

March 29, 2021

WRITER'S DIRECT NUMBER: (317) 236-2337
DIRECT FAX: (317) 592-4745
EMAIL: Nicholas.Merker@icemiller.com

CONFIDENTIAL

Via Electronic Mail

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

RE: Written Notification of a Data Breach

To Whom It May Concern:

On behalf of my client, Nachi America, Inc. ("Nachi"), I am hereby submitting written notification of a data breach, in compliance with N.H. Rev. Stat. § 359-C:20(I)(b). Nachi is a manufacturer located at 715 Pushville Road, Greenwood, Indiana 46143.

On March 17, 2021, Nachi identified that an unauthorized user gained access to a system which housed an application that stored information. The attacker initiated a ransomware attack on the system. Nachi provided notification to a limited set of individuals based on a sample set of documents it received from the attacker. We are notifying all employees out of an abundance of caution.

Upon discovery of the ransomware attack, we immediately engaged outside counsel and began an internal investigation into the unauthorized access to determine the full scope of the breach. We believe the following information may have been accessed:

- First and Last Name
- Address
- Social Security Number; and/or
- Passport or Government-issued Identification.

Based on the investigation, we have identified one (1) New Hampshire resident who was affected. Additionally, Nachi is offering identify theft protection services through Experian's IdentityWorks to provide complementary identity theft and fraud protection services for 24

Consumer Protection Bureau
Office of the Attorney General
March 29, 2021
Page 2

months to all New Hampshire residents. A copy of the notice that was sent to the affected New Hampshire residents on March 29, 2021 is enclosed herewith.

In an effort to remedy the breach and prevent reoccurrences of similar breach, Nachi took immediate action to identify the point of access used by the attacker and remediated that vulnerability by upgrading the security settings on the impacted container and added a layer of authentication. Nachi's security team, as well as external security experts, validated the remediation of the vulnerability. Furthermore, Nachi is reviewing and revising its cybersecurity policies and procedures to enhance its cybersecurity posture.

If you require further information about this matter, please contact me by telephone at (317) 236-2337 or via email at Nicholas.Merker@icemiller.com.

Sincerely,

ICE MILLER LLP

A handwritten signature in black ink, appearing to read 'NRM', with a long horizontal flourish extending to the right.

Nicholas R. Merker

Enclosure: Copy of Individual Notification Letter

cc: [REDACTED]



<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 2, 2021
Enrollment Code: XXXXXXXXXXXX

Dear <<Name>>,

Nachi America, Inc. (“Nachi”) takes the privacy and security of your personal information seriously. We are contacting you regarding a security incident which may have involved some of your information. We want you to understand what we are doing to address this issue and what steps you can take to protect yourself.

What Happened

On March 17, 2021, Nachi identified that an unauthorized user gained access to a system which housed an application that stored your information. The attacker initiated a ransomware attack on the system. In a ransomware attack, the risk is not usually to personal information and identity theft; rather, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers and demand a monetary payment to restore data. We are notifying you out of an abundance of caution.

Upon discovery of the ransomware attack, we immediately engaged outside counsel and began an internal investigation into the unauthorized access to determine the full scope of the breach.

What Information Was Involved

Through our investigation, we determined that some of the information that may have been accessed contained Passport, Social Security Number, and/or other Government-issued Identification for some of Nachi’s employees and independent contractors. However, based on a limited set of data received from the attacker, we do not believe that all employees’ or independent contractors’ information was in fact accessed.

What We Are Doing

Upon discovery of the unauthorized intrusion, Nachi took immediate action to identify the point of access used by the attacker and remediated that vulnerability by upgrading the security settings on the impacted container and added a layer of authentication. Nachi’s security team, as well as external security experts, validated the remediation of the vulnerability.

The investigation has not revealed any attempts at fraud or identity theft. Out of an abundance of caution, Nachi is offering a 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: **July 31, 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

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 **1 888 397 3742** by **July 31, 2021**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your one-year 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 **1 888 397 3742**. 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.

What You Can Do



NACHI AMERICA INC.

715 Pushville Road Greenwood, IN 46143 317.530.1001 Fax: 317.530.1011

We encourage you to remain vigilant in monitoring your account statements, financial transactions, and credit reports for incidents of fraud and identity theft, and to promptly report such incidents. Further, please routinely review bills, notices, and statements that you receive from financial institutions.

We also encourage you to contact us with any questions and to enroll in Experian IdentityWorks using the Enrollment Code provided above. Please note the deadline to enroll is **July 31, 2021**.

For More Information

Although there is no evidence that your information was accessed as a result of this incident, if you want to learn more about the steps you can take to protect against identity theft or fraud, please review the enclosed "Reference Guide" materials.

If you have any questions about this security incident, please call Nick Merker at (317) 236-2337.

Sincerely,

Nachi America, Inc.

Reference Guide

Order Your Free Credit Report

To order your free annual 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 ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus 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 credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

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 against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor 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 fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax Fraud

Reporting

1-800-525-6285

P.O. Box 105069

Atlanta, GA 30348-

5069

www.alerts.equifax.com

Experian Fraud

Reporting

1-888-397-3742

P.O. Box 9554

Allen, TX 75013

www.experian.com

TransUnion Fraud

Reporting

1-888-909-8872

P.O. Box 2000

Chester, PA 19022-2000

www.transunion.com

Security Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

As of September 21, 2018, you have the right to request a credit freeze from a consumer reporting agency, free of charge. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:



Equifax Security
Freeze
1-800-349-9960
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security
Freeze
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Security
Freeze
1-888-909-8872
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than one business day after receiving a request by phone or secure electronic means, and no later than three business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of New York

You may also obtain information about preventing and avoiding identity theft from the New York Attorney General’s Office:

Office of Attorney General of New York,
The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General’s Office:

North Carolina Attorney General’s Office, Consumer Protection Division,
Mail Service Center 9001, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM,
www.ncdoj.gov.

For Residents of Oregon

You may report suspected identity theft to law enforcement, including the Oregon Attorney General:

Office of the Attorney General of Oregon,
Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301, 1-877-877-9392,
www.doj.state.or.us/.