Clark Hill

Scott Koller
T (213) 226-4736
F (213) 488-1178
Email:skoller@clarkhill.com

Clark Hill LLP
555 South Flower Street, 24th Floor
Los Angeles, CA 90071
T (213) 891-9100
F (213) 488-1178

September 10, 2025

Via Electronic Mail

Office of the Attorney General
4 Howard Ave
Cranston, RI 02920
ag@riag.ri.gov

To Whom It May Concern:

We represent Peregrine Property Management, LLC and Peregrine Group, LLC ("Peregrine") with respect to a data security incident involving the potential exposure of certain personally identifiable information ("PII") described in more detail below. Peregrine, a property management and real estate advisory and investment group located in Rumford, RI, is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. **Nature of security incident.**

On April 16, 2025, Peregrine was alerted to unusual activity involving its information technology environment. In response, Peregrine immediately initiated their incident response protocols, began an investigation, and took steps to secure their systems. Additionally, a third-party forensic firm was engaged to assist in the investigation into the nature and scope of what occurred. On June 23, 2025, their investigation determined that while in the Peregrine IT environment, the unauthorized party may have access files that contained personal information. Peregrine then hired a vendor to do an in-depth review to determine what personal information may have been present on the systems involved and whom the information belonged to. On July 22, 2025, that analysis identified some information that was accessible, including individuals' names, and some combination of the following data elements: date of birth, driver's license or state ID number, Social Security number, financial information, passport information, or health related information.

2. **Number of residents affected.**

Five hundred and eighty-six (586) Rhode Island residents may have been affected and were notified of the incident. A notification letter was sent to potentially affected individuals on September 10, 2025. A copy of the form notification letter is enclosed.

3. Steps taken in response.

Since the incident, Peregrine has implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor their systems. Additionally, impacted individuals were offered 12 months credit monitoring and identity protection services through Haystack.

4. Contact information.

Peregrine takes the security of information in its control seriously and is committed to ensuring it is appropriately protected. 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 LLP

Scott Koller

[CLIENT LOGO]
<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you about a data security incident that may have involved some of your information stored on Peregrine Property Management, LLC and Peregrine Group, LLC (collectively, Peregrine) systems. We take the privacy and security of your information very seriously, and therefore we sincerely apologize for any concern or inconvenience this may cause you. 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 April 16, 2025, we were alerted to unusual activity involving our information technology environment. In response, we immediately initiated our incident response protocols, began an investigation, and took steps to secure our systems. Additionally, a third-party forensic firm was engaged to assist in the investigation into the nature and scope of what occurred.

What Information Was Involved?

On June 23, 2025, our investigation determined that while in our IT environment, the unauthorized party may have accessed files that contain some of your information, including your name in combination with your <<Breached Elements>>.

What We Are Doing:

To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems. In addition, while we are not aware of any misuse of your information, we have arranged for you to receive <<CM Duration>> months of credit monitoring and identity protection services through Haystack at no cost to you.

What You Can Do:

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see unauthorized charges or activity, please contact your financial institution immediately. We also encourage you to contact Haystack with any questions and take full advantage of the Haystack service offering. Additional information about protecting your identity is included in this letter, including recommendations by

the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

To enroll in the free credit monitoring services noted above, please log on to <<URL>> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <<Enrollment Code>>. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail address and may not be available to minors under the age of eighteen (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.

For More Information:

If you have any questions or concerns not addressed in this letter, please call <<NUMBER>> (toll free) during the hours of 8:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays)..

Your trust is our top priority, and we deeply regret any inconvenience that this matter may cause you.

Sincerely,

Peregrine Property Management, LLC

&

Peregrine Group, LLC

Recommended Additional Steps You Can Take to Protect Your Information

1. 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.

2. 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 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000 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.

3. Credit or 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.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

4. 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. Contact information for the Federal Trade Commission is as follows:

> *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Additional information for residents of the following states:

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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**,** www.oag.state.md.us/Consumer, 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: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. Total Rhode Island residents notified is (XX).

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