ALSTON&BIRD LLP

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404

202-239-3300
Fax: 202-654-4970
www.alston.com

RECEIVED
15 SEP 11 AM 10: 25
CONSUMER PROTECTION DIV.

Kimberly K. Peretti

Direct Dial: 202-239-3720

Email: kimberly.peretti@alston.com

September 10, 2015

CONFIDENTIAL
VIA OVERNIGHT DELIVERY

Office of the Attorney General
Consumer Protection Division
1305 E. Walnut St.
Des Moines, IA 50319

Re: Notice Pursuant to Iowa Code Ann. § 715C.2

To the Office of the Attorney General:

I am writing on behalf of our client, CVS Pharmacy, Inc. ("CVS"), to inform you of an incident at its independent vendor, PNI Digital Media ("PNI"), that may have involved the personal information of Iowa residents that used CVSPhoto.com. CVSPhoto.com is a part of CVS's Retail Pharmacy Segment that affords online photo finishing services to customers.

In July 2015, CVS learned of reports of unusual activity involving payment cards used on the CVSPhoto.com website, which is managed and hosted by PNI. CVS promptly disabled the CVSPhoto.com website to try to mitigate any potential loss of customer data and is not currently accepting online payments through that site. CVS also began working with PNI to investigate the reports of unusual activity. CVS is working diligently to re-launch the website, including conducting a comprehensive review of the security practices for the vendor who will host the service going forward. CVS continues to investigate the matter, working with PNI and experienced forensic investigators.

On August 13, 2015, investigators informed CVS that, between June 2014 and July 2015, there was an illegal intrusion into PNI's systems that host the CVSPhoto.com website. The intrusion potentially resulted in the unauthorized acquisition of data entered by certain users on CVSPhoto.com. Based on the facts known to the company at this time, the potentially affected personal information may have included first and last name, payment card number, expiration date, card verification code, mailing address, phone number, email address, and username and password for logging in to a CVSPhoto.com account. At this time, there is no indication that the malware was designed to or did capture pin numbers or photographic images.

CVSPhoto.com and its online payment system are completely separate from CVS.com and the company's pharmacies. The incident occurred only within PNI's network. The incident did not impact financial transactions on CVS.com or in-store.

CVS has arranged for Experian to provide 12 months of credit monitoring and resolution of identity theft services to individuals who used their payment card on CVSPhoto.com between June 2014 and July 2015 at no cost to the individuals. Pursuant to Iowa Code Ann. § 715C.2, CVS is sending written notification to those customers. A copy of that notice is attached to this letter.

For some CVSPhoto.com customers, the only information potentially affected by this incident was their first and last name, phone number, email address, and username and password (if they logged in to a CVSPhoto.com account). These customers paid for their photos in a CVS/pharmacy retail store and did not enter their payment card information into the CVSPhoto.com site. For these customers, CVS is sending a courtesy communication with information on the incident. A copy of that communication is also attached to this letter.

If you have any other questions regarding this incident or if you desire further information or assistance, please email me at kimberly.peretti@alston.com or call my direct line at (202) 239-3720.

Sincerely,

Kimberly K. Peretti

CVSphoto.com

CVS Photo Customer Care
One CVS Drive
Mail Code – B120
Woonsocket, RI 002895

Engagement #: PC96513

September 11, 2015

Dear [INSERT First_Last_Name],

In July 2015, CVS Pharmacy, Inc. ("CVS") learned of reports of unusual activity involving payment cards used on the CVSPhoto.com website, which is managed and hosted by an independent vendor, PNI Digital Media ("PNI"). We promptly took down the website, and began working with PNI to investigate the reports. We continue to actively investigate the matter, working with PNI and experienced forensic investigators.

On August 13, 2015, investigators informed CVS that, between June 2014 and July 2015, there was an illegal intrusion into PNI's systems that host the CVSPhoto.com website. This intrusion potentially resulted in the unauthorized acquisition of data entered by certain users on CVSPhoto.com. Based on the facts known to the company at this time, the potentially affected personal information may have included your first and last name, payment card number, expiration date, card verification code, address, phone number, email address, and username and password for logging in to a CVSPhoto.com account. Importantly, at this time, there is no indication that the potentially affected information included pin numbers or photographic images.

We want to assure our customers that the CVSPhoto.com website and online payment system are completely separate from CVS.com and our pharmacies. **The incident occurred only within PNI's network**. The incident did not impact financial transactions on CVS.com or in-store.

What we are doing to protect you

We have arranged for customers who used a payment card on CVSPhoto.com between June 2014 and July 2015 to receive one year of free credit monitoring and resolution of identity theft through Experian's® ProtectMyID® Alert To sign up for ProtectMyID® Alert please call 1-888—829-6553 or visit http://www.protectmyid.com/alert. To obtain the free service, you must use the following unique Activation Code to sign up for ProtectMyID® Alert no later than December 31, 2015: [INSERT CODES FROM EXPERIAN]. If you sign up for ProtectMyID® Alert without using this Activation Code, you will have to pay for the service personally.

As explained above, CVS promptly disabled CVSPhoto.com to try to mitigate any potential loss of customer data. We are working diligently to re-launch the website, including reviewing the security practices for the vendor host. We have also advised the three major U.S. credit reporting agencies about this incident.

What you can do to protect yourself

Regardless of whether you take advantage of the identity theft protection and credit monitoring services available from Experian, please review the information in the enclosed Reference Guide to learn about additional steps you can take to monitor and protect against unauthorized use of your personal information.

Please remember that CVSPhoto.com will never ask you for personal or account information in an e-mail. Please exercise caution if you receive any emails or phone calls that ask for personal information or direct you to a web site where you are asked to provide personal information. We also recommend that you change your password on any other website or for any other systems where you use the same or a similar username and password combination. We encourage you to use a "strong" password that is different from your prior CVSPhoto.com password. According to the Federal Trade Commission, strong passwords tend to be long and include a mix of letters, numbers and characters.

What should I do if I have any questions?

After reviewing the Reference Guide, if you have any questions regarding this incident or if you desire further information or assistance, please call 1-888-829-6553 between 6 a.m. and 6 p.m. PST, Monday through Friday and between 8 a.m. and 5 p.m. PST, Saturday and Sunday.

Neal Baker, VP & Chief Privacy Officer - CVS Health

Reference Guide - U.S. State Notification Requirements

For additional information, please see our website, www.CVSPhoto.com, or contact us by phone at 1-888-829-6553.

For residents of *California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia*, and *Wyoming*:
It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account by contacting any one or more of the national consumer reporting agencies listed below. They can also provide you with additional information about fraud alerts and security freezes.

Equifax
P.O. Box 740241
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834-6790
1-877-322-8228
www.transunion.com

For residents of *Illinois* and *West Virginia*:

Information Regarding Placement of a Security Freeze on your Credit File

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *California, Iowa, Illinois, Maryland* and *North Carolina*:
State laws require us to tell you that you can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or security freeze). Your state also may offer guidance about how you can prevent or respond to identity theft. In particular, you may report instances of identity theft to your state's Attorney General or to your local police or sheriff's department. Contact information for some states appears below.

MD Attorney General's Office
Consumer Protection Division
200 St. Paul Place 9001
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

NC Attorney General's Office
Consumer Protection Division
Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
http://www.ncdoj.gov

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

Director of Consumer

California Attorney General's

Protection Division	**Office**
Iowa Attorney General 1305 E. Walnut Street Des Moines, IA 50319 Telephone: 515-281-5926 www.iowaattorneygeneral.gov	California Department of Justice Attn: Office of Privacy Protection P.O. Box 944255 Sacramento, CA 94244-2550 Telephone: (916) 322-3360 Toll-free in California: (800) 952-5225

For residents of *Massachusetts*:

Placing a Credit Freeze: Massachusetts law also allows consumers to place a security freeze on their credit reports. See the description above about what a security freeze does and how to order them. Under Massachusetts law, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

Obtaining Police Reports: You have a right to obtain a police report relating to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *West Virginia*: You may call us at 1-866-443-0933 to learn what types of information, if any, we maintain about you and other individuals.

For residents of *California* and *Wyoming*: This letter has not been delayed by a law enforcement investigation.

If you would like to view this email in your web browser click here

CVS Photo

CVS Photo Customer Care
One CVS Drive
Mail Code - B120
Woonsocket, RI 02895

Engagement #: PCCVS123

Subject: CVSPhoto.com Security Incident Update

Dear Valued CVS Photo Customer:

As you may be aware, CVS recently took down the CVSPhoto.com website after learning of reports of unusual activity involving the site. CVSPhoto.com is managed and hosted by an independent vendor, PNI Digital Media, and we have been actively working with PNI and experienced forensic investigators to investigate the reports.

Unfortunately, our investigators recently informed us that there was an illegal intrusion into PNI's systems that potentially resulted in the unauthorized acquisition of data entered by certain customers on CVSPhoto.com. The potentially affected information may have included your first and last name, phone number, email address, and username and password (if you logged in to a CVSPhoto.com account). We do want to highlight that there is no indication that the incident involved your photographic images.

We want to assure you that the CVSPhoto.com website is completely separate from CVS.com and our pharmacies. The incident occurred only within PNI's network. Additionally, any information that customers entered on CVS.com or provided at CVS/pharmacy retail locations was unaffected.

Please remember that CVSPhoto.com will never ask you for personal or account information in an e-mail. Please exercise caution if you receive any emails or phone calls that ask for personal information or direct you to a website where you are asked to provide personal information. If you had a registered account with CVSPhoto.com, then we also recommend that you change your password on any other website or for any other systems where you use the same or a similar username and password combination. We encourage you to use a "strong" password that is different from your prior CVSPhoto.com password. According to the Federal Trade Commission, strong passwords tend to be long and include a mix of letters, numbers and characters.

Nothing is more central to us than protecting the privacy and security of our customer information. If you have any questions regarding this incident or if you desire further information or assistance please call 1-888-829-6551 between 6 a.m. and 6 p.m. PST, Monday through Friday and between 8 a.m. and 5 p.m. PST, Saturday and Sunday.

Neal Baker, VP & Chief Privacy Officer

CVS Health