myMatrixx®
good medicine for business

February 13, 2014

Via Federal Express
Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Breach of Security for New Hampshire Residents Pursuant to N.H. Rev. Stat. §§ 359-C:20

To Whom It May Concern:

myMatrixx is writing you to provide notice of a breach of security involving a New Hampshire resident.

We first learned limited information about this incident from federal law enforcement in Florida in late November 2013. At that time, we were informed by federal law enforcement of an investigation into one of our former employees, based in Florida, who was suspected of filing fraudulent tax returns. The employee in question had left our company several months prior to our learning about this situation from law enforcement. At the time, we were instructed by law enforcement not to make any disclosures concerning this investigation.

Subsequently, we were informed by law enforcement in late December 2013 that we could provide notification related to this incident. After that time, in mid-January 2014, we were provided additional information from law enforcement about much of the information that was subject to the potential security breach. This permitted us to identify individuals whose personal information was potentially affected by this incident.

Based on the information provided by federal law enforcement and our own investigation, we have notified one New Hampshire resident that her information was improperly accessed by this individual and was potentially subject to mis-use. We are not aware of any mis-use of this information, only that this individual may have accessed the information. This personal information included name and Social Security Number. This information DID NOT contain any credit card numbers.

myMatrixx notified this New Hampshire resident on or about February 7, 2014, and has arranged for her to receive free credit monitoring and identity protection services from First Watch Technologies, Inc. **Attached is a copy of a sample notice.** This service will help protect affected persons in the unlikely event of a loss and will be provided at no cost to them.

myMatrixx is reviewing its data security practices, and is reviewing additional security procedures in order to look for ways to improve its procedures. We already have made changes to our procedures for handling sensitive information.

Please do not hesitate to call me directly with any questions that you might have. Thank you for your consideration of this matter.

Very truly yours,

Ann E. Pointer
General Counsel
813.321.6317 Office
813.368.9493 Mobile
813.642.7813 Fax
apointer@mymatrixx.com

ATTACHMENT: Copy of notice to New Hampshire resident

[myMatrixx letterhead]

[Date]

[Claimant Name/Address]

Dear [Name of Claimant,]

As a precautionary measure, on behalf of [redacted], we are writing to let you know about a recent situation that involves some of your personal information. myMatrixx was formerly the pharmacy benefits manager for [redacted] in connection with workers' compensation claims. We take the privacy and security of your personal information very seriously, and we wanted to bring this issue to your attention.

We were recently informed by federal law enforcement that one of our former employees was being investigated in connection with the potential filing of fraudulent tax returns. While we were initially instructed by law enforcement not to release information about this incident or investigation, we now have been informed that we may contact individuals about this incident.

The employee in question had left our company several months prior to our learning about this situation from law enforcement. We have been made aware by law enforcement of a small number of situations where this former employee attempted to (and may have succeeded in) filing fraudulent tax returns. While we have learned of these events only recently, the inappropriate access to personal information took place in 2012 or earlier, and the fraudulent tax filings took place in the first half of 2012.

In the course of this law enforcement investigation, we were made aware of additional situations where this former employee had improperly accessed personal information about our claimants. This personal information included names and Social Security Numbers. **This information DID NOT contain any credit card numbers.** We do not know if this additional information (including your personal information) was used inappropriately in any way, but we wanted to bring this matter to your attention so that you can take appropriate action (as described below) if you wish.

For your peace of mind, we have arranged for you to receive free identity monitoring services from First Watch Technologies, Inc. These services will help protect you in the unlikely event of a loss and will be provided at no cost to you. *Please see the enclosed Information Sheet for additional details and instructions for activating coverage.* You will have until April 30, 2014, to activate this coverage, which will then continue at no cost to you for 12 months from the date of activation. We encourage you to take advantage of these free services.

Whether or not you sign up for the First Watch services, it is always a good idea to protect against possible identity theft. While we are unaware at this time of any specific inappropriate activity other than a small number of fraudulent tax returns, as a precaution, we recommend you carefully and regularly review your credit reports and all your credit card statements and other financial account information. If you find any unauthorized or suspicious activity, you should contact your credit card company or bank immediately. 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. We are enclosing a reference guide based on information from the Federal Trade Commission and other authorities to give you more information about identity theft, how to report it and how to protect yourself.

We understand how frustrating this experience may be for you and we apologize for the inconvenience. We deeply regret that the incident occurred and strongly encourage you to take the precautionary steps outlined in this letter. While this employee left our company several months ago, we have taken additional steps to increase the protections of personal information that we maintain about our claimants, to reduce the risk of any incident like this in the future.

If you have questions about this incident or any of the information in this letter, please contact us toll-free at 1-888-770-5571.

Sincerely,

Artemis Emslie
President

Enclosures as stated

cc: [redacted]

Allen, TX 75013

3. Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

Identity Monitoring Sign Up Information

To help safeguard you from misuse of your personal information, we have arranged monitoring of activity within the United States for 12 months at no cost to you. You can enroll in a professional identity monitoring service (First Watch ID) provided by First Watch Technologies, Inc. You can sign up for this service any time between now and April 30, 2014, using the verification code listed below. To enroll in this service, simply go to **www.firstwatchid.com** and:

* Click on the Verification Code button.
* Enter the appropriate information, including your unique 12-digit verification code: _____.

After enrollment, you will receive one year of proactive identity monitoring. First Watch ID will monitor thousands of databases and billions of records on your behalf to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is potentially fraudulent.

Additionally, if you enroll, First Watch provides you with easy online access to monitor your credit activity using the three major credit bureau services. Each credit bureau will provide you one free credit report annually. First Watch suggests you request your free credit report from one bureau at a time every four months. This allows you to monitor credit activity three times per year. First Watch will send you an email (at the email address you provide) every four months reminding you to request your free credit report from the appropriate bureau.

The First Watch ID service also includes up to $25,000 of identity theft insurance with $0 deductible, along with identity restoration coverage (certain limitations and exclusions may apply).

IDENTITY THEFT PREVENTION GUIDE

Sign up for free "fraud alert" and/or security/freeze: At your request, the three major credit bureaus will place a free "fraud alert" on your file letting creditors know that they should take extra steps to confirm your identity before granting credit in your name. You also can request a security freeze on your accounts if you wish. (Please note that these steps may make it more complicated for you to get new credit or make certain purchases.) A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. If you would like to place a fraud alert or security freeze, contact any one of the following bureaus and that one will inform the others:

Credit Bureau	Toll-Free No.	Website
Experian	888-397-3742	www.experian.com
Equifax	877-478-7625	www.fraudalerts.equifax.com
TransUnion	800-680-7289	www.transunion.com

Request a copy of your credit report: You are entitled to a free credit report every twelve (12) months. To request a free credit report, call 877-322-8228 or order on-line at www.annualcreditreport.com. Call the credit bureau immediately if you see any inaccurate information or accounts that you did not open on the report.

FTC information: For additional information on how to protect yourself against identity theft, you also may wish to visit the Federal Trade Commission's website at www.consumer.gov/idtheft/. You also can report potential identity theft or file a complaint with the FTC using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You also may wish to place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

1. Equifax Security Freeze
   P.O. Box 105788
   Atlanta, GA 30348

2. Experian Security Freeze
   P.O. Box 9554