

# Morgan Lewis

**Reece Hirsch**

Partner

+1.415.442.1422

Reece.hirsch@morganlewis.com

October 30, 2017

NH Department of Justice  
Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Breach

Dear Mr. Attorney General,

We are contacting you on behalf of our client Shop-Rite Supermarkets, Inc. to inform you of a security breach pursuant to N.H. Rev. Stat. § 359-C:20. This breach may have implications for two (2) New Hampshire residents. Enclosed, please find a sample copy of the notice that was sent to affected individuals on October 12, 2017.

On August 19, 2017, ShopRite learned that the pharmacy located in the ShopRite of Kingston, NY experienced a data security incident involving the loss of personal and medical information. A device used in the pharmacy to capture customer signatures was inadvertently disposed of in February 2016.

Customers who had prescriptions filled at the pharmacy located in the ShopRite of Kingston, NY between 2005 and 2015 signed this device to confirm acknowledgment of our privacy policy and payment by their insurance provider (if applicable). The personal and medical information included name, number, date of birth, prescription number, medication name, date and time of pick-up or delivery, signature, and zip code. These pharmacy customers were notified directly by ShopRite via U.S. Mail on October 12, 2017.

In addition, customers who purchased an over-the-counter product containing pseudoephedrine ("PSE"), such as certain cold or nasal medications, at the pharmacy located in ShopRite of Kingston, NY had personal and medical information stored on this device in order to meet legal requirements regarding PSE sales. The personal and medical information included name, driver's license number, zip code, and product purchased. ShopRite has provided conspicuous notice in major statewide media in order to reach these PSE customers, which ShopRite is unable to contact directly due to insufficient contact information.

It's important to note that Social Security numbers and debit and credit card information were not stored on this device.

DB2/ 32090553.5

**Morgan, Lewis & Bockius LLP**

101 Park Avenue  
New York, NY 10178-0060  
United States

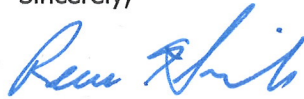
T +1.212.309.6000  
F +1.212.309.6001

October 30, 2017  
Page 2

ShopRite takes the protection of patient personal and medical information very seriously. We regularly review our systems and privacy and security practices to enhance those protections. In response to this incident, ShopRite is taking steps to prevent recurrence of similar incidents. We are providing supplemental privacy and security training for pharmacy staff and strengthening our security policies and practices relating to the appropriate removal of data from, and disposal of, computers and devices.

If you have any questions regarding this incident or if you desire further information or assistance, please contact Reece Hirsch at [reece.hirsch@morganlewis.com](mailto:reece.hirsch@morganlewis.com) or (415) 442 - 1422.

Sincerely,



Reece Hirsch

Enclosure

ShopRite Supermarkets, Inc.  
176 N. Main St.  
Florida, NY 10921



October 10, 2017

Via First Class, U.S. Mail

Re: Notification of Potential Breach Involving Personal Information of ShopRite of [REDACTED] Customers

Dear [REDACTED]:

As a valued customer of the pharmacy located in the ShopRite of [REDACTED], we are writing to make you aware of a data security incident involving your personal information that came to our attention on August 19, 2017. Although we have no reason to believe that your personal information has been accessed or misused in any way, we are writing to make you aware of the incident so that you may take any necessary precautions.

Our records indicate that you had a prescription filled at the pharmacy at the ShopRite of [REDACTED] store between 2005 and 2015. During your transaction, you signed a device that captured your signature confirming your acknowledgement of our privacy policy and payment by your insurance provider (if applicable). It was recently discovered that this device was inadvertently disposed of in February 2016.

As part of our investigation, we can confirm that the personal information stored on this device included your name, phone number, date of birth, prescription number, medication name, date and time of pick-up or delivery, signature, and zip code. ***It is important to note that your social security number and debit and credit card information were not stored on this device.***

ShopRite takes the protection of your personal and medical information very seriously. We regularly review our systems and privacy and security practices to enhance those protections.

In response to this incident, ShopRite is taking steps to prevent recurrence of similar incidents. We are providing supplemental privacy and security training for pharmacy staff and strengthening our security policies relating to the appropriate removal of data from, and disposal of, computers and devices.

We sincerely regret any inconvenience or concern caused by this incident. Although we are not aware that your information has been compromised and the risk of potential exposure is low, we want to make you aware of resources you may access to help safeguard your personal information. We have included additional information on identity protection and fraud prevention following the signature line of this letter.

If you have questions or concerns about this incident, please contact customer care at **1-800-954-5210**, Monday-Friday 9 a.m. to 5 p.m. EST or visit <http://facts.wakefern.com>

Very truly yours,

Brett Wing  
President & COO

## **Identity Protection and Fraud Prevention Tips**

We recommend that you consider taking steps to protect yourself from medical identity theft. Medical identity theft occurs when someone uses an individual's name, and sometimes other identifying information, without the individual's knowledge to obtain medical services or products, or to fraudulently bill for medical services that have not been provided. We suggest that you regularly review the explanation of benefits statements that you receive from your health plan. If you see any service that you did not receive, contact the health plan at the number on the statement.

Additionally, we recommend that you monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. You may also want to consider obtaining a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling 1-877-322-8228, or by completing an Annual Credit 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 [www.annualcreditreport.com/manualRequestForm.action](http://www.annualcreditreport.com/manualRequestForm.action).

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies listed below:

**Equifax**  
1-866-640-2273  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

**Experian**  
1-888-397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 2002  
Allen, TX 75013

**TransUnion**  
1-855-681-3196  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 2000  
Chester, PA 19016

You may also choose to contact the three national credit reporting agencies listed above for information about placing a "fraud alert" and/or a "security freeze" on your credit report to further detect any possible misuse of your personal information. Contact the Federal Trade Commission for additional information about "fraud alerts" and "security freezes," and about how to monitor and protect your credit and finances.

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, D.C. 20580  
(202) 326-2222  
[www.ftc.gov](http://www.ftc.gov)