



400 N. Main St.
Greenfield, MA 01301

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

[Date]

RE: Important Security Notification. Please read this entire letter.

Dear [First Name] [Last Name]:

Greenfield Savings Bank recently discovered an incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On August 14, 2025, Greenfield Savings Bank (GSB) was notified of a cybersecurity incident experienced by a third-party provider of marketing services. Upon learning of the incident, our vendor immediately launched an investigation, worked with us to understand the scope of the issue, and engaged the appropriate cybersecurity experts to assist. Our vendor also promptly notified law enforcement.

Importantly, there has been no evidence of unauthorized activity within GSB's own internal systems. The incident was limited to the vendor's environment.

What Information Was Involved? Based on the information available to date, the following data of yours was accessed without authorization: Date of Birth, Social Security Number, and Financial Account information. At this time, we have no evidence of the misuse, or attempted misuse, of personal information as a result of this incident.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. In addition to working closely with our vendor and cybersecurity experts, we have taken steps to help protect your information. These include ensuring the vendor has secured its systems and implemented additional safeguards, conducting an internal review of all systems connected to the vendor and enhancing our oversight protocols for third-party security management.

What You Can Do: We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you notice suspicious activity, please contact us immediately at the number shown at the bottom of this letter.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for **24** months.

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 **24** 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 **24**-month 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 November 30, 2025** (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 (833) 931-7577 by **November 20, 2025**. Be prepared to provide engagement number [\[B#####\]](#) as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call 1-888-324-3191.

Sincerely,

[\[Your Signature Graphic\]](#)

[\[Organization Contact, Title\]](#)

[\[Organization Name\]](#)

* 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.