Great Elm DME

"Where patients are our priority."

December 11, 2020

RE: Notice of Potential Breach of Personal Information

Dear Valued Customer:

This letter is being sent to you in order to notify you of a break-in at a United States Postal building in Arizona that may have involved theft of your checks to us and possibly Personal Health Information ("PHI"). This was a physical break-in and not a breach of our computer systems. Accordingly, limited information was taken. In accordance with Federal law, we are providing you this notification of a potential breach of your PHI. In addition to this individual notice, we will also provide notice to the Secretary of Health and Human Services.

What Happened

On Monday, November 23 (sometime between the night of November 20 and the morning of November 22), we discovered that over the previous weekend two of our post office boxes inside a United States Postal building had been broken into and certain items removed. Those items included incoming mail sent to Great Elm the previous days. The mail was last retrieved on the morning of November 20.

Generally, those post office boxes contain insurance and patient payments. We promptly filed a complaint with the United States Postmaster investigations unit. We are aware that the mail contained customer checks; but despite much research, we have been unable to identify specifically which customers' mail was received between November 20 (the last time the mail was retrieved) and November 23 (when we learned of the break-in). We are providing this notice to you because we value your business and want you to be able to take steps to protect your identity and personal information if affected. Most of you who are receiving this notification will not be directly affected by this incident.

What Information Was Involved

If your mail was among those stolen, the type of information that may have been taken would include:

- Information on your check, such as your name and address, the name of your bank, the name of our company, your routing and account number, and an authorized signature.
- An explanation of benefits, which may contain your name, insurance number, address, and date of birth.
- Patient payment that may include a coupon containing your name, address, and EMR system account number.

Great Elm DME

"Where patients are our priority."

What We Are Doing

We have been able to exclude many customers who do not send us checks through the mail or those whose checks were safely received on different days. We are diligently combing through our records and reaching out to third parties so that we can advise those affected. Again, most of you who are receiving this notification will not be directly affected by this incident. This will only affect those customers whose mail was in the incoming mail in the days leading up to November 23, 2020. If you would like to switch to electronic payments, please contact our billing office.

We have provided the following toll-free phone number 888-262-9945 and email address wecare@greatelmdme.com that you may contact to inquire whether your information may have been included in the breach. We have also posted a notice on the homepage of our website to inform you about the breach. The notice on our homepage and the toll-free phone number and email address will be available until April 1, 2020.

To further mitigate against this risk in the future, we have decided to begin using a new "Caller Service" offered by the post office at the affected locations. Caller Service offers an added level of security and protection because mail is collected at the post office call window or loading dock as opposed to being stored in a post office box. This service offered by the post office adds enhanced security for sensitive items such as checks and documents containing personal information.

What You Can Do

You can help us determine if your check has been stolen. If you mailed a check to us in the days leading up to November 23, 2020, we strongly recommend that you do the following:

1. Check your bank activity online or by telephone to determine the status of your check.
2. Contact our billing department at 888-262-9945 or wecare@greatelmdme.com to determine if we received your check.
3. If you believe the check may have been cashed by another party fraudulently, contact your bank and explain what happened. They will return the funds to your account.
4. Monitor your account closely for further fraudulent activity. Your bank or credit union may advise you to shut down the account on which the check was written and open a new one.
5. If your check remains uncashed and was mailed just prior to November 23, 2020, please stop payment on the check.

At Great Elm DME, Inc., we are deeply invested in securing the confidentiality of your information and sincerely apologize for this event and its aftereffects. The breach of information caused by this break-in was very upsetting and disturbing to us. We are dedicated to mitigating any adverse effects that this unfortunate break-in has or may have on you by providing this notice and the enclosed information from various private and government authorities on steps you can take to protect your information.

Great Elm DME

"Where patients are our priority."

Additionally, as mentioned above, we have decided to start using a "Caller Service" at the post office location where the break-in occurred in order to ensure greater security for customer mail.

If we determine that your check is involved, we will contact you as soon as we can. If you believe that you have been affected, please contact us immediately at 888-262-9945 or wecare@greatelmdme.com and you will be connected to our billing department. Please be assured that we are taking appropriate steps to ensure secure payment-by-mail methods for our customers and will work with you to establish electronic-payment methods if you desire to do so.

We look forward to continuing to serve your needs.

Sincerely,

David Derminio

David Derminio, President & COO

RESOURCES

What to do if your personal information may have fallen victim to identity theft and/or fraud.

From The Federal Trade Commission: The Federal Trade Commission has online resources and guides that can help advise you about how to protect your identity and personal information. The Federal Trade Commission created this booklet with helpful information and forms that consumers can use to notify credit bureaus about a potential identity theft: https://www.azag.gov/sites/default/files/docs/consumer/identity-theft/identity-theft-taking-charge.pdf.

The Federal Trade Commission can be reached toll-free at 1-877-382-4357. The Federal Trade Commission's address is 600 Pennsylvania Avenue, NW, Washington, DC 20580. The Federal Trade Commission website is: https://www.ftc.gov/

From The Arizona Attorney General: If your personal information has been involved in a data breach, you might want to take steps to protect yourself from identity theft and other forms of fraud. For example, you might consider placing a free "security freeze" or "fraud alert" on your credit reports with consumer reporting agencies, and you can request one free credit report from those agencies each year to monitor any potentially fraudulent activity. For more information, you can visit the "Identity Theft" section of this website, and additional resources are available at https://www.consumer.ftc.gov/ and https://www.identitytheft.gov/

You may consider placing a freeze on your credit reports: You must contact each consumer reporting agency with which you want to place or lift a freeze. Placing or lifting a freeze with one agency will not necessarily place or lift a freeze at any other agency.

Information about placing or lifting freezes with each of the three largest consumer reporting agencies can be found at:
Equifax: Equifax Disclosure Department, P.O. Box 740241, Atlanta, GA 30374
www.Equifax.com/personal/credit-report-services
800-685-1111
Experian: Experian National Consumer Assistance Center, P.O. Box 4500, Allen, Tx 75013
www.experian.com/freeze/center.html
888-EXPERIAN (888-397-3742)
Transunion: TransUnion LLC Consumer Disclosure Center, P.O. Box 1000 Chester, PA 19016
www.TransUnion.com/credit-freeze
888-909-8872
Consumers can also place a credit freeze with the National Consumer Telecom & Utilities Exchange (NCTUE), which is a consumer reporting agency used by many telecom companies and utilities to check credit history before opening new accounts. Information about placing a freeze with the NCTUE can be found at www.nctue.com/Consumers

You may consider placing a fraud alert on your credit reports: There are three types of fraud alerts available:

- Fraud Alert. If you're concerned about identity theft, but haven't yet become a victim, this fraud alert will protect your credit from unverified access for one year. You may want to place a fraud alert on your file if your wallet, Social Security card, or other personal or financial account information is lost or stolen.
- Extended Fraud Alert. For victims of identity theft, an extended fraud alert will protect your credit for seven years.
- Active Duty Military Alert. For those in the military who want to protect their credit while deployed, this fraud alert lasts for one year and can be renewed for the length of deployment. The consumer reporting agencies will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to do so.

To place a fraud alert on your credit reports, contact one of the three largest consumer reporting agencies. The agency you contact must tell the other agencies, and all three will place an alert on their versions of your report. This is different from placing or lifting a credit freeze, which requires that you contact each agency individually.
You can place a fraud alert with Experian. On its website, Experian states:

Add a fraud alert message to your credit report if you suspect that your identification information has been or could be used fraudulently. A fraud alert notifies potential credit grantors to verify your identity before extending credit in your name in case someone is using your information without your consent.
You can place a fraud alert with Experian online at: https://www.experian.com/fraud/center.html