Notice of Data Security Event
Updated March 17, 2026

Boston Capital publishes this notice of a computer network data security event. This notice provides individuals with information about what happened, steps we have taken in response, and steps individuals may take should they feel it is appropriate.

What Happened? On February 12, 2026, we began reviewing a claim that files were copied from a portion of our computer network. After receiving this information, we had our computer network reviewed by cybersecurity specialists to confirm that it was secure. While investigating this matter, we did learn that an unauthorized third party accessed our computer network. This involved a highly sophisticated social engineering methodology where an unauthorized individual had control of other legitimate companies' cloud systems and used those to circumvent our strict cybersecurity tools and permissions to gain access to our systems. This access allowed the third party to copy certain files from the computer network from January 16 through 22, 2026. The files are under review to determine their contents and to whom they relate. We will send direct notices to individuals when the review is complete.

What Information Was Involved? The types of information stored on the computer network varies by individual. However, name and the following types of information are collectively maintained on the computer network: Social Security number, driver's license number, passport number, other government identification number, and financial account information without codes to access accounts.

What We Are Doing. We are notifying individuals to ensure they are aware of this matter and providing complimentary identity monitoring. Additionally, we are providing individuals free resources and guidance on how to protect their information, should they feel the need to do so. While no safeguards can fully prevent all cybersecurity matters, we are evaluating additional technical measures, as well as reviewing our staff training and supervision practices, to reduce the risk of an issue like this reoccurring. We will continue to evaluate and update our policies and practices as appropriate.

What Individuals Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity and to detect errors. We also encourage individuals to review the "Steps Individuals Can Take To Protect Personal Information" section of this letter. This section contains free resources that are available, including guidance for monitoring free credit reports, how to place a fraud alert or security freeze on credit files, and contact information for the consumer reporting agencies and Federal Trade Commission.

For More Information. If you have questions about this matter, we have an assistance line with agents ready to help answer your questions. Please contact our toll-free assistance line at 1-833-877-7029, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern Time (excluding U.S. holidays). You may also write to us at Boston Capital Holdings LP, Attn: Legal Department, 11 Beacon Street, Ste. 325, Boston, MA 02108.

Sincerely,

Boston Capital Holdings LP

Frequently Asked Questions

What happened? In February 2026, an unknown cyber actor claimed to have accessed the computer network and copied certain files without permission. In response, we had the computer network reviewed by cybersecurity specialists to confirm that it was secure. Through this review, we validated the claim that the computer network was accessed without permission and that files were copied from January 16 through 22, 2026.

Was this a ransomware event? No. The investigation of this matter did not identify any files locked by a computer virus.

Did this affect Boston Capital's ability to provide services? No, we continue to provide high-quality services to our clients.

What information was potentially affected? The types of information stored on the computer network varies by individual. However, name and the following types of information are collectively maintained on the computer network: Social Security number, driver's license number, passport number, other government identification number, and financial account information without codes to access accounts.

Will Boston Capital send notices directly to individuals to let them know about this matter? Yes. When the file review is complete, we will work to locate contact information and reach out to individuals if verifiable contact information is available. If individuals have concerns, they may use the free resources and guidance in the "Steps Individuals Can Take To Protect Personal Information" section below.

Why did it take so long to put out this notice? When incidents like this happen to organizations, they are required to complete an investigation. Technical investigations are very complex and take time to complete. After the technical investigation is complete, regulations require organizations to identify the specific types of information in the involved files. This type of review is a time and resource intensive process.

What is Boston Capital doing to protect my information? We take this event and the security of information in our care very seriously. We have security measures in place designed to protect the files on our systems. While no safeguards can fully prevent all cybersecurity incidents, we are evaluating our technical measures and processes to further enhance our cyber security practices. We will also continue to assess and update security measures and the training of team members to safeguard the privacy and security of information in our care.

Was law enforcement notified? Yes, Federal law enforcement was notified of this event.

Is the computer network safe? Yes, the computer network was reviewed and confirmed to be secure.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Relevant 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 one-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—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

For loved ones that may have recently passed, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. Only one consumer reporting bureau needs to be notified, and it will notify the other two major consumer reporting bureaus. Individuals may complete this process using the information provided by the credit bureaus at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

Steps Individuals Can Take To Protect Their Minor Dependents' Personal Information

Monitor Relevant Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor dependent has a credit report or to request a manual search for your minor dependent's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit or contact the below credit bureaus.

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

To request information about the existence of a credit file in your minor dependent's name, search for your dependent's Social Security number, place a security freeze on your dependent's credit file, place a fraud alert on your dependent's credit report (if one exists), or request a copy of your dependent's credit report you may be required to provide some or all the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor dependent's birth certificate;
- A copy of your minor dependent's Social Security card;
- Your minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor dependent's date of birth; and
- Your minor dependent's previous addresses for the past two years.

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, DC 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. 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.

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/.

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 Avenue NW, 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.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event.