

Dear Director Jeff Karberg:

On behalf of my client, Siden & Associates, P.C. ("Siden Law"), a small law firm located in Boston, Massachusetts, I am writing to notify the Maryland Attorney General's Office of a data breach. On or about July 25, 2023, Siden Law became aware that it was experiencing a cybersecurity incident. Upon discovering this incident, Siden Law took immediate action to secure its network, reported it to federal law enforcement, and retained the services of third-party cybersecurity experts to conduct a comprehensive investigation. As a result of that investigation, Siden Law learned that from on or about July 17, 2023 through July 25, 2023, unauthorized person(s) had unlawfully obtained access to its network. This included two MD residents. Notifications will be mailed to these residents on October 6, 2023.

Siden Law has also taken measures to further strengthen its network to prevent incidents like this in the future. For instance, they disabled the affected accounts, rebuilt the affected systems, reset all domain and email passwords across its entire network, and enhanced its firewalls and hardened its network environment. They also terminated its information security provider as they learned that he was not providing the services that he was retained to perform. Siden Law has retained the services of a new managed services provider.

In an abundance of caution and to protect the MD residents from identity theft, Siden Law is providing all MD residents 24 months of Experian IdentityWorks, a credit monitoring/identity protection service. Attached is a copy of the breach notification letters that will be mailed to the affected persons tomorrow, October 6, 2023.

Please feel free to contact me with any questions.

Best regards,
Stephanie

B. Stephanie Siegmann

Partner

Hinckley Allen
28 State Street
Boston, MA 02109-1775
o: 617-378-4181 | c: 617-320-5045
ssiegmann@hinckleyallen.com
[LinkedIn B. Stephanie Siegmann](#)

SIDEN & ASSOCIATES, P.C.

Return Mail Processing
PO Box 589
Clasburg, PA 16625-0589

K1308-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



October 6, 2023

Re: Notice of Data Breach

Dear Sample A. Sample:

Siden & Associates, P.C. ("Siden Law" or "we") is writing to notify you of a recent data security incident that may have affected the security of your personal information. We take the protection of your information very seriously and are contacting you directly to provide you with information about the incident, steps we are taking in response, credit monitoring services and identity protection resources we are making available to you, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? We discovered that from on or about July 17, 2023 through July 25, 2023, unauthorized person(s) had unlawfully obtained access to our network. Upon discovering this incident, we took immediate action to secure our network and began an investigation to understand the full scope of the incident. We also reported this incident to federal law enforcement.

What Information was Involved? At the time of the data security incident, our network contained personal information of some individuals, which may have been accessed and acquired by unauthorized person(s). The personal information included first and last name combined with [REDACTED], [REDACTED].

What Are We Doing? We take this incident and the security of your personal information very seriously. Upon discovering this incident, we immediately took steps to restore the security of our network and launched an investigation with the assistance of third-party cybersecurity experts. We have also taken measures to further strengthen our network to prevent incidents like this in the future. For instance, we disabled the affected accounts, rebuilt the affected systems, reset all domain and email passwords across our entire network, installed a world-class endpoint detection and response system, and enhanced our firewalls and hardened our network environment. We also terminated our information technology services provider and retained the services of a new managed services provider.

As described below, for your protection and as a precautionary measure, we are providing you with access to single bureau credit monitoring services at no charge for a period of 24 months. Also, we have detailed in the attachment to this letter entitled "Information About Identity Theft Protection" steps you can take to protect yourself from identity theft and protect your personal information.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

0000002



K1308-L02

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by January 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by January 31, 2024. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Please review the enclosed *Information about Identity Theft Protection* for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call [REDACTED] toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number [REDACTED].

If you would like to speak to someone at Siden Law to discuss this incident, please email us at [REDACTED] or call [REDACTED]

Sincerely,



Ryan Siden
Managing Partner

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed here:

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-916-8800
www.transunion.com

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

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed here:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-525-6285
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

0000002



Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

Additional Information

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and immediately report any suspicious activity or suspected identity theft to us and the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC).

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: **Maryland Office of the Attorney General**, Consumer Protection Division, 200 St. Paul Place, Baltimore MD 21202, 1-888-743-0023, www.marylandattorneygeneral.gov/pages/identitytheft/

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 receive; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, D.C. 20552.

For resident of New York: You may obtain information about identity theft prevention and protection from:

New York Attorney General
Consumer Frauds & Protection Bureau
The Capitol
Albany, NY 12224-0341
(800) 771-7755

<https://ag.ny.gov/bureau/consumer-frauds-bureau>

New York Department of State
Division of Consumer Protection
99 Washington Ave., Suite 650
Albany, NY 12231
(800) 697-1220

www.dos.ny.gov

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: **North Carolina Attorney General's Office**, Consumer Protection Division, 9001 Mail Service Center, Raleigh N.C. 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400. There were three Rhode Island residents impacted by this incident.