Corporate Office
99 Seaview Blvd., Port Washington, NY 11050
Toll Free: 877.224.0946 • 516.998.4600
www.drivemedical.com

17196

July [redacted], 2020

[redacted]
[redacted], Massachusetts [redacted]

NOTICE OF SECURITY INCIDENT

Dear [redacted],

We are writing regarding a cybersecurity incident that occurred at Drive Medical. We want to reinforce at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred.

WHAT INFORMATION WAS INVOLVED?

Depending on your relationship with us, the information involved may have included some combination of your name, Social Security number, bank account number, tax identification number and the amount of tax withheld, information you shared with us related to health conditions, and other information related to normal HR administration, including for payroll, benefits administration, and tax purposes. If you are a current or former employee, it may also have included any personal information you chose to save to the H:Drive.

WHAT WE ARE DOING

Our IT team took prompt steps to address this incident, including contacting law enforcement and engaging outside cybersecurity experts to help remediate and ensure the ongoing security of our systems.

As a current or former employee of Drive Medical or someone who has been designated as a beneficiary of a current or former employee's benefits, you will receive a complimentary two-year membership to Equifax Credit Watch Gold with Web Detect (U.S.), which helps detect misuse of your personal information and provides you with identity protection focused on identification and resolution of identity theft.

July [redacted], 2020
Activation Code: [redacted]
Expiration Date: January 31, 2021

Equifax® Credit Watch™ Gold with WebDetect Features

- Equifax® credit file monitoring and alerts to key changes to your Equifax credit report
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax credit report
- Internet Scanning[1] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Automatic Fraud Alerts[2] with a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Up to $25,000 Identity Theft Insurance[3]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

To sign up online for online delivery go to http://myservices.equifax.com/efx1_bresngis

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

00000003 00011 00002-00005

You need to activate your membership in order to receive your benefits, and must do so no later than **January 31, 2021 11:59pm ET. Your Activation Code will not work after this date.**

If you have questions about our provision of this complementary credit monitoring service to you, please contact Equifax at **844-959-0472.**

[1]Internet scanning, will scan for your Social Security number (if you choose to), up to 5 bank account numbers, up to 6 credit/debit card numbers you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to 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 Internet scanning is 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 made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

WHAT YOU CAN DO

We strongly encourage you to contact Equifax and take advantage of the credit monitoring and identity theft protection services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity, especially over the next 24 months.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

We take our responsibility to protect your information extremely seriously, and sincerely regret any inconvenience that this unfortunate incident has caused you. If you have any questions regarding this incident or the services available to you, please contact Equifax at **844-959-0472**.

Sincerely,

Nora Coleman
EVP, General Counsel
Medical Depot, Inc.

00000003 00011 00003-00005

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements 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 incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

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

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays 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.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report and obtain a copy of it.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

***

00000003 00011 00005-00005