhanced 24x7 monitoring and detection technologies to our network environment.

We have reviewed the data that we believe was copied from our network, which contained names, birthdates, driver's license numbers, social security numbers, and medical information.

2. What we are doing:

Given the nature of this attack and based on our ongoing review, we believe the risk of harm to you is low. Nonetheless, and out of an abundance of caution, we wanted to notify you of the incident so that you can take any necessary precautions.

Although NORPAC is unaware of any misuse of your information, we are enrolling you and your dependents in LifeLock for one year at no cost to you to ensure the security of your information. If you do not wish to be enrolled in LifeLock, contact any member of the NORPAC HR team and we'll cancel the LifeLock subscription.

Please understand that we take this incident very seriously and apologize for any inconvenience it may have caused. We are implementing additional safeguards to ensure our information is appropriately protected. We are singularly focused on protecting our employees' interests.

3. For more information:

If you have questions that are not addressed in this letter, please call Eddie Martin at 360-636-6444. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,



Craig Anneberg
Chief Executive Officer

Reference Guide

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-888-4213
www.transunion.com

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: At no charge, you can also 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 can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) social security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Additional Information: You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, <https://ncdoj.gov/>, 919-716-6000.