Schroeder, Chris N.

From: -Info-Consumer Protection
Sent: Wednesday, May 8, 2019 12:50 PM
To: Schroeder, Chris N.
Subject: FW: Incident Notice - N.D. Cent. Code §51-30-02
Attachments: ND Regulator Notice - 05082019.docx; ND Individual Notification Final 2019-05-03_19.docx

Jessica Seibel
Consumer Protection & Anti-trust Div
ND Attorney Generals Office
1050 E Interstate Ave Ste 200
Bismarck ND 58503-5574

(B) 701-328-3404
(F) 701-328-5568
(O) 800-472-2600 (ND only)

From: -Info-Attorney General <ndag@nd.gov>
Sent: Wednesday, May 8, 2019 11:39 AM
To: -Info-Consumer Protection <cpat@nd.gov>
Subject: FW: Incident Notice - N.D. Cent. Code §51-30-02

From: Dorazio, Jessica <DorazioJ1@aetna.com>
Sent: Wednesday, May 8, 2019 11:37 AM
To: -Info-Attorney General <ndag@nd.gov>
Subject: Incident Notice - N.D. Cent. Code §51-30-02

Good afternoon,

In accordance with N.D. Cent. Code §51-30-02, please see the attached incident notice and template member notification.

If you have any questions, please do not hesitate to contact us.

Thank you,
--Jessica Dorazio

JESSICA DORAZIO
Executive Director, Senior Counsel – Privacy & Security
☎ 860.273.4006 | C: 860.305.9867 I 151 Farmington Avenue, RE6A, Hartford, CT 06156

CVS pharmacy®
One CVS Drive
Woonsocket, RI 02895

VIA ELECTRONIC MAIL

May 8, 2019

Office of the North Dakota Attorney General
ndag@nd.gov

Re: Notice of Security Incident

Dear Office of the Attorney General,

CVS is writing to notify the Office of the Attorney General of a security incident that may have involved the personal information of 1,126 North Dakota residents.

CVS Health places a high priority on protecting the privacy and security of our customers' information and takes its responsibility to safeguard this information very seriously. We recently detected automated attempts to fraudulently log in to certain customer accounts on our retail web site (www.cvs.com), using customer credentials obtained from other sources (a practice known as "credential stuffing").

CVS's internal systems were not impacted by this incident. Instead, credential stuffing works when a person uses the same credentials (user name and password) across multiple web sites. When credentials are stolen from one web site, it provides an opportunity to gain access to other web sites where the same credentials are used.

On April 8, 2019, we determined that certain elements of personal information pertaining to North Dakota residents may have been obtained as a result of this activity.

The personal information that may have been obtained include first name, last name, date of birth, email address, and in some cases, ExtraCare® account number and/or the answer to account security questions (mother's maiden name, as an example). The incident did not involve Social Security numbers, full credit or debit card numbers, or bank account information.

Upon detection of the activity, we acted swiftly to reset the passwords of impacted accounts. We have taken steps on all of our web sites to further deter this type of activity. We are actively investigating this incident, and have notified and are working with law enforcement.

In accordance with our obligations under North Dakota law, CVS is sending written letter notifications to the impacted customers by first class U.S. mail. CVS will mail such notifications on May 8, 2019. A template copy of the notification that will be sent to the impacted customers is attached.

I want to assure you that CVS adheres to the highest of privacy standards. If you have any questions, you may contact me at 860-273-1091 and ScrabaT@aetna.com or by mail at 151 Farmington Avenue, RE6A, Hartford, CT 06156.

Sincerely,

Tracey E. Scraba
Chief Privacy Officer

CVS pharmacy®
One CVS Drive
Woonsocket, RI 02895

May 8, 2019

[First][Last]
[Address 1][Address 2]
[City],[State] [Zip]

Notice of Security Incident

Dear Valued Customer,

We are writing to share with you some important information regarding an incident that involved some of your personal information.

What Happened?

CVS Health places a high priority on protecting the privacy and security of our customers' information and takes its responsibility to safeguard this information very seriously. We recently detected automated attempts to fraudulently log in to certain customer accounts on our retail website (www.CVS.com), using customer credentials obtained from other sources (a practice known as "credential stuffing").

CVS's internal systems were not impacted by this incident. Instead, credential stuffing works when a person uses the same credentials (user name and password) across multiple web sites. When credentials are stolen from one web site, it provides an opportunity to gain access to other web sites where the same credentials are used.

On April 8, 2019, we determined that certain elements of personal information pertaining to North Dakota residents, including yourself, may have been obtained as a result of this activity.

What Information Was Involved?

The personal information that may have been obtained include your first name, last name, date of birth, email address, and in some cases, ExtraCare® account number and/or the answer to your account security question (mother's maiden name, as an example). The incident did not involve your Social Security number, full credit or debit card number, or bank account information.

What We Are Doing.

Upon detection of the activity, we acted swiftly to reset the passwords of impacted accounts. We have taken steps on all of our websites to further deter this type of activity. We are actively investigating this incident and have notified and are working with law enforcement.

What You Can Do.

When you log in to your CVS.com account, you may be prompted to change your password. You can also change your password by visiting www.cvs.com/reset and entering the email address that is associated with your CVS.com account, and we will send you a link to set your new password.

While your Social Security number and financial account information were not compromised, we nevertheless always encourage you to remain vigilant in monitoring your account statements and credit reports for incidents of unauthorized activity, and to promptly report such incidents.

Customers can also take steps to protect their online account information by not re-using the same password across multiple accounts. It is good practice for consumers to choose different account passwords for the various web sites they visit.

For more information on how to protect your personal information and online accounts, please visit https://www.consumer.ftc.gov/blog/2016/06/password-breaches-what-do.

Please know that we regret any inconvenience this event may cause you. If you have any additional questions regarding this notice, please call 800-399-4322, available 9:00 am to 8:00 pm EST, Monday – Friday.

Sincerely,

CVS/Pharmacy Privacy Office