



July 28, 2023

attorneygeneral@doj.nh.gov  
NH Department of Justice  
33 Capitol Street  
Concord, NH 03301

Re: Elgon, Inc. – Data Incident  
Our File No. 41088-00231

Dear Sir or Madam:

We are writing to notify you of a data security incident involving 3 New Hampshire residents. We are submitting this notice on behalf of our client, Elgon, Inc. (“Elgon”). Elgon provides a cloud-based integrated home health management system to medical providers.

### **Nature Of The Security Breach**

On approximately April 3, 2023, Elgon became aware that certain computer systems in its environment were inaccessible as a result of malicious file encryption. Elgon immediately launched an extensive investigation, aided by third party computer forensic specialists, to determine the nature and scope of the event and worked quickly to secure its systems, restore access to the information and investigate what happened and whether this resulted in any unauthorized access to information by any unknown actor. Through Elgon’s investigation, Elgon determined that an unknown actor gained access to a limited number of its systems and certain files in those systems were accessed and potentially downloaded by an unknown actor.

The clients<sup>1</sup> involved in this incident were forwarded letters notifying them of this incident. A copy of the form letter is attached hereto.

### **Steps Being Taken Related To The Incident**

Elgon took steps to address this incident promptly after it was discovered, including conducting an investigation to understand what had taken place and how. Elgon has secured their system and offices. Elgon has also reviewed their internal data management and protocols and have implemented enhanced security measures to help prevent this type of incident from recurring.

---

<sup>1</sup> The mailings were sent to those whom Elgon had consent from the medical providers.

In addition, Elgon is offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

Should you need additional information regarding this matter, kindly contact me.

Very truly yours,

*/s/ David J. Shannon*

DAVID J. SHANNON

DJS/kr

<<Date>>

Dear

Elgon Information Systems (“Elgon”) is writing to provide information regarding an event that involves certain information relating to your personal information. Although at this time, there is no indication that the information has been fraudulently misused in relation to this event, we are providing you with further information about the event, our response to it, and additional measures that may be taken to protect certain individuals’ information should you feel it is appropriate to so. We take this event very seriously and remain committed to safeguarding your organization’s information within our care.

### **What Happened**

On approximately April 3, 2023, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. We immediately launched an extensive investigation, aided by third party computer forensic specialists, to determine the nature and scope of the event and worked quickly to secure our systems, restore access to the information and investigate what happened and whether this resulted in any unauthorized access to information by any unknown actor. Through our investigation, we determined that an unknown actor gained access to a limited number of our systems and certain files in those systems were accessed and potentially downloaded by an unknown actor.

### **What Information Was Involved**

In an abundance of caution, we performed a comprehensive review of the contents of the affected systems to determine what information could be contained in the impacted files and to whom the information related. The review was recently completed. Although the investigation could not determine the specific files, at the time of the event, of certain individuals could have been stored within the impacted systems. To date, we have not received reports of any fraudulent misuse of any information potentially impacted by the event.

### **What We Are Doing**

We took steps to address this incident promptly after it was discovered, including conducting an internal investigation to understand what had taken place and how. We have also reviewed our internal data management and protocols and have implemented enhanced security measures to help prevent this type of incident from recurring.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: of credit and CyberScan

monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

**What You Can Do**

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN] or going to [URL] and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is [DATE].

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

**For More Information**

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call [PHONE] or go to [URL] for assistance or for any additional questions you may have.

Sincerely,

Elgon Information Systems  
(Enclosure)

CONFIDENTIAL



## Recommended Steps to help Protect your Information

**1. Website and Enrollment.** Go to \_\_\_\_\_ and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at \_\_\_\_\_ to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive

confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 1-877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 1-401-274-4400. One Rhode Island resident was affected.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.