Clark Hill

Scott Koller
T: (213) 226-4736
Email: skoller@clarkhill.com

Scott Koller
T: (213) 226-4736
Email: skoller@clarkhill.com

March 23, 2026

VIA PORTAL SUBMISSION

Office of the Attorney General
6 State House Station
Augusta, ME 04333-0006

Dear Attorney General Frey:

We represent DHJJ, Ltd. ("DHJJ") with respect to a data security incident involving personal information as described below. DHJJ takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On November 21, 2025, DHJJ was alerted to unusual activity involving its information technology environment. In response, DHJJ initiated an investigation and took steps to secure its systems. Additionally, a third-party forensic firm was engaged to assist in the investigation.

Impacted information includes names, addresses, dates of birth, and Social Security numbers.

2. Number of Maine residents affected

Five (5) residents of Maine were notified of the incident. Notification letters were sent to potentially affected individuals on March 19, 2026. A copy of the notification letter is attached as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, DHJJ immediately implemented additional security measures to help secure its systems and prevent future unauthorized access. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through TransUnion.

4. Contact information

DHJJ takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at skoller@clarkhill.com or (213) 226-4736.

Sincerely,

CLARK HILL

Scott Koller
Member

cc: Sunaina Ramesh – sramesh@clarkhill.com

DHJJ, Ltd.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

March 19, 2026

NOTICE OF DATA SECURITY INCIDENT

Dear [redacted],

DHJJ, Ltd. ("DHJJ") is writing to inform you of a data security incident that may have involved some of your personal information. DHJJ may have received your information in the course of providing tax services. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What Happened? On November 21, 2025, we were alerted to unusual activity involving our information technology environment. In response, we initiated an investigation and took steps to secure our systems. Additionally, a third-party forensic firm was engaged to assist in the investigation.

What Information Was Involved? On February 13, 2026, our investigation determined that an unauthorized party may have accessed files that contain some of your information, including your name, address, date of birth, and Social Security number.

What We Are Doing: Upon discovering the incident, we immediately implemented additional security measures to help secure our systems and prevent future unauthorized access. To further protect your information, we are offering 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 12 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 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. For more information on identity theft prevention, please see the pages following this letter.

What You Can Do: We wanted to let you know this happened and assure you that we take this seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity over the next 12 to 24 months. If you see unauthorized charges or activity, please contact your financial institution immediately. For more information on the identity protection services we are providing, including instructions on how to enroll, please see the pages that follow this letter.

For More Information: We sincerely regret this incident occurred and apologize for any inconvenience. If you have any questions, please call [redacted] Monday to Friday 8:00 am to 8:00 pm Eastern time, excluding holidays.

Sincerely,

DHJJ, Ltd.

P 0000101102G0400

Recommended Steps to help Protect your Information

1. Website and Enrollment. 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 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.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, oag.maryland.gov, Telephone: 1-888-743-0023.

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, 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 get based on information in your credit report; and you may seek damages from a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of [XX] Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.