Troutman Pepper Hamilton Sanders LLP
5 Park Plaza, Suite 1400
Irvine, CA 92614-2545

troutman.com

troutman pepper

Kamran Salour
kamran.salour@troutman.com

RECEIVED
AUG 08 2022
CONSUMER PROTECTION

August 4, 2022

OVERNIGHT MAIL

Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street Concord, NH 03301

To Whom It May Concern:

I write on behalf of my client, Community Surgical Supply Inc., located at 163 Rte 37 W, Toms River, New Jersey 08755 about a recent data security incident. Community Surgical provides home care equipment. This incident potentially impacted 122 New Hampshire residents. Notice of the incident will be sent to such residents via US mail on or about July 29, 2022, and a dedicated call center will be set up for impacted individuals to call should they have any questions or concerns.

Incident

On October 15, 2021, Community Surgical Supply Inc. learned of a data security incident that encrypted portions of our network. We immediately secured our digital environment and engaged a leading computer forensic firm and cybersecurity experts to investigate to determine what happened. The investigation revealed that an unauthorized party gained access to portions of our digital environment and accessed certain files and data stored in Community Surgical's digital environment. Community Surgical completed a comprehensive review of the data that could have potentially been accessed by the unauthorized party and, on July 1, 2022, determined that information some information of New Hampshire residents.

Potentially Impacted Information

While the information varies based on the individual at issue, the information involved consisted of first and last name, plus one or more of the following: address, first and last name, address and Social Security number. We have no indication that your information has been misused.

Remedial Steps

Once we became aware of the incident, we promptly took steps to determine the nature and scope. We also hired a leading forensic investigator to assist in our investigation. In addition, we are providing instructions to individuals on ways to protect their personal information. As an added safeguard, Community Surgical Supply Inc. is providing individuals whose Social Security Number or government identifiers (e.g., driver's license number) may have been impacted with complimentary credit monitoring services for a period of 12 months. Such services shall be provided by Equifax.

troutman pepper

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the contact information provided below.

Sincerely,

Kamran Salour
Direct: 949.622.2441
kamran.salour@troutman.com

COMMUNITY SURGICAL SUPPLY

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a recent data security incident we experienced that may have involved some of your information. This letter notifies you of the incident and informs you about steps you can take to help protect your personal information.

What Happened: On October 15, 2021, Community Surgical Supply Inc. experienced a data security incident that encrypted portions of our network. We immediately secured our digital environment and engaged a leading computer forensic firm and cybersecurity experts to investigate to determine what happened. The investigation revealed that an unauthorized party gained access to portions of our digital environment and accessed certain files and data stored in Community Surgical's digital environment.

What Information Was Involved: Community Surgical completed a comprehensive review of the data that could have potentially been accessed by the unauthorized party and, on July 1, 2022, determined that information included your: first and last name, address, Driver's license or other government identification number, passport number, Social Security number, or date of birth. **We have no indication that your information has been misused.**

[IF AG953 – General 12]
<<**What We Are Doing:** We are implementing additional technical security measures. And we are providing you with information about steps that you can take to help protect your personal information, including offering you complimentary identity protection services through Equifax that includes 12 months of credit monitoring.>>

[IF AG954 – General 24]
<< **What We Are Doing:** We are implementing additional technical security measures. And we are providing you with information about steps that you can take to help protect your personal information, including offering you complimentary identity protection services through Equifax that includes 24 months of credit monitoring.>>

What You Can Do: While we do not have any indication that you information has been misused, we advise you to remain vigilant for signs of unauthorized activity by reviewing your financial statements. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 877-607-3756 Monday through Friday between 9 a.m. to 9 p.m. Eastern Time.

The security of your information is a top priority for Community Surgical. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Community Surgical Supply

Additional 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, your state attorney general, and/or the Federal Trade Commission (FTC).

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

***Fraud Alerts*:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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.

Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

***Credit or Security Freezes*:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit.

How do I place a freeze on my credit reports? You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies identified above. In order 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

How do I lift a freeze from my credit reports? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

Additional Information for residents of the following states: You can obtain information for the offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take to prevent identity theft.

- **Colorado:** You may contact and obtain information from your state attorney general at: Colorado Attorney General's Office, Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203; 1-720-508-6000; www.coag.gov.
- **Illinois:** You may contact and obtain information from your state attorney general at: 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.
- **Maryland:** You may contact and obtain information from your state attorney general at: 200 Saint Paul St, Baltimore, MD 21202; (410) 576-6350; www.marylandattorneygeneral.gov.
- **North Carolina:** You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699; 1-919-716-6000 / 1-877-566-7226; www.ncdoj.gov.

- **New York:** For more information about preventing identity theft, you can visit New York Department of State Division of Consumer Protection: http://www.dos.ny.gov/consumerprotection or at:
    - New York State Division of Consumer Protection 123 William Street New York, NY 10038-38041 (800) 697-1220;
    - One Commerce Plaza 99 Washington Ave. Albany, NY 12231-0001
- **Washington DC:** You may contact and obtain information from your state attorney general at: Washington DC's Attorney General's Office, 441 4th St NW, Washington, DC 20001; (202) 727-3400; www.oag.dc.gov.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580; www.consumer.gov/idtheft; 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.
- **Obtaining a Free Credit Report:** You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to: Annual Credit Report Request Service, P.O. Box 1025281, Atlanta, GA 30348-5283.

EQUIFAX®

Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*