

May 4, 2018

RECEIVED  
MAY 07 2018  
CONSUMER PROTECTION

**VIA FEDERAL EXPRESS**

NH Department of Justice  
Gordon J. MacDonald, Attorney General  
33 Capitol Street  
Concord, New Hampshire 03301

Re: RxValet - Notice of Data Breach

Ladies and Gentlemen:

Our Firm represents Rx Valet LLC (the "Company"). Please be advised that in late 2017, a third-party vendor configured a server and left Company customer information exposed on the internet for some period of time. The Company learned of the incident in early 2018 and published notice of it on the Company website. Since the incident occurred, the Company has investigated to ascertain whether the problem is contained, and has taken steps to prevent further accidental exposure of such information in this fashion.

We are notifying your office on behalf of the Company pursuant to New Hampshire Revised Statutes Chapter 359-C, § 359-C:20. We believe approximately two (2) persons in New Hampshire may have been affected by this incident and those persons will receive notification of this security breach by the enclosed letter.

Please contact the undersigned if your office has any questions or concerns regarding this matter.

Very truly yours,



Mitzi L Hill

MLH/ pr

Enclosure

[MyRxValet.com LETTERHEAD]

[INDIVIDUAL NAME]  
[STREET ADDRESS]  
[CITY, STATE AND POSTAL CODE]  
[DATE]

### **NOTICE OF DATA BREACH**

Dear [INDIVIDUAL NAME]:

We at MyRxValet.com (the “Company”) value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involves your personal information. **This letter follows up on the public notice we published on the Company website in March regarding this incident.**

#### **WHAT HAPPENED?**

Some time in late 2017, a database containing the Company’s customer order records (the “Database”) became publicly exposed to the internet as a result of a server misconfiguration. While the Database was exposed to the internet, it was possible for persons using the internet to access customer records from the Database. We have confirmed that customer records for approximately one hundred one customers, including you, were actually accessed during the period when the Database was exposed to the internet. The server configuration, which was handled by a third party service provider of the Company, has been rectified, and the Database is no longer exposed to the internet.

We confirmed the incident in March, after an outside source brought the matter to our attention. We coordinated the early part of our investigation to include that source’s information.

Based on what we have learned, we do not believe that your information was misused or is reasonably likely to be misused.

#### **WHAT INFORMATION WAS INVOLVED?**

The data exposed and accessed included personal information such as name, email address, physical address, and order information including (1) items ordered, including medication name and (2) obscured credit card numbers (in which only the last four digits of the card number were readable). To our knowledge, the full credit card number was not exposed; neither were the CVV or expiration date of the card. We have confirmed with our credit card processor that the last four digits of your credit card, alone, do not permit an unauthorized person to use the card. Also, the Company does not have your Social Security Number on file, and so that was also not exposed.

#### **WHAT WE ARE DOING**

The Company values your privacy and deeply regrets that this incident occurred. When we learned of the incident, we started investigating using both internal and external resources to

try to ascertain the scope of the incident. We also notified customers via the home page of the Company website, [www.myrxvalet.com](http://www.myrxvalet.com), after confirming the incident in March; that notice remains on our website as of the date of this notice.

The Company used outside forensic and legal experts to assist in our investigation. Because the incident involved a third party's services and an outside source, investigating the scope of the records made available to the internet took several weeks from the date we first confirmed the incident.

We have conducted an extensive review of the matter, and will notify you if there are any significant developments. The Company has caused the third-party service provider to rectify the server error, and has implemented additional security measures designed to prevent a recurrence of such an issue and to protect the privacy of the Company's valued customers.

### **WHAT YOU CAN DO**

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information, and how to receive free identity theft protection from Guardians ID Theft services for one year.

### **FOR MORE INFORMATION**

For further information and assistance, please contact the Company at 1-833-798-2538 between 8 a.m.- 5p.m. Eastern time daily, or email us at [importantinfo@myrxvalet.com](mailto:importantinfo@myrxvalet.com).

Thank you for using RxValet.com.

Sincerely,

Greg Santulli  
CEO

## Steps You Can Take to Further Protect Your Information

- **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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](http://IdentityTheft.gov) or call 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.

- **Obtain and Monitor Your Credit Report**

We recommend that you 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 access the request form at <https://www.annualcreditreport.com/requestReport/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  | Experian   | TransUnion   |
| (800) 685-1111                                       | (888) 397-3742   | (800) 888-4213   |
| <a href="http://www.equifax.com">www.equifax.com</a> | <a href="http://www.experian.com">www.experian.com</a> | <a href="http://www.transunion.com">www.transunion.com</a> |
| P.O. Box 740241                                      | P.O. Box 4500  | 2 Baldwin Place  |
| Atlanta, GA 30374                                    | Allen, TX 75013  | P.O. Box 1000  |
|  |  | Chester, PA 19016  |

- **Consider Placing a Fraud Alert on Your Credit Report**

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>.

- **Identity Theft Protection Services**

In addition, the Company has arranged with Guardian Identity Theft Protection Program to provide you with identity theft protection services for one year, at no cost to you. The Theft Protection Program package provides you with the following benefits:

- Unlimited Recovery
- Unlimited Restoration
- \$25,000 Insurance via AIG

*To take advantage of this offer, you must enroll within 30 days from receipt of this letter.*

To enroll, send an email to [importantinfo@myrxvalet.com](mailto:importantinfo@myrxvalet.com). Provide your name, email, and phone number and tell us you want Guardian Protection. We will enroll you in the program for one year at no charge to you.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

## **OTHER IMPORTANT INFORMATION**

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift, or remove the security freeze.