

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

Julie Siebert-Johnson
jsjohnson@c-wlaw.com

Sam Son
yson@c-wlaw.com

March 12, 2025

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Notice of Data Event

To Whom It May Concern:

We represent The Seltzer Firm, located at 37 West 20th Street, Suite 901, New York, NY 10011, and write to notify you of a recent data security event involving The Seltzer Firm and one (1) Maryland resident affiliated with one of The Seltzer Firm's clients, The University of Texas MD Anderson Cancer Center. By providing this notice, The Seltzer Firm does not waive any rights or defenses under Maryland law, including the Maryland data breach notification statute. This notice may be supplemented should additional relevant facts be determined.

On December 14, 2024, The Seltzer Firm identified suspicious activity on its computer network and quickly engaged third-party specialists to investigate and determine the nature and scope of the activity. After significant efforts by all involved, the investigation determined that as part of the activity, certain information housed on a single system within its network may have been accessed or downloaded without authorization between December 10, 2024 and December 14, 2024. After the scope of the unauthorized activity was confirmed, The Seltzer Firm conducted a diligent review of the relevant information to determine the types of information contained therein and to whom the information related to assess potential notification obligations. Once the preliminary information was confirmed on January 25, 2025, The Seltzer Firm thereafter worked to align resources and further prepare to provide notification, after which, on February 4, 2025, The Seltzer Firm promptly notified The University of Texas MD Anderson Cancer Center, the data owner, for necessary confirmation and approval to provide notification on its behalf.

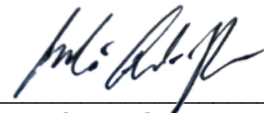
On February 17, 2025, The University of Texas MD Anderson Cancer Center provided the necessary information and authorization, and The Seltzer Firm thereafter worked to provide notification as quickly as possible. On March 12, 2025, on behalf of The University of Texas MD Anderson Cancer Center, The Seltzer Firm began providing written notification to potentially impacted individuals, including one (1) Maryland resident affiliated with The University of Texas MD Anderson Cancer Center, with access to complimentary credit/identity monitoring services. A representative copy of the notice is attached hereto as ***Exhibit A***.

As noted in the letter, the categories of information potentially impacted in connection with this matter varies by individual but may include name, Social Security number, driver's license number, date of birth, and/or passport number or other government-issued identification number, as applicable.

In response to this event, The Seltzer Firm took steps to secure its environment and conducted a comprehensive investigation, which was aided by third-party forensic specialists, into the activity. Once the information that may have been impacted was confirmed, The Seltzer Firm diligently reviewed the information and to whom it related in order to assess potential notification obligations, including working with involved entity clients, as necessary, to obtain information and authorization to act on their behalf. The Seltzer Firm also notified federal law enforcement regarding this matter. The obligation to safeguard information in its care is of paramount importance to The Seltzer Firm, and in response to this matter, The Seltzer Firm has taken steps to further enhance its existing cybersecurity infrastructure, as well as implemented additional policies and procedures to minimize the reoccurrence of future similar events.

Please contact me at jsjohnson@c-wlaw.com should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Julie Siebert-Johnson', written over a horizontal line.

Julie Siebert-Johnson

Exhibit A



March 12, 2025

[REDACTED]

The Seltzer Firm is writing to inform you of a recent data event that may affect certain information related to you. As you may recall, we were previously referred by [REDACTED] to provide immigration legal assistance and counsel to you/your family member, which therefore also included assistance for you. This letter includes information about the matter, our response, and resources we are making available to you on behalf of [REDACTED]

What Happened? On December 14, 2024, we first identified suspicious activity on our computer network and quickly engaged third-party computer specialists to investigate and determine the nature and scope of the activity. After significant efforts by all involved, the investigation determined that as part of the activity, certain information housed on a single system within our network may have been accessed or downloaded without authorization between December 10, and December 14, 2024. After the scope of the unauthorized activity was confirmed, we conducted a diligent review of the relevant information to determine the types of information contained therein and to whom the information related to assess potential notification obligations. This review completed on January 25, 2025, after which we promptly notified [REDACTED] on February 4, 2025 for necessary approval and contact information for you to issue this notification. On February 20, 2025, [REDACTED] provided the necessary information, and we thereafter worked to provide notification as quickly as possible.

What Information Was Involved? The categories of information potentially impacted in connection with this matter varies by individual but may include information collected in connection with the provision of legal services related to the immigration assistance we provided, including your name, Social Security number, driver's license number, date of birth, and/or passport number or other government-issued identification number, as applicable.

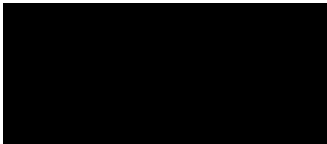
What We Are Doing. In response to this event, we took steps to secure our environment and conducted a comprehensive investigation, which was aided by third-party forensic specialists, into the activity. Once the information that may have been impacted was confirmed, we diligently reviewed the information and to whom it related in order to assess potential notification obligations. We also notified federal law enforcement regarding this matter. Nevertheless, the obligation to safeguard information in our care is of paramount importance to The Seltzer Firm, and in response to this matter, we have taken steps to further enhance our existing cybersecurity infrastructure, as well as implemented additional policies and procedures to minimize the reoccurrence of future similar events.

Additionally, out of an abundance of caution, on behalf of [REDACTED] we are offering you access to 12 months of credit monitoring and identity protection services through Cyberscout, a TransUnion company, at no cost to you. Please understand that due to privacy laws, neither The Seltzer Firm nor [REDACTED] are able to activate these services for you directly. Additional information regarding how to activate the complimentary monitoring service is in the “*Steps You Can Take to Help Protect Your Information*” section of the letter below.

What You Can Do. We recommend that you remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is recommended that you promptly contact your financial institution or credit/debit card company. Additionally, you can enroll to receive the complimentary credit monitoring and identity protection services we are making available to you. You can also review the enclosed “*Steps You Can Take to Help Protect Your Information*” for additional information and resources.

For More Information. We understand you may have additional questions about this matter. Should you have questions or concerns regarding this matter or offered monitoring service, please contact our dedicated assistance line through Cyberscout, a TransUnion company, at [REDACTED] which is available Monday to Friday between the hours of 8:00 a.m. and 8:00 p.m. Eastern Time.

Sincerely,



Suzanne B. Seltzer,
Principal
The Seltzer Firm

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Offered Monitoring Services

We are providing you with access to credit monitoring services at no charge. To enroll in the monitoring services, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to enroll in the offered monitoring services: [REDACTED]

Below please find descriptions of the offered services we are providing through Cyberscout, a TransUnion company.

- Credit Monitoring
 - o Provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. The alert will be sent to you the same day that the change or update takes place with the bureau.
- Identity Theft Insurance
 - o Enrolled individuals will have access to \$1,000,000 in insurance coverage to protect against potential damages related to identity theft and fraud.
 - o Available worldwide and includes coverage for identity theft expenses as well as unauthorized electronic fund transfer fraud.
- Fraud Remediation Services
 - o Access to team of dedicated specialists at Cyberscout, a TransUnion company, to help you in the event you experience fraud and assist with remediation.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. concerning identity theft, if you are a victim of identity theft. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency



00001020280000

P

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. The Seltzer Firm is located at 37 West 20th Street, 901 New York, NY 10011.

For 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents potentially impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.