

2017 MAY -8 AM 11:42

May 5, 2017

WRITER'S DIRECT NUMBER: (312) 726-2504

DIRECT FAX: (312) 726-2695

EMAIL: Nicholas.Merker@icemiller.com

VIA U.S. MAIL

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

Dear Sir or Madam:

Ice Miller LLP represents Equian, LLC and its subsidiaries, including Nurse Audit, LLC ("collectively referred to herein as "Equian"). We are writing to notify you of a security incident involving the personal information of one (1) New Hampshire resident.

On or about March 29, 2017, Equian discovered that on August 23, 2016, an unauthorized third party may have received access to 2015 W-2 tax information for current and former Equian employees through a phishing email scam. The information contained in the W-2 tax forms included the first and last names, addresses, and Social Security numbers of one (1) New Hampshire resident.

After Equian discovered the incident, it advised the affected employees about the incident and the steps they can take to protect themselves from any harm that may result from the incident. Equian is currently assessing the security measures we have in place to minimize the chances that a similar incident will occur in the future. Equian's investigation into the incident is ongoing, and Equian will continue to implement security enhancements as needed. We have no reason to believe that the personal information involved has been used to engage in identity theft. Nevertheless, Equian has offered complimentary identity theft protection services to the affected New Hampshire resident through Experian for twelve (12) months.

Please direct any questions or requests for additional information to me.

Sincerely yours,

ICE MILLER LLP



Nicholas R. Merker

Enclosures: Template Notification

STATE OF NH
DEPT OF JUSTICE
2017 MAY -8 AM 11:42

Attachment A
Template Notification

May 5, 2017

[NH RESIDENT NAME]
[ADDRESS]
[CITY, STATE ZIP]

Dear [NH RESIDENT]:

At Equian, we take the privacy and security of our employees' information seriously. We are writing to inform you that, despite our best efforts, Equian has been the victim of unauthorized access to our company information.

On or about March 29, 2017, we discovered that on August 23, 2016, an unauthorized third party may have received access to 2015 W-2 tax information for current and former Equian employees through a phishing email scam. Unfortunately, these types of attacks are becoming commonplace and hackers are growing more sophisticated. The information contained in the W-2 tax forms included employees' first and last names, addresses, and Social Security numbers.

After we discovered the attack, we advised the affected employees about the incident and the steps they can take to protect themselves from any harm that may result from the incident. We are currently assessing the security measures we have in place to minimize the chances that a similar incident will occur in the future. Our own investigation into the incident is ongoing, and we will continue to implement security enhancements as needed.

Although Equian has no reason to believe that your tax information has been used to engage in identify theft, we would like to provide you with twelve (12) months of credit monitoring and identify theft protection services with a third-party service provider, Experian, at no cost to you. 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 fraud resolution support is needed then an Experian Fraud Resolution 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 this offer 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.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID® Elite as a complimentary one-year 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: [date] (Your code will not work after this date.)
- Visit the ProtectMyID website to enroll: www.protectmyid.com/enroll
- Provide your activation code: [code]

If you have questions about the service, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-441-6943 by [enrollment end date]. Be prepared to provide engagement number [engagement number] as proof of eligibility for the fraud resolution services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment in ProtectMyID.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- Experian credit report at signup: See what information is associated with your credit file.
- Active Surveillance Alerts: Monitors Experian, Equifax and Transunion files for indicators of fraud.
- Internet Scan: Alerts you if your information is found on sites containing compromised data.
- Address Change Alerts: Alerts you of changes to your mailing address
- Fraud Resolution: Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- ExtendCARE: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- \$1 Million Identity Theft Insurance*: Provides coverage for certain costs and unauthorized electronic fund transfers.
- Lost Wallet Protection: Get help replacing credit, debit, and medical insurance cards.

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.experian.com/fraudresolution for this information.

We also recommend that you consider filing IRS Form 14039 immediately. IRS Form 14039 permits the reporting of any event involving your personal information that may at some

Consumer Protection and Antitrust Bureau
Office of the Attorney General
May 5, 2017
Page 4

future time affect your federal tax records. You can obtain IRS Form 14039 from the following website: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>. You may wish to print the form and mail or fax it according to the instructions. In most cases, in response to such a submission, the IRS will confirm your identity and begin monitoring your federal tax account. In some cases, you may also be issued a unique Identity Protection Personal Identification Number (IP PIN) for tax filing purposes. The IP PIN is a unique six-digit number that verifies your identity at the time your taxes are filed. If you wish, you may visit the following website to request an IP PIN to use when you file your taxes: <https://www.irs.gov/individuals/get-an-identity-protection-pin>.

Additionally, we advise you to remain vigilant for incidents of fraud and identity theft by periodically reviewing your account statements and monitoring free credit reports. If you would like to learn more about the steps you can take to protect against identify theft or fraud, please review the enclosed "Important Identify Theft Information" materials.

The security of your information is important to Equian, and the safety and well-being of our employees is our highest priority. We apologize for any inconvenience this incident may cause you and thank you for your understanding and cooperation. Please feel free to contact me to learn more about the incident, inquire about the personal information we maintain about you, or request any type of assistance. You may reach me at 502-214-1194 or dgibson@equian.com.

Sincerely,

Daniel T. Gibson
General Counsel and Chief Administrative Officer

Enclosure: "Important Identity Theft Information"

Important Identity Theft Information

You can help protect yourself from identity theft or other unauthorized use of personal information by taking some simple steps.

Remain vigilant. We recommend you remain vigilant for possible incidents of fraud and identity theft by reviewing your account statements and monitoring free credit reports. Credit reports can be obtained at:

Equifax
1-800-685-1111
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-916-8800
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). More information is available on the FTC's web site, at www.consumer.gov/idtheft. You can also call the FTC at (877) IDTHEFT (438-4338) or write to the FTC at the following address:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

If you are a resident of Maryland or North Carolina, you may reach your state's attorney general using the contact information below to learn more about preventing identity theft:

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
1-877-5-NO-SCAM (566-7226)
www.ncdoj.com

Add fraud alerts to your credit file. You can add a fraud alert to your credit report file to help protect your credit information at no charge. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. To place a fraud alert in your file, call one of the three nationwide credit bureaus. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which will also place fraud alerts in your file.

Place a security freeze on your credit report. You may have the right to put a credit freeze, also known as a security 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information about the process:

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
1-888-766-0008

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

TransUnion LLC
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Report potential tax fraud to the appropriate state agency. In addition to filing IRS Form 14039, you can report potential tax fraud to the appropriate agency within the state in which you file taxes.

- If you file taxes in Alabama, you can report potential tax fraud to the Alabama Department of Revenue at: <http://revenue.alabama.gov/invest/forms.cfm>
- If you file taxes in Arizona, you can report potential tax fraud to the Arizona Department of Revenue at: <https://www.azdor.gov/IdentityTheft.aspx>
- If you file taxes in California, you can report potential tax fraud to the California Franchise Tax Board at: https://www.ftb.ca.gov/online/fraud_referral/index.shtml
- If you file taxes in Colorado, you can report potential tax fraud to the Colorado Department of Revenue at: <https://www.colorado.gov/pacific/tax/criminal-investigations>
- If you file taxes in Connecticut, you can report potential tax fraud to the Connecticut Department of Revenue Services at: <http://www.ct.gov/drs/cwp/view.asp?a=3863&q=480132>
- If you file taxes in Florida, you can report potential tax fraud to the Florida Department of Revenue at: <http://floridarevenue.com/dor/taxes/violations.html>
- If you file taxes in Georgia, you can report potential tax fraud to the Georgia Department of Revenue at: <https://dor.georgia.gov/webform/fraud-referral-form>
- If you file taxes in Illinois, you can report potential tax fraud to the Illinois Department of Revenue at: <http://www.revenue.state.il.us/fraud/fraudreport.htm>
- If you file taxes in Indiana, you can report potential tax fraud to the Indiana Department of Revenue at: <http://www.in.gov/dor/4788.htm>
- If you file taxes in Iowa, you can report potential tax fraud to the Iowa Department of Revenue at: <https://tax.iowa.gov/webform/report-fraud>
- If you file taxes in Kentucky, you can report potential tax fraud to the Kentucky Department of Revenue at: <http://revenue.ky.gov/Special-Investigations/Pages/Report-Tax-Fraud.aspx>
- If you file taxes in Louisiana, you can report potential tax fraud to the Louisiana Department of Revenue at: <http://revenue.louisiana.gov/TaxFraud/ReportTaxFraud>
- If you file taxes in Massachusetts, you can report potential tax fraud to the Massachusetts Department of Revenue at: <http://www.mass.gov/dor/individuals/identity-theft-information>
- If you file taxes in Maryland, you can report potential tax fraud to the Comptroller of Maryland at: http://taxes.marylandtaxes.com/Individual_Taxes/Taxpayer_Assistance/Identity_Protection/
- If you file taxes in Michigan, you can report potential tax fraud to the Michigan Department of Treasury at: <http://www.michigan.gov/treasury/0,4679,7-121--8483--,00.html>
- If you file taxes in Minnesota, you can report to the Minnesota Department of Treasury at: http://www.revenue.state.mn.us/tax_fraud/Pages/Criminal-Investigation.aspx
- If you file taxes in Missouri, you can report potential tax fraud to the Missouri Department of Revenue at: <https://sa.dor.mo.gov/fraud/>
- If you file taxes in Mississippi, you can report potential tax fraud to the Mississippi Department of Revenue at: <http://www.dor.ms.gov/Pages/Report-Fraud.aspx>
- If you file taxes in North Carolina, you can report potential tax fraud to the North Carolina Department of Revenue at: <http://www.dor.state.nc.us/taxes/reportfraud.html>
- If you file taxes in New Hampshire, you can report potential tax fraud to the New Hampshire Department of Revenue Administration at: <http://www.revenue.nh.gov/contact-us/phone-subject.htm>
- If you file taxes in New Jersey, you can report to potential tax fraud to the New Jersey Department of Treasury at: <http://www.state.nj.us/treasury/taxation/catch.shtml>
- If you file taxes in Nevada, you can report potential tax fraud to the Nevada Department of Taxation at: https://tax.nv.gov/Contact/Contact_Us/
- If you file taxes in New York, you can report potential tax fraud to the New York Department of Taxation and Finance at: <https://www.tax.ny.gov/help/contact/fraud-scams-idtheft.htm>

- If you file taxes in Oklahoma, you can report potential tax fraud to the Oklahoma Tax Commission at: <https://www.ok.gov/tax/IDtheft.html>
- If you file taxes in Oregon, you can report potential tax fraud to the Oregon Department of Revenue at: <https://revenueonline.dor.oregon.gov/tap/>
- If you file taxes in Pennsylvania, you can report potential tax fraud to the Pennsylvania Department of Revenue at: <http://www.revenue.pa.gov/>
- If you file taxes in South Carolina, you can report potential tax fraud to the South Carolina Department of Revenue at: <https://dor.sc.gov/communications/security-center>
- If you file taxes in Tennessee, you can report potential tax fraud to the Tennessee Department of Revenue at: <https://tn.gov/revenue/article/tax-fraud-reporting-tennessee-tax-fraud-online>
- If you file taxes in Texas, you can report potential tax fraud to the Texas Comptroller at: <https://www.comptroller.texas.gov/programs/support/investigation/reporting.php>
- If you file taxes in Wisconsin, you can report potential tax fraud to the Wisconsin Department of Revenue at: <https://www.revenue.wi.gov/Pages/TaxPro/news-2010-100127b.aspx>