EXHIBIT 1

We represent Lewis Baach Kaufmann Middlemiss PLLC ("LBKM") located at 1050 K Street, NW, Suite 400, Washington, DC 20001, and are writing to notify your office, on behalf of LBKM's clients and other relevant third parties, known as "relevant third parties," of an incident that may affect the security of certain personal information relating to two (2) Nebraska residents. By providing this notice, LBKM does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

LBKM is a law firm specializing in litigation, ADR, international disputes, and insurance and reinsurance coverage disputes. As such, LBKM often receives personal information from clients and third parties during the course of litigation and other legal proceedings.

On August 13, 2025, LBKM identified suspicious activity on certain of its computer systems. LBKM immediately took steps to secure its systems and launched an investigation, with the assistance of outside counsel and third-party consultants, into the nature and scope of the activity. Through its investigation, LBKM determined that an unknown actor gained access to certain of its internal systems between August 2, 2025, and August 10, 2025, and was able to view or download certain data.

Upon becoming aware of the unauthorized access, as part of the investigation, LBKM began a review to ascertain specifically what information was involved, what party owns the information, as well as the identity of the individuals to whom the information relates. LBKM recently completed this process.

Starting on February 4, 2026, LBKM began providing notice of this event to affected third parties whose data was involved and provided them with additional information about the type of information that may have been impacted by this event.

The information that could have been subject to unauthorized access for state residents includes name, date of birth, Social Security number, and medical information.

Notice to Nebraska Residents

On or about March 4, 2026, LBKM began providing written notice of this incident to individuals on behalf of relevant third parties. On or about April 29, 2026, LBKM provided written notice of this incident to an additional two (2) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, LBKM moved quickly to investigate and respond to the incident, assess the security of LBKM systems, and identify potentially affected individuals. Further, LBKM notified federal law enforcement regarding the event. LBKM is also working to implement additional safeguards and training to its employees. LBKM is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, LBKM is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. LBKM is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

LBKM is providing written notice of this incident on behalf of third parties to relevant state regulators, as necessary.

EXHIBIT A

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<VARIABLE DATA 1>>

Dear <<Full Name>>:

Lewis Baach Kaufmann Middlemiss PLLC ("LBKM") is writing to inform you of a recent event that appears to involve information related to you. LBKM is a law firm that received your personal information in connection with the provision of legal services. As described below, it appears that your data was implicated by this data security event. While we are not aware of any actual or attempted identity theft or fraud as a result of this event, this notice provides information about what happened, our response, and resources available to help protect your information from possible misuse, should you feel it is appropriate to take steps to do so.

What Happened? On August 13, 2025, LBKM identified suspicious activity on certain of its computer systems. We immediately took steps to secure our systems and launched an investigation, with the assistance of outside counsel and third-party consultants, into the nature and scope of the activity. Through our investigation, we determined that an unknown actor gained access to certain internal systems between August 2, 2025 and August 10, 2025 and was able to view or download certain data.

Upon becoming aware of the unauthorized access, as part of the investigation LBKM began a review to ascertain specifically what information was impacted, as well as the identity of the individuals to whom the information relates. We have recently completed this process.

What Information Was Involved? Based on the review, we determined that the impacted information includes your name and the following information: <<Breached Elements>>.

What We Are Doing. Upon becoming aware of the suspicious activity, we moved quickly to investigate and respond, assess and further strengthen the security of our systems, and notify potentially affected individuals. As an added precaution, we are also offering credit monitoring and identity restoration services through Epiq - Privacy Solutions ID for <<CM Duration>> months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your bank, credit card company, or other applicable institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the credit monitoring and identity restoration services we are making available without cost to you. Enrollment instructions are attached to this letter.

For More Information. We understand you may have questions about this event that are not addressed in this letter. ***If you have additional questions, please call our dedicated assistance line at 844-425-3638, Monday through Friday from 9:00 am to 9:00 pm Eastern Time, excluding major U.S. holidays.*** Please have this letter ready if you call. You may also write to us at the following address: LBKM Response Team, 1050 K Street, NW, Suite 400, Washington, DC 20001.

Sincerely,

Lewis Baach Kaufmann Middlemiss PLLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID
3B Credit Monitoring

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

3-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score with Score Tracker[1]
1-Bureau VantageScore®3.0 (monthly) and Credit Score Tracker.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also contact directly the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/get-credit-report https://www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, PO Box 2000 Chester, PA 19016

Additional Information

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

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.