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 17, 2017

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. § 359-C:20

Dear Attorney General Foster:

This law firm represents The J.N. Phillips Company, Inc. (the "Company"). On February 16, 2017, an unknown, unauthorized person from outside the Company impersonated a member of the Company's management 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 personnel of the Company and its subsidiaries, Windshield Centers LLC and Strategic Claim Services, Inc. The possibility of inadvertent disclosure was brought to the attention of management at the Company on March 7, 2017, and an investigation began immediately to determine what happened and to 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. § 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 the Company's computer systems or network.

Nature of the Information and Number of Affected New Hampshire Residents

The personal information disclosed to the unknown third person consisted of the following information for each individual affected: first and last name, home address, Social Security number, salary information, deductions and any other information disclosed on their W-2 tax form. Our analysis suggests that the aforementioned personal information of twenty-four (24) New Hampshire residents was disclosed to the unauthorized third party.

Remediation Steps

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 repair and restoration 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 and awareness programs to ensure that personal information is protected.

A sample copy of the Company's notification to the affected New Hampshire residents is attached. The notification will be mailed to affected residents no later than March 20, 2017.

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

Attachments

JN Phillips Auto Glass 877-AUTOGLASS | WINDSHIELD CENTERS 877-AUTOGLASS | StrategicClaim Easier. Faster. More Accurate. Dynamic Claim Reporting & Resolution

Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 20, 2017

Dear John:

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 additional details regarding what happened and to advise you about steps to take in order to help prevent identity theft and fraud.

What Happened

On February 16, 2017 an unknown, unauthorized person from outside of J.N. Phillips impersonated a member of J.N. Phillips management and, using what appeared to be that person's legitimate J.N. Phillips email address, convinced one of our employees to provide certain personal information about all personnel of The J.N. Phillips Company, Inc., Windshield Centers LLC and Strategic Claim Services, Inc. employed during the 2016 tax year. The possibility of inadvertent disclosure was brought to the attention of management at J.N. Phillips on March 7, 2017, and an investigation began immediately to determine what happened. This information was stolen through an email phishing scam for employee information that has affected many companies and tens of thousands of individuals and did not involve any intrusion into our computer systems or network — this disclosure was the result of an unfortunate human error, not a failure of network security.

What Information Was Involved

The personal information disclosed to the unknown third person consisted of the following information for each individual affected: first and last name, home address, Social Security number, salary information, and any other information disclosed on your W-2 tax form, such as deductions. The disclosure did not include any bank or financial account information (such as a routing number), spousal or dependent information, or health information.

What You Can Do

We recommend that you take these immediate next steps:

1. IRS Notices. 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. If you received a notice related to a state tax return, you should check your state department of revenue website (listed on the Appendix) to see whether the state has a similar form.

2. Identity Protection Services. To ensure that we are taking proactive steps to protect you against identity theft or fraud, we have arranged to have AllClear ID protect your identity for the next two (2) years at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next two (2) years.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-861-4031 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-861-4031 using the following redemption code: Redemption Code.

Information on the services and how to take advantage of them is included with this letter. Please note that additional steps may be required by you in order to activate your phone alerts and monitoring options.

3. Fraud Alert. Because your Social Security number was involved, if you do not choose to activate the AllClear ID identity protection services, 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 at an earlier time. Please note that no one is allowed to place a fraud alert on your credit report except for you. All you need to do is contact one of the three credit reporting agencies by using the contact details provided below. 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 Freezes.

General information about credit freezes: In addition to the AllClear ID services (or the fraud alert), a credit freeze is a further 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. Credit freeze laws vary from state to state and the cost of placing, temporarily lifting, and removing a credit freeze varies by state, and is generally $5 to $20 per action at each credit reporting agency. *Unlike a fraud alert, each credit reporting agency must be contacted individually.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies by using these contact details:

Experian
- Address: P.O. Box 9554, Allen, TX 75013
- Online: www.experian.com

TransUnion
- Address: P.O. Box 2000, Chester, PA 19022
- Online: www.transunion.com

Equifax
- Address: P.O. Box 105788, Atlanta, GA 30348
- Online: www.equifax.com

Additional credit freeze 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. *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.

Additional credit freeze information for Rhode Island residents: Rhode Island 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 report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address 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: 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 valid police report, investigative report, or compliant with a law enforcement agency about the unlawful use of your identifying information. 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 $10 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft and have submitted a valid police report, investigative report, or complaint with a law enforcement agency about the unlawful use of your identifying information to the credit reporting company. If you are 65 years of age or older the fee will be waived.

5. Keep Aware! 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. It is also advisable to report suspected identity theft to local police and to the Attorney General's office in your state.

What We Are Doing

We are 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.

For More Information

Please refer to the Appendix to this notice for additional information about protecting your identity or about how to respond if you are the victim of identity theft. Important information relevant to the state where you reside may also be found on the Appendix.

Please accept our sincerest apologies for any inconvenience caused by this incident.

Very truly yours,

Maureen D. Confalone
Managing Director
Chief Financial Officer

APPENDIX

Information about Identity Theft Prevention

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

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338) (toll-free number). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

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

For residents of North Carolina: You may 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 (toll-free number), www.ncdoj.gov.

For residents of Rhode Island: You also have the right to file or obtain a police report, and you may obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office:

Rhode Island Attorney General's Office, Consumer Protection Unit
150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov/.

Information about State Department of Revenue Websites

Connecticut – http://www.ct.gov/drs/cwp/view.asp?a=4834&q=576872
Florida – n/a
Georgia – https://dor.georgia.gov/webform/fraud-referral-form
Illinois – http://tax.illinois.gov/Fraud/IdentityTheft.htm
Massachusetts – http://www.mass.gov/dor/docs/dor/identity-theft/ita.pdf
Maine – call 207-624-9600
North Carolina – http://www.dornc.com/individual/identitytheft.html
New Hampshire – n/a
New York – https://www.tax.ny.gov/pdf/current_forms/misc/dtf275_fill_in.pdf
Pennsylvania – http://www.revenue.pa.gov/FormsandPublications/otherforms/Documents/rev-1196.pdf
Rhode Island – http://www.tax.ri.gov/Tax%20Website/TAX/Advisory/ADV%202015-03.pdf
South Carolina – http://www.consumer.sc.gov/Documents/PUBLICATIONS/IDTheftUnit/IDT%20Intake%20Form%20V2_KLF%208x11%20-%20Use%20for%20Web.pdf
Virginia – n/a
Wisconsin – https://datcp.wi.gov/Documents/IDTheftTaxFraudPacket665.pdf