Warner Norcross + Judd LLP

February 8, 2024

Via Email

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: **Notice of Data Event**

To Whom It May Concern:

We represent National Nail Corp., which recently suffered a data breach, and are notifying you pursuant to New Hampshire law of an incident that may affect the security of certain personal information of three New Hampshire residents. We have also attached a sample of the notification that will be sent to New Hampshire residents as ***Exhibit A***. By providing this notice, National Nail Corp. does not waive any rights or defenses regarding the applicability of New Hampshire Law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Brief description of the nature of the breach:

In mid-November 2023, National Nail's computer systems were breached by an unauthorized outside party in a ransomware attack exploiting a vulnerability in third-party software. This breach caused an outage of computer systems, phones, email, and the encryption of work documents. An external party was immediately engaged and recently completed a forensic analysis. These experts determined that the threat actors exfiltrated work documents from National Nail's computer systems. On December 19, 2023, National Nail discovered that personal information had in fact been accessed and had been leaked onto the dark web. National Nail's payroll and accounting system was not affected by this incident, but data stored on some servers was.

Number of New Hampshire Residents to be notified:

3

What information has been compromised:

The information the unauthorized third party potentially had access to may have included: .

Any steps the business is taking to restore the integrity of the system:

When National Nail discovered the attack, they immediately disabled all access to their servers. They then engaged forensic experts to determine the source of the attack and assist in recovery. Their investigation eventually led them to determine that certain servers were compromised, and the threat actors had exfiltrated the data. When they determined that the attack was the result of threat actors they notified and worked with law enforcement. National Nail has taken steps to address this incident and reduce the likelihood of a recurrence. These steps include end-user training, installing patches to vulnerable systems, clarifying responses to suspicious emails, updating their policies and procedures related to potentially compromised accounts, and working with our third-party service providers to provide more timely alerts of potentially suspicious login attempts.

Very truly yours,

Nathan W. Steed

NWS/sdp
Enclosure
30018403

EXHIBIT A

2964 Clydon Ave SW
Grand Rapids, MI 49519

[Insert recipient's Name]
[Insert Address]
[Insert City, State, Zip] [Date]

Notice of Data Breach

Dear [First Name][Last Name]:

We are sending this letter to you to inform you that National Nail Corp recently discovered an incident potentially involving your personal information.

What Happened? In mid-November 2023, our computer systems were breached by an unauthorized outside party. This breach caused an outage of computer systems, phones, email, and the encryption of work documents. An external party was immediately engaged and recently completed a forensic analysis and determined that work documents were extracted from National Nail's computer systems which may lead to unauthorized access to personal information.

What Information Was Involved? The information the unauthorized third party potentially had access to may have included: .

What Are We Doing? We have taken steps to address this incident and reduce the likelihood of a recurrence. Among these include the notification of law enforcement, and other actions to prevent a similar event. These include end-user training, clarifying responses to suspicious emails, updating our policies and procedures related to potentially compromised accounts, and working with our third-party service providers to provide more timely alerts of potentially suspicious login attempts.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, we are offering complimentary access to Experian IdentityWorks℠ for .

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B######] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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 specialists 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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do: In addition to enrolling in the complimentary IndentityWorks program, we remind you to remain vigilant for signs of fraud or identity theft. Please review the enclosed "Steps You Can Take to Protect Your Information" page.

We are committed to keeping your information safe, and we want to assure you that we have taken steps to prevent this type of incident in the future.

Please do not hesitate to contact us with any questions about this incident or to request additional information. You can contact Jason Williams at .

Sincerely,

President/CEO
National Nail Corp

* 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.

Steps You Can Take to Protect Your Information

- **Monitor Your Credit Report and Accounts**. You should closely monitor your credit report, credit cards, bank accounts, and online accounts for signs of any unauthorized or suspicious activity that may indicate fraud or identity theft, and be aware that criminals may attempt to send you targeted emails seeking to obtain other confidential information from you or may otherwise try to use your personal information. If you notice any illegal, unauthorized or suspicious activity, always report it to law enforcement, and the appropriate financial institution and government authorities.

- **Request a Free Initial Fraud Alert**. You should consider placing a free initial fraud alert on your credit report. An initial fraud alert lasts for ninety (90) days, and warns any creditor who orders a credit report during that period that they must not extend new credit in your name without first verifying that you are the applicant. You can renew the initial fraud alert for additional periods of ninety (90) days. If you are a victim of identity theft, you can request an extended fraud alert. To request a fraud alert, call any one of the three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.alerts.equifax.com	www.experian.com/fraud	TransUnion Fraud Victim
Equifax Consumer Fraud	Experian Fraud Center	Assistance Dept.
Division	P.O. Box 2002	www.transunion.com/fraud
P.O. Box 105139	Allen, TX 75013	P.O. Box 2000
Atlanta, GA 30348-7289		Chester, PA 19016

  You only need to contact one of the three national credit reporting agencies to place a fraud alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a credit reporting agency, you should contact that agency directly to place a fraud alert.

- **Consider Asking for a Freeze on Your Credit Report**. You may also consider asking for a freeze on your credit report. Freezing your credit report prevents a credit reporting agency from providing your credit report or credit score to anyone without your permission. You should ask about a credit freeze when you place a fraud alert on your account. There are, however, some disadvantages to a credit freeze. You will need to lift the freeze whenever you want to open a new credit account or get a new loan. This will take time and may delay your credit transaction. There is no charge for implementing or lifting a freeze. For more information about credit freezes, how to request them, and their advantages and disadvantages, go to: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

- **Review Federal Trade Commission's Identity Theft Information**. You should review information about personal identity theft and fraud at the Federal Trade Commission ("FTC") website (http://www.consumer.gov/idtheft). You may also enter your information into the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for use in their investigations, at their website or by calling 1-877-ID-THEFT. If at some point you believe any bank or credit accounts have been used fraudulently, the FTC recommends that you 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 https://www.consumer.ftc.gov/articles/pdf-0094-identity -theft-affidavit.pdf) when you dispute new unauthorized accounts.

- For **Maryland** residents: You may contact the Maryland Attorney General at 1-888-743-0023, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/.
- For **North Carolina** residents: You may contact the North Carolina Attorney General at ((919) 716-6000 , 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.gov/.
- For **New Mexico** residents: You have rights under the Fair Credit Reporting Act (FCRA), such as the right to be told if information in your credit file has been sued against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Under FCRA, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. For more information about your rights, please visit http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rightsunder-fcra.pdf, or https://www.consumerfinance.gov, or www.ftc.gov.
- For **New York** residents: For more information on placing a security freeze on your credit reports, please go to the New York Department of State Division of Consumer Protection website at https://dos.nysits.acsitefactory.com/consumer-protection. For more information on identity theft, you can visit the following websites or contacting via phone:
  New York Department of State Division of Consumer Protection: (800) 697-1220, www.dos.ny.gov/consumer-protection, NYS Attorney General at: 1-800-771-7755, www.ag.ny.gov, and Federal Trade Commission at: www.ftc.gov/bcp/edu/microsites/idtheft/