



Nortrax, Inc.  
396 County Road  
Westbrook, ME 04092

January 14, 2019

Gordon J. MacDonald  
Attorney General  
33 Capitol Street  
Concord, NH 03301  
attorneygeneral@doj.nh.gov  
phone: 603-271-3658 fax: 603-271-2110

Re: Legal Notice of Information Security Breach Pursuant to N.H. Rev. Stat. Ann. § 359-C:19

Dear Mr. MacDonald:

In accordance with the above referenced provision of New Hampshire law, I write to inform you of a data security incident affecting residents of New Hampshire.

During routine security monitoring, we identified suspicious activity related to an employee's email account and immediately launched an investigation. On November 30, 2018, our investigation determined that an unauthorized user likely accessed an employee's email account and obtained copies of certain emails sent to our employee between August 18, 2018 and October 26, 2018. These emails may have contained personal information including, among other types of information, individuals' names, addresses, phone numbers, Social Security numbers, or driver's license numbers.

Upon learning of this incident, we launched an investigation into the incident and contacted law enforcement. Upon determining that the incident may have resulted in access to certain personal information, we undertook a process to identify information that may have been accessed and to notify those individuals that may have been impacted.

We plan to notify four potentially affected individuals who are residents of New Hampshire. Enclosed is a copy of the notification letter that will be sent to affected New Hampshire residents via first-class mail today, January 14th. The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by Nortrax to protect personal information from further unauthorized access; (3) a toll-free phone number to call for further information and assistance; (4) information on how an individual may enroll in free credit monitoring and other complimentary services arranged by Nortrax; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free number, address, and website for the Federal Trade Commission, and a statement that individuals can obtain information on identity theft from this source; and (8) advice that directs the individual to remain vigilant by reviewing and monitoring account statements and credit history.

If you have any questions or need further information regarding this incident, please contact our counsel, Jason Stanley, at StanleyJason@JohnDeere.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Chris Holmes". The signature is fluid and cursive, with a prominent initial "C" and "H".

Chris Holmes  
President & CEO  
Nortrax, Inc.

Enclosure



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

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

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

January 14, 2019

**NOTICE OF DATA SECURITY INCIDENT**

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

We are writing to share important information about a data security incident that may have affected some of your personal information.

**What Happened?**

During routine security monitoring, Nortrax Inc. identified suspicious activity related to an employee’s email account and immediately launched an investigation. On November 30, 2018, our investigation determined that an unauthorized user likely accessed an employee’s email account and obtained copies of certain emails sent to our employee between August 18, 2018 and October 26, 2018. These emails may have contained your personal information.

**What Information Was Involved?**

Although our investigation into this incident is ongoing, we understand that the personal information may have included, among other types of information, your name, address, phone number, Social Security number, or driver’s license number.

**What Are We Doing?**

Upon learning of this incident, we launched an investigation into the incident and contacted law enforcement. Upon determining that the incident may have resulted in access to certain personal information, we undertook a process to identify information that may have been accessed and to notify those individuals that may have been impacted, including you.

Although our investigation into this incident is ongoing, we are not aware of any personal information being misused. However, we are offering you and other affected individuals MyIDCare™ identity theft protection services through ID Experts®, the data breach and recovery services expert. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

## **What Can You Do?**

We encourage you to contact ID Experts with any questions and to enroll in the free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Please note the deadline to enroll is April 14, 2019. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Regardless of whether you elect to enroll in the credit monitoring and identity-theft protection services, we recommend that you remain vigilant of the risk of identity theft by regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity and notify your financial institution if you suspect any unauthorized activity. We also recommend that you remain cautious of phishing emails, which may contain website links or other information that appear legitimate. **Attachment A** contains detailed instructions for enrollment in the MyIDCare services and more information about steps you can take to protect yourself against fraud and identity theft.

## **For More Information.**

We consider the security of personal information to be a top priority. Please be assured that we are taking steps to address the incident and to continue protecting the security of your data. If you have any questions about this notice or the incident, please feel free to call 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect> for assistance.

Sincerely,



Chris Holmes  
President & CEO  
Nortrax Inc.



## ATTACHMENT A

### **Recommended Steps to help Protect your Information**

- 1. Website and Enrollment.** Go to <https://app.myidcare.com/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 MyIDCare 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, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare 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](http://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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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 the 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 or obtain 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.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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.

**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.

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