BerkshireBank

March 4, 2020

16605

«name»
«addr»
«city», «st» «Zip»

RE: IMPORTANT MESSAGE REGARDING YOUR DEBIT CARD ENDING IN «F2»

Dear «name»:

At Berkshire Bank, our top priority is to make sure personal financial information is safe and secure. So when we identify a potential risk, our policy is to contact our customers immediately and work quickly to resolve the issue. Therefore, we are notifying you that your Berkshire Bank Debit or ATM card number ending in «F2» may have been compromised. To avoid possible fraudulent activity, we will be issuing you a new MasterCard Debit Card to replace your existing card. Your new card will arrive within the next 7 to 10 business days. **Your current card will be cancelled once you activate your new card. If you do not activate your new card, your current card will be cancelled on March 23, 2020.**

To activate your new card, simply use it at any Berkshire Bank or NYCE® ATM or make a PIN-based transaction at any merchant, **using your current PIN number**. If you prefer, you can activate your card through Berkshire Bank's telephone banking system; just call 888-685-8300, choose option 7 and then press 1 to activate your card.

If you have provided your current MasterCard Debit Card number to any vendor to be used for automatic payments, you will need to provide that vendor with your new MasterCard number as soon as possible.

Email and text message alerts of your debit card activity are now available through your Online Banking account at BerkshireBank.com. Under the Customer Service menu select *Manage Alerts* then *ATM/Debit Card Alerts* to receive alerts of your debit card activity. Berkshire Bank also provides free security monitoring for "out of the ordinary" transactions for all Berkshire Bank debit cards. This would be for activity that varies from your normal activity.

We hope this will not create any inconvenience to you. We take our obligation to safeguard personal information very seriously. We encourage you to remain vigilant and regularly review and monitor your credit reports and medical benefits statements. The attached **Reference Guide** provides details on these and other steps you may wish to consider.

If your card ending in «F2» has already been replaced since February 26,2020, please disregard this letter. If you have any questions or concerns, please contact us at 800.773.5601.

Sincerely,

Berkshire Bank Electronic Banking Team

Berkshire Bank is a wholly owned subsidiary of Berkshire Hills Bancorp, Inc.

Reference Guide

We encourage individuals take the following steps to review and monitor credit reports:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open and medical bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

Place a Security Freeze on your Credit Report: You have a right to place a "security freeze" on your credit report at no cost, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.