

# PROSKAUER ROSE LLP

1001 Pennsylvania Avenue, NW  
Suite 400 South  
Washington DC 20004-2533  
Telephone 202.416.6800  
Fax 202.416.6899

NEW YORK  
LOS ANGELES  
BOSTON  
BOCA RATON  
NEWARK  
NEW ORLEANS  
PARIS

## Fax Transmittal

**Date** March 19, 2009 **Client-Matter** 19077.001

**Total Pages (Including Cover)** 5

**From** Brendon M. Tavelli

**Sender's Voice Number** 202.416.6896

**Sender's Room Number** DC

**Sender's Email Address** btavelli@proskauer.com

**Main Fax Number** 202.416.6899

**To:** Mary Thayer, Consumer Protection and Antitrust Bureau

**Fax No.:** (603) 223-6202

**Company:** New Hampshire Office of the Attorney General

**Voice No.:**

### Message

### CONFIDENTIAL

**Please see the attached notice submitted on behalf of LifeWatch Corporation.**

**Confidentiality Note:** This message is confidential and intended only for the use of the addressee(s) named above. It may contain legally privileged material. Dissemination, distribution or copying of this message, other than by such addressee(s), is strictly prohibited. If you have received this message in error, please immediately notify us by telephone and return the original to us at the address above. We will reimburse you for the cost of the telephone call and postage. Thank you.

BOCA RATON  
BOSTON  
CHICAGO  
LONDON  
LOS ANGELES  
NEW ORLEANS  
NEW YORK  
NEWARK  
PARIS  
SÃO PAULO

## PROSKAUER ROSE LLP

1001 Pennsylvania Avenue, NW  
Suite 400 South  
Washington DC 20004-2533  
Telephone 202.416.6800  
Fax 202.416.6899

**Brendon M. Tavelli**  
Attorney at Law

Direct Dial 202.416.6896  
btavelli@proskauer.com

March 19, 2009

**By FAX (603) 223-6202**

Office of the Attorney General  
Attn: Mary Thayer  
Consumer Protection and Antitrust Bureau  
33 Capitol Street  
Concord, NH 03301

Re: Legal Notice of Information Security Breach

Dear Ms. Thayer:

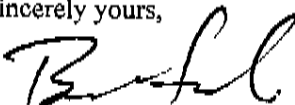
I write on behalf of LifeWatch Corp. ("LifeWatch") to inform you of an information security breach potentially involving approximately three residents of your state. On Friday, February 20, 2009, LifeWatch learned that some LifeWatch user files inadvertently were available on a publicly accessible company website. As a result, personal information in the user files, including name, birth date, health diagnoses and some related monitoring reports and in some cases Social Security numbers, potentially were exposed for approximately three weeks.

Upon learning of the issue, LifeWatch acted immediately to ensure the information was no longer accessible and began investigating to determine the exact nature of the breach for the individuals potentially affected. Based on our investigation, we do not believe any New Hampshire resident's personal information actually was accessed while the information was available on the LifeWatch website, although we cannot rule out the possibility of access. LifeWatch has no reason to believe that any personal information has been or will be misused.

Nonetheless, out of an abundance of caution, LifeWatch is notifying all potentially affected individuals of the possible information security breach via written letter to each through first class mail. Mailings will begin this afternoon. For your convenience, a copy of the form of notice is attached.

If you have any questions or need further information regarding this incident, please let me know.

Sincerely yours,



Brendon M. Tavelli

Enclosure



10255 W. Higgins Road, Ste. 100, Rosemont, IL 60018

March 19, 2009

Dear

We are writing to inform you of a recent incident involving the potential exposure of personal information concerning some users of LifeWatch Corp. ("LifeWatch") services. On February 20, 2009, we learned that some of your patient information may have been made available inadvertently on a publicly accessible website. This occurred because of a unique combination of factors that led to the accidental mis-configuration of computer equipment at LifeWatch. As a result, your personal information, including your name, birth date, health diagnoses, and some related cardiac event monitoring reports were potentially exposed on the Internet for approximately three weeks.

Immediately upon learning of the incident, we took steps to ensure all personal information was promptly removed. While we deeply regret the incident, it was an accident. It was not a targeted attack where individuals intentionally were attempting to obtain personal information. Moreover, we conducted an investigation into the incident and all indications are that only a small number of individuals' personal information was actually accessed. Your personal information was **not** among the population we know was accessed. For all of these reasons, we believe the risk of identity theft is extremely low.

Nonetheless, out of an abundance of caution, we do want to make you aware of steps you can take to guard against identity fraud. In addition, because we realize that the thought of potential identity theft can be of concern, we are making available to you a free credit monitoring product, Triple Alert<sup>SM</sup>, for 24 months to help you detect possible misuse of your data. If you choose to enroll in this product, you must activate your credit monitoring membership within 90 days from the date of this letter by visiting <http://partner.consumerinfo.com/LFW> and using your **unique single-use activation code**

Please see the attached pages containing additional information on this product including important enrollment and reimbursement instructions and other useful information.

LifeWatch has always been a leader in the remote cardiac monitoring industry and its leadership has been based as much on its relationships with its customers and users as it has been on its technology. As such we have taken and will continue to take actions well beyond our formal obligations to do what we can to address any concerns you may have in light of this unfortunate accident. We encourage you to call our dedicated toll-free number at [redacted] for additional information to answer any questions you may have. Moreover, not only have we corrected the situation, we have taken steps to ensure it does not happen again. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Dr. Yacov Geva  
Chairman & CEO



Accredited by the Joint Commission

### Additional Information

Lifewatch has engaged ConsumerInfo.com, Inc., an Experian® Company, to provide you with their Triple Alert<sup>SM</sup> Credit Monitoring product, which includes daily monitoring of your credit reports from the three national credit reporting companies (Experian, Equifax® and TransUnion®) and email monitoring alerts of key changes to your credit file. As part of the Triple Alert<sup>SM</sup> Credit Monitoring product, residents of states other than New York will also receive \$25,000 in identity theft insurance\* provided by Virginia Surety Company, Inc., with no deductible as well as access to dedicated fraud resolution representatives if needed. \*Please note that, due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

- To learn more about Triple Alert and to enroll, go to <http://partner.consumerinfo.com/LFW> and follow the instructions. You will need the activation code we provided to you. This code is unique for your use and should not be shared.
- Should you need further assistance, including credit monitoring enrollment support for those that may not have a computer, please call ConsumerInfo.com toll-free at **866-252-0121**. The ConsumerInfo.com customer service representatives are available weekdays, from 9 a.m. to 9 p.m. ET, and on Saturday and Sunday, from 11 a.m. to 8 p.m. ET.

Even if you do not feel the need to register for the credit monitoring service, we recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report 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 30348-5281 (you can print a copy of the request form at <http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtml>). You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies:

Equifax  
(800) 885-1111  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374-0241

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 9532  
Allen, TX 75013

TransUnion  
(800) 916-8800  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 6790  
Fullerton, CA 92834-6790

When you receive your credit reports, review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. An initial fraud alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you have been a victim of identity theft and you provide the credit reporting company with the documentary proof it requires. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three credit reporting companies provided above.

**Credit Freezes:** In some U.S. states, you have the right to put a "credit freeze" (also known as a "security freeze") on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. Therefore, using a credit freeze may interfere with or delay your ability to obtain credit. In addition, you may incur fees to place, lift, and/or remove a credit freeze. There may be fees for placing, lifting, and/or removing a credit freeze, which generally range from \$5-20 per action. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.