

Stanley J. Reed
Attorney
301-657-0177 (Phone)
301-347-1796 (Fax)
sjreed@lerchearly.com

April 29, 2024

VIA EMAIL

Maryland Attorney General's Office
Attn: Security Breach Notification
idtheft@oag.state.md.us
200 St. Paul Place, 25th Floor
Baltimore, MD 21202

Re: Data Breach Notification

To Whom It May Concern:

Pursuant to the requirements of the Maryland Personal Information Protection Act ("MPIPA"), I am writing to follow-up my telephone conversation of several weeks ago with Jeff Karberg, in which I reported a data security breach at my law firm, Lerch Early & Brewer Chtd. (the "Firm"). I am the Firm's general counsel and I have been involved in addressing and remediating the issues arising from that breach.

Briefly put, the Firm's affected clients are [REDACTED], for whom the Firm provides estate planning legal services. The Firm prepared a thumb drive containing PDFs of the [REDACTED] estate planning documents, and at their express request, placed the drive in a sealed envelope and mailed it to them via USPS on March 28, 2024. Due to a miscommunication with the Firm's IT specialists, the thumb drive was not encrypted.

On April 6, 2024, the [REDACTED] notified the Firm that when the envelope arrived at their home, it appeared to have been torn open and the thumb drive was missing. The personal information elements contained within the estate planning documents on the thumb drive, which may have been exposed to an unauthorized person in this incident, include the [REDACTED] names, addresses, telephone numbers, dates of birth, and social security numbers.

Upon learning of this potential data breach, we immediately advised [REDACTED] to place a fraud alert on their credit files. We have followed up with a letter to the [REDACTED] a copy of which is attached. As you will note, we also have offered to provide [REDACTED] at the Firm's expense, with LifeLock protection for two years. To date, [REDACTED] have reported no issues or problems with their credit.

Since December 2023, the firm has had in effect a Privacy Breach Response Plan (the “Plan”), copy of which is also attached. In light of the circumstances surrounding this incident, the Plan is in the process of being revised to require that all thumb drives containing client specific information must be encrypted, and instructions have been provided to our IT personnel to ensure that is being done.

I believe that this letter satisfies the notice requirements of the MPIPA. Please contact me if you have any further questions, or need additional information.

Very truly yours,

Stanley J. Reed

cc: David H. Anderson, COO

Enclosures

SJR/ram

Amanda Sauer McGrath
301-657-0737
acsauer@lerchearly.com

April 23, 2024

VIA Regular Mail and email to: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Re: Data Breach Notification

Dear [REDACTED]:

We are writing to follow-up on our prior communication with you regarding a recent data breach incident at Lerch, Early & Brewer (the "Firm"). This notification is sent pursuant to Maryland law requiring us to notify you in the event your personal information may be compromised.

As I have previously explained to you, we prepared a thumb drive containing PDFs of your estate planning documents and, upon your request, placed the drive in a sealed envelope and mailed it to you via USPS on March 28, 2024. Due to a miscommunication with our IT specialists in the Firm, the thumb-drive was not encrypted. You notified us on April 6, 2024 that when the envelope arrived at your home, the envelope appeared to have been torn open and the thumb-drive was missing. The personal information elements contained within the estate planning documents that were saved on the thumb drive which may have been exposed to an unauthorized person in this incident include your names, addresses, telephone numbers, dates of birth, and social security numbers.

To protect yourself from the possibility of identity theft, we strongly recommend that you immediately place a fraud alert on your credit files, if you have not already done so. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the credit card company or lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to obtain new credit.

An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, you must contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will

then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

Equifax (888)766-0008 or www.fraudalert.equifax.com
Experian (888) 397-3742 or www.experian.com
TransUnion (800) 680-7289 or www.transunion.com

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant, and regularly review your credit reports from each of the three major credit reporting agencies.

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: <https://consumer.ftc.gov/> and mailing to:

Annual Credit Report Request Service
P.O. Box 1025281
Atlanta, GA 30348-5283

We also recommend that you subscribe to LifeLock for two years, at the Firm's expense. LifeLock is a software company, which works to detect and prevent identity theft. The cost of LifeLock's Ultimate LifeLock Plus protection for two years for both of you is \$1,075.87. If you choose to use this service, please send the Firm your paid invoice and we will reimburse you fully.

You also may obtain information from the Maryland Office of the Attorney General and the U.S. Federal Trade Commission about steps you can take to avoid identity theft. You may contact the Maryland Attorney General and the U.S. Federal Trade Commission at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023
410-576-6300
www.oag.state.md.us

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
202-326-2222
877-382-4357
www.consumer.ftc.gov
www.identitytheft.gov

The Firm takes its responsibility to safeguard personal information seriously. We are very sorry this incident occurred, and regret any inconvenience or concern this may have caused you. Please be assured that the Firm remains committed to protecting the privacy and security of personal information, and has taken appropriate steps to prevent any reoccurrence of the issue you experienced.

If there is anything we can do to further assist you, please call do not hesitate to contact me.

Sincerely yours,

A handwritten signature in blue ink that reads "Amanda McGrath". The signature is fluid and cursive.

Amanda Sauer McGrath

Privacy Breach Response Plan

Effective 12/2023

Introduction

This Privacy Breach Response Plan establishes a clear and comprehensive framework for addressing and mitigating privacy breaches within Lerch, Early & Brewer (the “Firm”). This plan applies to all employees, contractors, and third-party entities that handle personal information on behalf of the firm.

Breach Identification and Assessment

1. Initial Identification

A privacy breach, in the context of the Privacy Breach Response Plan, refers to the unauthorized access, disclosure, or acquisition of personal or sensitive information that compromises the privacy and confidentiality of the Firm’s clients or employees or other persons whose information is maintained in the firm’s custody or control. A privacy breach can involve information stored in electronic or physical formats.

2. Reporting

The Firm’s employees should report any potential privacy breach to the Chief Operating Officer. He or she will conduct an initial assessment and determine what other parties and resources need to take further action.

3. Incident Response Team

If a privacy breach occurs, an incident response team is responsible for implementing the breach response plan. The team will consist of the following individuals, each acting appropriate to their respective job roles.

- Chief Operating Officer
- Director of Marketing and Communications
- Director of Information Technology
- Director of Human Resources

The initial tasks of the Incident Response Team are to:

- Identify and confirm the occurrence of a privacy breach; and
- Determine the scope and nature of the breach, including the number of affected parties, the information compromised and the extent of the impact.

4. Breach Response

Once a breach is confirmed, the Incident Response Team will take the following actions as appropriate to their job roles:



2. Engage external cybersecurity experts, legal counsel, or forensic investigators, if necessary.

2. Remediation and Mitigation

The Incident Response Team will implement an appropriate remediation and mitigation plan including:

- a. Develop a plan to remediate the impact on affected parties.
- b. Provide support services as needed, such as credit monitoring or identity theft protection.
- c. Identify and address the security vulnerabilities that led to the breach.
- d. Implement measures to prevent future breaches.
- e. Conduct regular security assessments and audits.
- f. Update policies and procedures based on lessons learned.

3. Post-Incident Review

Following the conclusion of remediation and mitigation, the Incident Response Team will conduct a post-incident review to identify lessons learned and areas for improvement. Areas for improvement should be included in future revisions of this policy and privacy breach plans.

4. Training and Awareness

Employees will receive regular training on privacy and security best practices, handling and safeguarding sensitive information, and reporting suspicious activities or potential breaches promptly.

5. Compliance Monitoring

The firm will conduct periodic audits to ensure ongoing compliance with Maryland PIPA and modify its policy and plans based on changes in laws and regulations.