TOPSTEP

141 W. Jackson Blvd. Suite 4240
Chicago, IL, 60604

January [ ], 2026

RE: Notice of Data Breach. Please read this entire letter.

Dear, [First Name], [Last Name]

We are writing to inform you that Topstep LLC ("Topstep") recently discovered a cybersecurity incident that may have affected your information. The cybersecurity incident is described below along with steps you can take to protect yourself against identity theft and information on credit monitoring services that Topstep is providing to you at no charge.

Why are we contacting you?

On December 14, 2025, Topstep was subject to a cybersecurity attack that resulted from cyber threat actors engaging in credential-stuffing. Through this attack, the cyber threat actor may have accessed your individual's Topstep account. Topstep discovered the attack on December 15, 2025, and upon detecting the attack, Topstep acted quickly and diligently to contain and combat the attack. Specifically, Topstep conducted a thorough investigation and analysis of the attack. To date, Topstep is not aware of any breach of its security measures that lead to the cybersecurity attack. Topstep's investigation revealed that the cybersecurity attack was likely the result of cyber threat actors using credentials stolen from sources outside of Topstep and using credential stuffing to gain access. Credential stuffing is the automated injection of stolen username and password pairs ("credentials") into website login forms to fraudulently gain access to user accounts in hopes that users employ the same credentials across multiple platforms. If accounts utilize credentials that are the same across multiple platforms, cyber threat actors can use stolen credentials to gain unauthorized access to various accounts utilizing those credentials.

What Personal Information Was Involved?

Based on Topstep's investigation, Topstep determined the unauthorized cyber threat actors may have gained access to records containing name, contact information, profile information (i.e., screen name), date of birth, phone number, government identification numbers, tax information, and social security numbers of some users.

What Are We Doing?

Upon becoming aware of the cybersecurity attack, IP addresses identified as sending high volumes of traffic were immediately blocked at the Web Application Firewall (WAF) and ALB level. Topstep also forced a password reset for all potentially affected accounts, specifically prohibiting the re-use of old passwords. In keeping with best practices, Topstep continuously looks for ways to improve its IT systems and security infrastructure to better deter and protect against future cybersecurity attacks. Topstep is also working to implement additional security features to its login processes to assist data subjects protect their information, such as mandatory multifactor authentication (currently, users have the option to use multifactor authentication).

What You Can Do.

We recommend that you stay vigilant with respect to your personal information and notify us immediately using the contact information in the "For More Information" section, if there are any changes to your information that you did not authorize with respect to us.

Additionally, to protect yourself from the possibility of identity theft, we recommend that you review your credit files and if you see any suspicious activity, we suggest placing a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other

two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

Experian (888) 397-3742 or
www.experian.com or
P.O. Box 2104, Allen, TX 75013

Equifax (888) 766-0008 or
https://www.equifax.com/ or
P.O. Box 740241, Atlanta, GA 30374

TransUnion (800) 680-7289 or
www.transunion.com or
P.O. Box 2000, Chester, PA 19016

When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies and in reviewing your account statements. You may obtain a free copy of your credit report once every 12 months by:

visiting www.annualcreditreport.com,

calling toll-free 877-322-8228, or

completing an Annual Credit Request Form found at:
www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:
Annual Credit Report Request Service,
P.O. Box 1025281
Atlanta, GA 30348-5283

For more information on identity theft, you can visit the following Federal Trade Commission website at: www.ftc.gov/bcp/edu/microsites/idtheft/. You can contact the Federal Trade Commission the following methods for more information about protecting your identity:

- Visiting: https://www.ftc.gov/about-ftc/contact
- Calling: 877-382-4357
- Mailing: 600 Pennsylvania Avenue, NW, Washington, DC 20580

Additionally, if you received correspondence or any communication from the Internal Revenue Service that you may have been a victim of tax-related identity theft or that your tax filing was rejected as a duplicate, you should immediately fill out a Form 14039 Identity Theft Affidavit and submit it to the Internal Revenue Service. You should continue to file your tax return, as applicable, and attach the Form 14039 Identity Theft Affidavit to the return. Tax-related identity theft occurs when someone uses a taxpayer's stolen Social Security number to file a tax return claiming a fraudulent refund.

For more information on when to file a Form 14039 Identity Theft Affidavit, you can visit the following Internal Revenue Service website: https://www.irs.gov/newsroom/when-to-file-an-identity-theft-affidavit

For more information on tax-related identity theft, you can visit the following Internal Revenue Service website: https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft

You also have the right to put a Security Freeze on your credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a Security Freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. A separate Security Freeze must be requested and placed on the applicable credit file with each credit reporting agency. To place a Security Freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and

a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a Security Freeze.

You may also have the right to request and obtain a police report with regard to the cybersecurity attack.

Credit Monitoring.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for [Length of Service] months. This will be separate from the fraud alert you may put on your credit files, as explained above.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Length of Service] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks℠ as a complimentary [Length of Service] membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks℠ website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks℠ online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B######] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [LENGTH OF SERVICE] MONTH EXPERIAN IDENTITYWORKS℠ MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks℠. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks℠:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks℠ membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call [Experian TFN] toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number [B######].

If you have further questions or concerns, or if there is anything that we can do to further assist you, please call, write, or email us at Topstep Customer Support at 888-407-1611, 141 W Jackson Blvd. Suite 4240, Chicago, IL 60604, or dpo@topstep.com. You can also use the support channels provided at https://help.topstep.com/en/articles/8284118-how-do-i-contact-the-support-team.

Additional State Specific Information.

If you are a resident of North Carolina:

- For more information on identity theft, you can visit or contact the Office of the North Carolina Attorney General at the following:
  - Website: https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/
  - Phone Number: 919-716-6000
  - Address: 114 West Edenton Street, Raleigh, NC 27603

If you are a resident of New York:

- For more information on identity theft, you can use the following sources:
  - New York Department of State Division of Consumer Protection https://dos.nysits.acsitefactory.com/consumer-protection
  - NYS Attorney General at: http://www.ag.ny.gov/home.html
  - Phone Number: 800-771-7755

If you are a resident of Maryland:

- For more information on identity theft, you can contact the Maryland Attorney General at the following:
  - Website: https://oag.maryland.gov/i-need-to/Pages/identity-theft-information.aspx
  - Phone Number: 888-743-0023
  - Address: 200 St. Paul Place, Baltimore, MD 21202

If you are a resident of Rhode Island:

- For More Information on identity theft, you can visit or contact the Office of the Rhode Island Attorney General at the following:
  - Website: https://riag.ri.gov/
  - Phone Number: 401-274-4400

Sincerely,

James Spolar
Deputy General Counsel