Attachment A

Baker & McKenzie LLP
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

[redacted]

October 27, 2026

Re: Notice of Data Breach

[redacted]

Baker & McKenzie LLP ("Baker McKenzie") is a global law firm which obtained information about you in connection with legal services it provided to its clients[redacted] We are writing to inform you of a recent cybersecurity incident. Please read this notice carefully, as it provides you with information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring and identity protection services.

What happened:

On August 14 and 17, 2026, a threat actor socially engineered two of our users and obtained a limited number of files. As soon as we discovered this issue, we immediately activated our incident response protocols, engaged a leading cybersecurity forensics firm to investigate, notified law enforcement, and took measures to contain and remediate the unauthorized access. Our cybersecurity forensics firm has confirmed that our remediation efforts were successful, and that the incident has been contained. We have no evidence that the unauthorized actor compromised any user credentials or additional user accounts, and there was no independent malicious access to our systems.

What Personal Information was involved:

Baker McKenzie has been conducting a thorough and extensive analysis of the impacted files to determine what personal information they contained and to whom that information belongs. We recently determined that your personal information was contained in one of the files impacted in the incident. Specifically, your [redacted] in an impacted file.

What we are doing:

We are offering you at no cost a 24-month membership to TransUnion's credit monitoring. To activate your membership and start monitoring your personal information, visit https://bfs.cyberscout.com/activate and provide the activation code contained in Attachment A.

You must enroll by January 27, 2027 to receive these services.

Please see Attachment A for additional details regarding these services.

Draft

Baker McKenzie has also taken additional steps to reinforce our security practices and is actively reviewing our systems and policies to assess what enhanced security monitoring and controls may be necessary to mitigate the risk of similar incidents in the future.

What you can do:

In addition to enrolling in the credit monitoring service being offered to you at no charge, we encourage you to take the following precautions:

- Remain cautious about any unsolicited communications (such as emails, text messages, social posts or phone calls), asking you to provide your personal information. Please avoid clicking on suspicious web links or downloading attachments without confirming they are from a legitimate source.
- Remain vigilant against threats of identity theft or fraud and regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you suspect that you are the victim of identity theft or fraud, you can contact your local police department. Additional information about how to protect your identity is contained in Attachment B.

For more information:

We have established a dedicated call center to answer questions about the cybersecurity incident as well as the TransUnion services that we are offering to you. If you have any questions, please call +1-855-711-3692, from 8 a.m. to 8 p.m. ET Monday through Friday, excluding major U.S. holidays.

Sincerely,

Baker & McKenzie, LLP
300 E. Randolph St., Ste. 5000
Chicago, IL 60601
(312) 861-8000

Draft

Attachment A – ADDITIONAL DETAILS REGARDING YOUR 24-MONTH TRANSUNION CREDIT MONITORING SERVICES

To activate your membership and start monitoring your personal information, please follow the steps below:

In response to the cybersecurity incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services:

[redacted]

In order for you to receive the Credit 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 Credit Monitoring services, you may be asked to provide personal information for your own protection to confirm your identity.

Draft

Attachment B – INFORMATION FOR U.S. CUSTOMERS

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. customers are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free +1 (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR A SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

You may also place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must contact the three credit bureaus below. To place a fraud alert on your credit report, you must contact one of the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000
+1 (888) 378-4329	+1 (888) 397-3742	+1 (800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide some or all of the following information, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five (5) years;
5. Proof of current address such as a current utility bill or a telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).
7. Social Security Card, pay stub, or W-2
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

You may also contact the U.S. Federal Trade Commission (FTC) for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 600 Pennsylvania Avenue NW, Washington, DC 20580; telephone +1 (877) 438-4338 or www.identitytheft.gov.

Draft

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

California residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia residents: The District of Columbia Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; +1 (202) 727-3400, oag@dc.gov and www.oag.dc.gov.

Iowa residents: The Attorney General can be contacted at the Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; +1 (515) 281-5926, www.iowaattorneygeneral.gov.

Kentucky residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, +1 (502) 696-5389, www.ag.ky.gov.

Maryland residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023 or www.oag.maryland.gov.

Massachusetts residents: Under Massachusetts law, you have the right to obtain any police report filed in connection with the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. The Attorney General's office can be contacted by telephone at +1 (617) 727-8400 or online at www.mass.gov/orgs/office-of-the-attorney-general.

North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6000 or www.ncdoj.gov.

New Mexico residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-march-2026.pdf or www.ftc.gov. The Attorney General can be contacted by telephone at +1 (505) 490-4060 or at the addresses listed on nmdoj.gov/contact-us/.

New York residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; +1 (800)-771-7755 or www.ag.ny.gov.

Oregon residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400 or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

For Arizona, California, District of Columbia, Iowa, Montana, North Carolina, Washington and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Draft

Draft