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 31, 2020

WRITER'S DIRECT NUMBER: (317) 236-2391
DIRECT FAX: (317) 592-4736
EMAIL: Stephen.Reynolds@icemiller.com

**CONFIDENTIAL**

**Via Electronic Mail**

Office of the New Hampshire Attorney General
DOJ-CPB@DOJ.NH.gov
33 Capitol Street
Concord, NH 03301

***RE: Written Notification of an Information Security Incident***

Dear Attorney General:

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

Ontario Systems, LLC discovered that an unauthorized third party improperly obtained credentials belonging to one of its employees via phishing attack. The unauthorized third party used the improperly obtained credentials to access the company email account of the employee. It is believed that the unauthorized access may have occurred between June 19, 2020 and June 22, 2020. The unauthorized access was discovered on June 22, 2020. This may have resulted in unauthorized access to Ontario Systems, LLC's employees' personal information. This information may have included name, address, date of birth, social security number, and financial account information. Based on Ontario Systems, LLC investigation, there is no reason to believe that any other systems or network have been otherwise compromised.

Ontario Systems, LLC's investigation also revealed that the unauthorized actor created message forwarding rules for emails received by the employee, where the subject or body of the email contained the following keywords: value; wire transfer; ACH; payment; invoice; Bank transfer; and, bank information. This suggests that the unauthorized actor was seeking information about Ontario Systems, LLC's financial activities, and likely directed at facilitating fund transfer fraud activities using Ontario Systems, LLC's finance department. Based on our investigation of this incident, and experience handling other similar incidents, we believe Ontario Systems, LLC, as the company, was the target; and not its employees or employees' personal information.

Ontario Systems, LLC performed forced password reset for its impacted employee and forced log-outs for all of its employee. Additional tools to help prevent these types of emails getting through to employees were implemented. In addition, Ontario Systems, LLC further

implemented multi-factor authentication to help prevent this type of access occurring even if a phishing attack is successful.

At this time, we believe the security incident may have involved unauthorized access to the information of **one (1)** New Hampshire resident. A copy of the notice that will be sent to the affected New Hampshire resident on December 31, 2002 is attached hereto. Credit monitoring will be offered to the New Hampshire resident. Ontario Systems, LLC is continuing to investigate this incident and will provide further updates as appropriate.

If you require further information about this matter, please contact me by telephone at (317) 236-2391 or via email at stephen.reynolds@icemiller.com.

Very truly yours,

ICE MILLER LLP

Stephen E. Reynolds

Attachments: Copy of Notice

ONTARIO SYSTEMS

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

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

December 31, 2020

Dear <<First Name>> <<Last Name>>,

Ontario Systems, LLC ("Ontario Systems") takes the privacy and security of your personal information seriously. We are contacting you regarding an 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 June 22, 2020, we discovered that an unauthorized actor from outside Ontario Systems was able to improperly obtain email login credentials belonging to one of our employees through a phishing email. The unauthorized actor then used the improperly obtained credentials to access the employee's company email account for a brief period of time. It is important to note that the employee had no access to any of our clients' data and our clients' data was not impacted.

Upon learning of the incident, we immediately took action to secure the employee's email account to prevent further access. We also launched an investigation and engaged a leading forensic security firm to assist in our investigation. As part of that investigation, we searched for any personal information in the email account that could have been accessed.

**What Information Was Involved**

Through our investigation, we determined that the email account contained records that included some of your personal information. The personal information included in those documents included your <<PII types>>. We have no evidence to suggest that this information was actually accessed, viewed or acquired by the unauthorized actor.

**What We Are Doing**

As soon as we learned of the unauthorized access, we immediately took action to secure the employee's email account to prevent any further access and implemented additional tools to further prevent these types of attacks. We also engaged a leading forensic security firm and launched an investigation. As part of that investigation, we searched for any personal information in the email account that could have been viewed. We recently completed our investigation and have determined that the email account contained records that included some of your personal information.

The investigation has not revealed any access to, or misuse of your information, or any attempts at fraud or identity theft. Out of an abundance of caution, we are offering complimentary identity theft protection services through IDX, experts in data breach and recovery services. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

**What You Can Do**

We encourage you to remain vigilant in monitoring your account statements and financial transactions 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 IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 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.

We take the protection of your personal information seriously. If you want to learn more about the steps you can take to protect against identity theft or fraud, please go to https://app.idx.us/account-creation/protect or call 1-800-939-4170, toll free Monday through Friday from 9 am - 9 pm Eastern Time. The toll-free number has been created specifically to answer your questions about the incident services.

Sincerely,

Ontario Systems, LLC

**Recommended Steps to help Protect your Information**

**1. Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

**Credit Bureaus**

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

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

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.
In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

**Iowa Residents:** Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515281-5926, www.iowaattorneygeneral.gov.

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

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

**New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-7717755; https://ag.ny.gov/.

**North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401274-4400

**Washington State Residents:** The Attorney General can be contacted by mail at Office of the Attorney General, 1125 Washington St SE, P.O. Box 40100 Olympia, WA 98504, (360) 753-6200, 1-800-551-4636, or online at https://www.atg.wa.gov.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.