MINTZ LEVIN

Cynthia J. Larose | 617 348 1732 | cjlarose@mintz.com

One Financial Center
Boston, MA 02111
617-542-6000
617-542-2241 fax
www.mintz.com

March 14, 2016

Via Email (attorneygeneral@doj.nh.gov) and Federal Express
The Honorable Joseph Foster
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Reporting of Security Incident Pursuant to N.H. Rev. Stat. Section 359-C:20

Dear Attorney General Foster:

This law firm represents Mitchell International, Inc. (the "Company"). On February 24, 2016, an unknown, unauthorized person from outside the Company impersonated a member of the Company's leadership team and, using what appeared to be that person's legitimate Company email address, convinced an employee of the Company to provide certain personal information about current and former employees. The Company discovered the inadvertent disclosure on March 3, 2016, and has worked diligently to investigate and resolve this unfortunate situation. This letter serves to notify your office of the situation, and to comply with the requirements of N.H. Rev. Stat. Section 359-C:20.

Nature of the Security Incident

The disclosure that occurred was the result of human error prompted by a sophisticated phishing scam. The incident did not involve any customer information or an intrusion into our computer systems or network.

Nature of the Information Acquired and Number of Affected New Hampshire Residents

The personal information disclosed about each affected individual was limited to first and last name, Social Security number, and salary information. Our analysis suggests that the aforementioned personal information of three (3) New Hampshire residents was disclosed to the unauthorized third party.

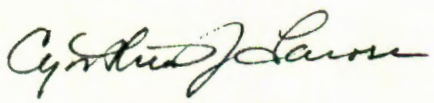
Remediation Steps

The Company has no knowledge of any personal information being used improperly to date. However, out of an abundance of caution the Company will be providing notice to all affected individuals, including both current and former employees, and will be providing twenty-four (24) months of identity protection and credit monitoring services through AllClear ID at no cost to any of the individuals affected. Additionally, the Company is continuing to assess its procedures and employee training programs to ensure that personal information is protected.

A sample copy of the Company's notification to affected New Hampshire residents is attached. The notification will be mailed to affected residents no later than March 14, 2016.

If you have any questions or concerns, please do not hesitate to contact me at (617) 348-1732 or at CJLarose@mintz.com.

Very truly yours,



Cynthia J. Larose

46546578v.1

mitchell

Mitchell
6220 Greenwich Drive
San Diego, California 92122
858.368.7000 | 800.238.9111
mitchell.com

March 11, 2016

<<First>> <<Last>>
<<Address_1>>
<<Address_2>>
<<City>>, <<State>> <<Zip Code>>

Dear <<First>>:

We are writing to you because of a recent phishing scam that has resulted in an inadvertent disclosure of your personal information. We deeply regret that this has occurred and are sending you this letter to provide details regarding what happened and to advise you about steps to take in order to help prevent identity theft and fraud.

On February 24, 2016, an unknown, unauthorized person from outside of Mitchell impersonated a member of Mitchell's executive leadership team and, using what appeared to be that person's legitimate Mitchell email address, convinced one of our employees to provide certain personal information about current and former employees. We discovered the inadvertent disclosure on March 3rd and we immediately began investigating what happened. We also began to address this matter with the appropriate authorities. Please know that this information was stolen through a sophisticated phishing scam for employee information and did not involve any customer information or an intrusion into our computer systems or network. This disclosure was the result of an incredibly unfortunate human error.

The personal information disclosed to the unknown third person was limited to the following information for each individual affected: first and last name, Social Security number, and salary information. The disclosure did not include any home address information, bank or financial account information (such as a routing number), spousal or dependent information, or health information.

Mitchell is aware of the increasing threat of cybersecurity attacks and we are committed to making sure that we have security measures in place and effective training for our employees in order to help prevent such attacks from happening. We will continue to work hard to protect your personal information.

We recommend that you take these immediate next steps:

1. IRS/State Notices. To minimize the risk of tax fraud, if you have not already filed, we recommend that you file your tax return as soon as possible. Additionally, you should complete Form 14039-Identity Theft Affidavit (https://www.irs.gov/pub/irs-pdf/f14039.pdf) and submit this form to the Internal Revenue Service ("IRS") by fax or mail. This is a proactive measure to notify the IRS that your personal information may have been compromised and to alert them about potential suspicious activity involving your tax return. The IRS has also published informational "tips" at: https://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers,-Victims-about-Identity-Theft-and-Tax-Returns. We also recommend that you consult the website of your state's tax authority to file any state-provided similar identity theft notices or forms.

2. Identity Protection Services. To ensure that we are taking proactive steps to protect you against identity theft or fraud, we will be providing you with identity protection services from AllClear ID for a period of two years. This service will include credit monitoring, identity repair services, and a $1 million identity theft insurance policy.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call AllClear ID at (855) 683-1166 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

- AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. Beginning **TUESDAY, MARCH 15** at 8 am Central time, you may sign up online at enroll.allclearid.com or by phone by calling AllClear ID at (855) 683-1166 and using the following redemption code: {RedemptionCode}.

We will provide the identity protection services described above at no cost to you and we encourage you to take advantage of each of them. All are available to you any time during the next two years.

3. Fraud Alert. If you do not choose to activate the AllClear ID identity protection services, because your Social Security number was involved, we recommend that you place a fraud alert on your credit file. A fraud alert requires potential creditors to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days or until you choose to remove it. Please contact one of the three credit reporting agencies by using the contact details provided on this page. Doing so will automatically place an alert with all three agencies. You will receive letters from each confirming the fraud alert and letting you know how to get a free copy of your credit report.

- **Experian**
  - Phone: 1-888-397-3742 (toll-free number)
  - Address: P.O. Box 4500, Allen, TX 75013
  - Online: www.experian.com

- **TransUnion**
  - Phone: 1-800-680-7289 (toll-free number)
  - Address: P.O. Box 2000, Chester, PA 19022
  - Online: www.transunion.com

- **Equifax**
  - Phone: 1-800-525-6285 (toll-free number)
  - Address: P.O. Box 740241, Atlanta, GA 30374
  - Online: www.equifax.com

4. Credit Freeze. In addition to the AllClear ID services (or the fraud alert), a credit freeze is an additional step to help alleviate concerns about becoming a victim of identity theft or fraud. It prevents creditors from seeing your credit report and credit score unless you decide to unlock the credit reporting file using a PIN code. Please note that when you have a credit freeze in place, you will be required to take special steps in order to apply for any type of credit. This process is also completed through each of the credit reporting agencies. Unlike a fraud alert, each credit reporting agency must be contacted individually by using these contact details:

- **Experian Credit Freeze**
  - Phone: 1-888-397-3742 (toll-free number)
  - Address: P.O. Box 9554, Allen, TX 75013
  - Online: www.experian.com

- **TransUnion Credit Freeze**
  - Phone: 1-800-909-8872 (toll-free number)
  - Address: P.O. Box 6790, Fullerton, CA 92834
  - Online: www.transunion.com

- **Equifax Credit Freeze**
  - Phone: 1-800-685-1111 (toll-free number)
  - Address: P.O. Box 105788, Atlanta, GA 30348
  - Online: www.equifax.com

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 agency.

Specific information for Massachusetts residents: Massachusetts law gives you the right to place a security (credit) freeze on your credit reports. A security (credit) freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security (credit) freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit reports by sending a request to the credit reporting agencies listed above by certified mail, overnight mail, or regular mail to the addresses listed above. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

In the coming months it is essential that you remain vigilant for incidents of identity theft and fraud. You should frequently review account statements and monitor your free credit reports. Look for accounts you did not open or inquiries from creditors that you did not initiate. If you see anything suspicious, immediately call the credit-reporting agency at the telephone number on the report and report the suspicious activity to AllClear ID as described elsewhere in this letter.

If you are the victim of identity theft, we encourage you to contact local law enforcement, the Attorney General's office in your state, and the Federal Trade Commission (contact details below). From these government agencies you can also obtain additional information about fraud alerts and credit freezes and learn more about preventing and managing identity theft and fraud.

Federal Trade Commission
877-438-4338 (toll-free number)
www.identitytheft.gov/

600 Pennsylvania Ave., NW
Washington, DC 20580

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Attorney General:

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

For residents of Massachusetts: You also have the right to obtain a police report.

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

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

This notice is dated March 11, 2016 and is provided by Mitchell International, Inc., 6220 Greenwich Drive, San Diego, CA 92122, Toll-Free Number: 1-800-238-9111, Fax: 858-653-5778.

If you should have questions about this incident or the identity theft and fraud services we have described in this letter, please contact AllClear ID at (855) 683-1166.

Please accept our sincerest apologies for this inadvertent disclosure and for any inconvenience it causes you.

Very truly yours,

Stephanie Kroon
SVP, General Counsel and Secretary