16169

WINDROSE
HEALTH INVESTORS

Michael Spiciarich
Controller & Chief Compliance Officer
WindRose Health Investors
632 Fifth Ave., 16th Floor
New York, NY 10022

Name
Address
City, State, Zip

Dear _____,

We are writing to follow up on an incident that we first reported to you on November 21st when a phishing email was sent to many of our contacts from an address that was posing as WindRose. We have subsequently completed a forensic review of the incident and would like to provide you with an update on our findings. Our review showed that WindRose's email system was hacked which resulted in a data security incident that may involve your personal information. We value the trust that you place in us as investors and deeply regret that private information was put at risk. While we have always taken steps to protect against such breach, we have engaged external resources to help further protect against a future occurrence. Below we have outlined more details on the data breach and some ways that we would like to assist in mitigating your current and future risk related to the incident.

What happened?
In mid-November, our administrative team was in phone and email contact with one of our vendors about a legitimate invoice. Unfortunately, it appears that this vendor's email account had been compromised and instead of the expected invoice, the threat actor (posing as our vendor) sent an email with a link to an invoice that was actually a compromised link. This link was clicked on by one of our employees which enabled the threat actor to access the email account of that employee. An unknown party had access to our employee's email account between November 18 and November 21, 2019 and therefore may have had access to your personal data. On November 21st, this threat actor caused an email that appeared to be from WindRose to be sent to many of you. Upon seeing that email, we quickly identified that we had an issue and were able to retake the email account and quarantine the issue.

What information was involved?
The personal data that may have been compromised due to this incident may include your tax ID number, Social Security number, bank account information, name, address, phone number, and/or email.

What are we doing?
Although we have always maintained reasonable measures to protect and secure our data and networks, including through technical, physical and administrative means, we are in the process of evaluating those safeguards and will update them as necessary to further protect our systems and help to prevent any reoccurrence of such an attack. We tasked our regular IT provider and an external computer forensics team to determine the scope of the incident. Both concluded that the only access the threat actor had was to this one email account. Additionally, both confirmed the threat was no longer present. We have also notified law enforcement and are working with them to ensure this incident is properly addressed.

What you can do:
Review Your Account Statements and Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. Contact information for the FTC is:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-ID-THEFT (877-438-4338)

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.

If you are a resident of Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact your state attorney general to report suspected identity theft or to obtain information about preventing identity theft at:

Maryland: 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, http://www.marylandattorneygeneral.gov.
Massachusetts: 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago.
North Carolina: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226 / 1-919-716-6400, www.ncdoj.gov.
Rhode Island: 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

Copy of Credit Report
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax: 1-800-685-1111, www.equifax.com, P.O. Box 740241, Atlanta, GA 30374.
Experian: 1-888- 397-3742, www.experian.com, 535 Anton Blvd., Suite 100, Costa Mesa, CA 92626.
TransUnion: 1-800-916-8800, www.transunion.com, P.O. Box 6790, Fullerton, CA 92834.

Police Report
If you are a resident of Massachusetts or Rhode Island, you have the right under your state's law to file and obtain a copy of a police report. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Security Freeze
You have the right to place a security freeze (also known as a credit freeze) on your credit file free of charge. A security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. Placing a freeze, however, may delay or otherwise interfere with the timely approval of any subsequent credit request or application you make. To request a security freeze, you must contact each of the three credit bureaus listed above and may be asked to provide:

- Your full name,
- Social Security number,
- Date of birth,
- If you have moved in the past five (5) years, addresses where you have lived over those five (5) years,
- Proof of current address,
- A copy of a government issued identification card, and
- If you are an identity theft victim, the police report, investigative report or complaint to a law enforcement agency.

The credit bureaus have one (1) to three (3) business days upon receipt of your request (depending on the method used to submit) to place a security freeze on your credit report. They must also send written confirmation within five (5) business days and provide you with a personal identification number (PIN) that you can use to remove the freeze. You may contact the three credit bureaus or the FTC for more information concerning security freezes. A consumer reporting agency must allow a consumer to place, lift or remove a security freeze free of charge.

Fraud Alert
You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Credit Report Monitoring
To help relieve concerns following this incident, we are offering the services of Kroll to provide identity monitoring at no cost to you for a minimum of one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. To take advantage of this offer, please email me in the next 60 days for instructions.

Other Free Resources on Identity Theft
You may wish to review the tips provided by the Federal Trade Commission. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

More Information
For further information and assistance, please contact me by email at spiciarich@wendroselaw.com or phone at 212-887-2195.

Thank you,

Michael Spiciarich