Hightower Holding, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

March 23, 2026

NOTICE OF DATA BREACH

Dear [redacted]

Hightower Holding, LLC (collectively, with its wholly-owned subsidiaries, including Hightower Advisors, LLC, Hightower Securities, LLC, and Hightower Trust Company, N.A., the "Company"), is writing to notify you of two recent events that affected personal information related to you. We are providing you with information about the events, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On January 9, 2026, the Company became aware of a compromised user account resulting in unauthorized access to our environment. In response, we promptly took steps to secure our network and initiated a comprehensive investigation to determine the full nature and scope of the event with the assistance of third-party cybersecurity and digital forensic specialists. The investigation determined that between January 8, 2026 and January 9, 2026, certain files within the Company's environment were downloaded without authorization.

While completing our investigation of the January 9, 2026, incident, the Company became aware of another compromised user account on January 19, 2026, which also resulted in unauthorized access to our environment. In response, we promptly reassessed the security of our network and initiated a second comprehensive investigation with the assistance of third-party cybersecurity and digital forensic specialists. The investigation determined that between January 19, 2026 and January 20, 2026, additional files within the Company's environment were downloaded without authorization.

The Company identified the affected files from both incidents and engaged third-party data review specialists to conduct a time-intensive and thorough review of the files to identify sensitive information contained therein and to whom the information relates. This process was recently completed, and we are notifying you because the review determined certain information related to you was contained within the affected files.

What Information Was Involved? The review determined that [redacted] and the following types of information related to you were present in the affected files at the time of the event: [redacted] Please note that we have no indication that your information has been used to commit identity theft or fraud in relation to this event.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care are among the Company's highest priorities. Upon learning of the events, we promptly commenced an investigation and response that included confirming the security of our network, investigating to determine the information that was impacted, and reviewing the contents of relevant data for sensitive information.

000010102G0500

P

The incidents that triggered this notification to you was not due to a deficiency in the Company's environment, but rather as a result of two compromised user credentials. In connection with our review of the two incidents, we have undertaken additional measures to further strengthen the Company's cybersecurity posture even with respect to credentialed users.

As an added precaution, the Company is offering you immediate access to complimentary single bureau credit monitoring and fraud assistance for twelve (12) months from the date of enrollment, at no cost to you through Cyberscout, a TransUnion company. You can find information on how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Personal Information*. We encourage you to enroll yourself in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information.

For More Information. We understand that you may have questions about these events that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at [redacted] from 8:00am - 8:00pm, Eastern Time, Monday through Friday, excluding major U.S. holidays.

We sincerely regret any inconvenience or concern these events may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Hightower Holding, LLC

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring 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 monitoring services described above, you must enroll within ninety (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 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.

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 directly contact 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 you 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/data-breach-help
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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their 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) 442-9828; and oag.dc.gov. The Company can be contacted at 200 W Madison, 25th Floor, Chicago, IL 60606.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. The Company can be contacted at 200 W Madison, 25th Floor, Chicago, IL 60606.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

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. The Company can be contacted at 200 W Madison, 25th Floor, Chicago, IL 60606.