IceMiller
LEGAL COUNSEL

One American Square | Suite 2900 | Indianapolis, IN 46282-0200
Chicago Columbus DuPage County, Ill.
Indianapolis New York Philadelphia Washington, D.C.

December 26, 2019

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

CONFIDENTIAL

Via Certified Mail

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

RE: Written Notification of an Information Security Incident

To Whom It May Concern:

On behalf of my client, Equian, LLC ("Equian"), I am hereby submitting written notification of an Information Security Incident, in compliance with N.H. Rev. Stat. § 359-C:20(I)(b).

On May 24, 2019, Equian learned that a very limited number of their employee email accounts were potentially compromised as a result of a phishing attack. The event was discovered when an attacker attempted to engage in social engineering using legitimate employee email correspondence as an authenticator. To our knowledge, the social engineering attack was not successful. Upon discovery, Equian began investigating the incident and hired undersigned counsel, who hired a leading computer security and forensics firm to assist with the investigation to determine the full scope of the incident. Equian reviewed over 35,500 email messages and attachments across impacted accounts.

Equian serves as a third-party service provider for a number of clients, including NCA Comp, Inc. ("NCA Comp"). After completing the investigative process into the scope of the incident, which included the manual review of a great number of email messages, Equian notified NCA Comp of the incident on July 19, 2019. On November 15, 2019, NCA Comp delegated individual and regulatory notification responsibilities to Equian.

Based on the investigation, Equian has no reason to believe that any of their other systems or networks have otherwise been compromised at this time. Equian further has no evidence to suggest that any personal information was actually accessed or acquired by any unauthorized third party. The information that may have been accessed potentially included: first and last name, social security number, or address. In an effort to remedy the incident, Equian reset the passwords of the employees whose email accounts were compromised, implemented multi-factor authentication for email access, and provided additional training regarding phishing emails. Furthermore, Microsoft Conditional Access has been implemented.

At this time, we believe the incident may have involved unauthorized access to the information of two (2) New Hampshire residents. A copy of the notice that will be sent to affected New Hampshire residents on December 27, 2019 is enclosed hereto. Credit monitoring will be offered to affected New Hampshire residents.

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

Nicholas R. Merker

Enclosure: Copy of Individual Notification Letter

EQUIAN
Equian, LLC
26555 Evergreen Road
Suite 200
Southfield, MI 48076

December 27, 2019

F1891-L02-0000880 P003 T00005 *********ALL FOR AADC 130
SAMPLE A SAMPLE - L02 NCACOMP INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A Sample,

We are contacting you regarding a security incident which may have involved some of your information with our client, NCA Comp, Inc. We, and NCA Comp, Inc., take the privacy and security of your personal information seriously and for this reason want you to understand what we are doing to address this issue and what steps you can take to protect yourself.

What Happened

On May 24, 2019, we learned that a limited number of employee email accounts were potentially accessed on May 24, 2019 by an unauthorized third party.

What Information Was Involved

Following an investigation into the limited number of email accounts that were potentially accessed, we discovered that your information was in one or more messages in the compromised email accounts. The information that may have been accessed may have included your first and last name, medical information, health insurance information, social security number, or address. We have no evidence to suggest that your personal information was actually accessed or acquired by any unauthorized third party. However, we are unable to rule out the remote possibility that your information was accessed. Therefore, out of an abundance of caution, we are providing you with this notice in the unlikely event your information was compromised.

What We Are Doing

As soon as we learned of the unapproved access, we began an investigation. Among other things, we reset the passwords of all employees whose accounts were accessed. Further, we engaged a leading digital forensics firm to assist in investigating the scope of the incident. With them, we are using this incident as an opportunity to consider any additional enhancements to our security controls to help to prevent a similar incident in the future.

What You Can Do

Although there is no evidence that your information was accessed or acquired as a result of this incident, consumers should always remain vigilant in monitoring account statements and transactions for incidents of fraud and identity theft, and promptly report such incidents. The enclosed "Reference Guide" includes additional information on general steps you can take to monitor and protect your personal information.

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**: **03/31/2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: 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 (877) 715-8889 by **03/31/2020.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-month 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 (877) 715-8889. 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.

For More Information

We take the protection of your personal information seriously and are taking steps to prevent a similar incident from occurring in the future. Although there is no evidence that your information was accessed or acquired 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 (877) 715-8889 toll free during weekdays from 9:00am to 9:00pm ET and weekends from 11:00am to 8:00pm ET. The toll free number has been created specifically to answer your questions about the incident services.

Sincerely,

Equian, LLC

* 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.

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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-888-909-8872
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	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	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	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 Iowa

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

Iowa Attorney General's Office, Director of Consumer Protection Division,
1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.

As a resident of Iowa, beginning July 1, 2018, consumer reporting agencies are prohibited from charging you a fee for placing, removing, suspending or reinstating a security freeze.

A security freeze prevents potential creditors and other third parties from accessing credit reports without your approval. Typically, businesses will not open credit card or loan accounts without checking your credit history. You must contact each of the credit reporting agencies individually online or by postal mail.

There is **no cost** to place or lift a security freeze. For more information, see detailed instructions entitled "Placing a Security Freeze on Your Credit Report to Protect Yourself from Identity Theft" at the Iowa Attorney General website at https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/security-freeze-identity-theft/.

For Residents of Kentucky

You may also obtain information about preventing and avoiding identity theft from the Kentucky Attorney General's Office:

Office of the Attorney General of Kentucky,
700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, 1-502-696-5300, www.ag.ky.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

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, Office of the Attorney General,
1162 Court Street NE, Salem, OR 97301-4096, **1-877-877-9392**, www.doj.state.or.us