

July 15, 2026

<<Name>>

<<Address>>

<<City>>, <<State>> <<Zip>>

Re: NOTICE OF DATA SECURITY INCIDENT

Dear <<Name>>:

We are writing to inform you of a data security incident that may have involved some of your personal information. Protecting the privacy and security of personal information is a responsibility we take seriously, and we regret any concern this incident may cause.

What Happened

On June 2, 2026, SOC was alerted to suspicious activity involving unauthorized access to a single company email account. Upon investigation, SOC determined that the incident was isolated to the affected email account and found no evidence that any other company systems or accounts were impacted. However, SOC cannot rule out the possibility that information contained within the account may have been accessed or compromised.

What Information Was Involved

Our review determined that the affected information may have included your:

- First name and last name
- <<Data Element Impacted>>
- <<Data Element Impacted>>
- <<Data Element Impacted>>
- <<Data Element Impacted>>
- <<Data Element Impacted>>
- <<Data Element Impacted>>

What We Are Doing

Immediately upon discovering the incident, we took steps to contain and remediate the issue, including:

- Securing the affected email account;
- Conducting a forensic investigation with our cybersecurity team;
- Reviewing potentially affected information; and
- Reinforcing employee security awareness and training.

We continue to evaluate our security controls and make improvements where appropriate.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits statements, and credit reports for suspicious activity.

As a precaution, you may wish to:

Monitor Your Accounts

Carefully review bank accounts, credit card statements, medical benefit statements, and other financial accounts for unauthorized activity.

Credit Monitoring and Obtaining your Reports

As a Massachusetts resident, you are entitled to eighteen (18) months of credit monitoring services at no cost to you. You may select a credit monitoring service of your choice and submit documentation of your enrollment and payment to Day & Zimmermann for reimbursement. You may also obtain a free copy of your credit report from each of the three nationwide credit reporting agencies through:

www.annualcreditreport.com

or by calling:

1-877-322-8228

Consider a Fraud Alert or Security Freeze

A fraud alert notifies creditors to take additional steps to verify your identity before opening new accounts. Additionally, a security freeze restricts access to your credit report and can help prevent unauthorized accounts from being opened in your name. To place a fraud alert or security freeze at no cost to you, contact one of the three major credit bureaus listed below. You may be asked to provide personal information to verify your identity.

Equifax www.equifax.com 1-800-525-6285

Experian www.experian.com 1-888-397-3742

TransUnion www.transunion.com 1-800-680-7289

Monitor Medical and Government Records

Because the affected information may include medical and government-issued identification information, we recommend reviewing any healthcare statements, insurance records, passport records, and immigration-related documentation for unusual activity.

Report Suspicious Activity

If you detect suspicious activity or believe you are the victim of identity theft, contact your financial institution or the Federal Trade Commission (FTC). You have the right to file or obtain a police report with your local law enforcement agency.

FTC Identity Theft Resources:

www.identitytheft.gov

1-877-438-4338

For More Information

If you have questions regarding this incident, please contact:

Day & Zimmermann

(267) 804-5322

Privacy@dayzim.com

1835 Market St.

Philadelphia, PA 19103