

October 23, 2020

Dear Customer,

## IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION

A security incident occurred at a merchant location that may involve your personal information. Investigation determined that data may have been exposed on transactions conducted between July 15, 2019 and July 10, 2020. Salem Five has reason to believe that your name and address in conjunction with your debit card number may have been compromised or may be in the possession of unauthorized individuals.

### The Actions We Have Taken / Mitigation Services

Salem Five acts quickly upon receipt of such reports to protect our customers' data and accounts. In this case, as a security precaution, Salem Five has issued a new debit card and your old card will be closed on November 12, 2020.

### The Actions We Recommend You Take

- 1. Please be vigilant.** As always, your best defense against fraudulent activity is to monitor your account activity often and closely through our free phone or Internet access services and by reviewing your periodic statements. Your vigilance is particularly important over the next 12 to 24 months. If you become aware of any incidents involving the suspected unauthorized use of your card or your identity, please notify us immediately at the Bank's phone number below.
- 2. You have the right to obtain a police report.** As of the date of this letter, Salem Five is unaware of any police report having been filed in regard to this incident. If you discover suspicious activity on your credit report, your accounts or by any other means, you may wish to file a police report. You have a right to obtain a copy of any police report you file.
- 3. Learn more about identity theft.** The Federal Trade Commission's (FTC) web site provides information and guidance about steps you can take to protect against identity theft, fraud alerts and security freezes, and where you can report suspected identity theft to the FTC. Salem Five encourages you to report any incidents of identity theft. The web site is [www.ftc.gov](http://www.ftc.gov) or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). You may report suspected identity theft to the FTC at 877-438-4338 (877-ID-THEFT), 1-866-653-4261 (TTY); [www.identitytheft.gov/steps](http://www.identitytheft.gov/steps) and 600 Pennsylvania Avenue, NW, Washington DC 20580.
- 4. Contact consumer reporting agencies.** You may contact the fraud departments of the three major consumer reporting agencies to discuss your options. You may obtain your report from the consumer reporting agencies; you may also receive one free annual credit report at [www.annualcreditreport.com](http://www.annualcreditreport.com). You have the right to place a free 90-day fraud alert on your credit file which will let creditors know to contact you before opening new accounts and may delay your ability to obtain credit. To place a fraud alert, contact the consumer reporting agencies below:

Experian  
[www.experian.com](http://www.experian.com)  
(888) 397-3742  
P.O. Box 9532

Equifax  
[www.equifax.com](http://www.equifax.com)  
(877) 478-7625  
P.O. Box 740241

TransUnion  
[www.transunion.com](http://www.transunion.com)  
(800) 680-7289  
P.O. Box 6790

Allen, TX 75013

Atlanta, GA 30374

Fullerton, CA 92834

5. You have the right to place a security freeze on your consumer credit report. Federal law mandates that a consumer reporting agency allow a consumer to place, lift, or remove a security freeze "free of charge." The security freeze prohibits a consumer reporting agency from releasing information in your consumer report without your express authorization. A security freeze may be requested by sending a request either by toll-free telephone, secure electronic means (Equifax Security Freeze 1-800-349-9960 <https://www.equifax.com/personal/credit-report-services>; Experian Security Freeze 1-888-397-3742 <https://www.experian.com/freeze/center.html>; TransUnion Security Freeze 1-888-909-8872 <https://www.transunion.com/credit-freeze>) or mail (certified, overnight, regular stamped) to a consumer reporting agency. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. A security freeze may delay, interfere with, or prevent the timely approval of any subsequent credit request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions or other services, including an extension of credit at point of sale.

In order to request a security freeze, you will need to provide the following information to the consumer reporting agency:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.); social security number; and date of birth;
- If you have moved in the past five years, the addresses where you previously lived in those years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card such as state driver's license or I.D. card or a military I.D. card;
- Social security card, pay stub, or W2; and
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning the identity theft.

The consumer reporting agencies have three business days after receiving your request to place a security freeze on your credit report, and they must send a written confirmation to you within five business days, providing you with a unique personal identification number or password, or both, that you can use to authorize the removal or lifting of the security freeze.

#### How We Will Assist You

We will continue to monitor the effects of the security incident and take appropriate actions. We apologize for any inconvenience this situation may cause. If you have any questions about this notice, please allow our Customer Service Center to assist you at (800) 850-5000.

Sincerely,



Steven Belt  
VP, Customer Experience Director



October 23, 2020

Dear Customer,

**IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION**

A security incident occurred at a merchant location that may involve your personal information. Investigation determined that data may have been exposed on transactions conducted between July 15, 2019 and July 10, 2020. Salem Five has reason to believe that your name and address in conjunction with your PREVIOUSLY CLOSED debit card number may have been compromised or may be in the possession of unauthorized individuals.

**The Actions We Have Taken / Mitigation Services**

Salem Five acts quickly upon receipt of such reports to protect our customers' data and accounts. In this case, Salem Five has confirmed that this incident was not related to an active debit card and is informing you of the incident.

**The Actions We Recommend You Take**

- 1. Please be vigilant.** As always, your best defense against fraudulent activity is to monitor your account activity often and closely through our free phone or Internet access services and by reviewing your periodic statements. Your vigilance is particularly important over the next 12 to 24 months. If you become aware of any incidents involving the suspected unauthorized use of your card or your identity, please notify us immediately at the Bank's phone number below.
- 2. You have the right to obtain a police report.** As of the date of this letter, Salem Five is unaware of any police report having been filed in regard to this incident. If you discover suspicious activity on your credit report, your accounts or by any other means, you may wish to file a police report. You have a right to obtain a copy of any police report you file.
- 3. Learn more about identity theft.** The Federal Trade Commission's (FTC) web site provides information and guidance about steps you can take to protect against identity theft, fraud alerts and security freezes, and where you can report suspected identity theft to the FTC. Salem Five encourages you to report any incidents of identity theft. The web site is [www.ftc.gov](http://www.ftc.gov) or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). You may report suspected identity theft to the FTC at 877-438-4338 (877-ID-THEFT), 1-866-653-4261 (TTY); [www.identitytheft.gov/steps](http://www.identitytheft.gov/steps) and 600 Pennsylvania Avenue, NW, Washington DC 20580.
- 4. Contact consumer reporting agencies.** You may contact the fraud departments of the three major consumer reporting agencies to discuss your options. You may obtain your report from the consumer reporting agencies; you may also receive one free annual credit report at [www.annualcreditreport.com](http://www.annualcreditreport.com). You have the right to place a free 90-day fraud alert on your credit file which will let creditors know to contact you before opening new accounts and may delay your ability to obtain credit. To place a fraud alert, contact the consumer reporting agencies below:

Experian  
[www.experian.com](http://www.experian.com)  
(888) 397-3742  
P.O. Box 9532

Equifax  
[www.equifax.com](http://www.equifax.com)  
(877) 478-7625  
P.O. Box 740241

TransUnion  
[www.transunion.com](http://www.transunion.com)  
(800) 680-7289  
P.O. Box 6790

Allen, TX 75013

Atlanta, GA 30374

Fullerton, CA 92834

5. You have the right to place a security freeze on your consumer credit report. Federal law mandates that a consumer reporting agency allow a consumer to place, lift, or remove a security freeze "free of charge." The security freeze prohibits a consumer reporting agency from releasing information in your consumer report without your express authorization. A security freeze may be requested by sending a request either by toll-free telephone, secure electronic means (Equifax Security Freeze 1-800-349-9960 <https://www.equifax.com/personal/credit-report-services>; Experian Security Freeze 1-888-397-3742 <https://www.experian.com/freeze/center.html>; TransUnion Security Freeze 1-888-909-8872 <https://www.transunion.com/credit-freeze>) or mail (certified, overnight, regular stamped) to a consumer reporting agency. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. A security freeze may delay, interfere with, or prevent the timely approval of any subsequent credit request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions or other services, including an extension of credit at point of sale.

In order to request a security freeze, you will need to provide the following information to the consumer reporting agency:


- Your full name (including middle initial as well as Jr., Sr., II, III, etc.); social security number; and date of birth;
- If you have moved in the past five years, the addresses where you previously lived in those years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card such as state driver's license or I.D. card or a military I.D. card;
- Social security card, pay stub, or W2; and
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning the identity theft.

The consumer reporting agencies have three business days after receiving your request to place a security freeze on your credit report, and they must send a written confirmation to you within five business days, providing you with a unique personal identification number or password, or both, that you can use to authorize the removal or lifting of the security freeze.

#### How We Will Assist You

We will continue to monitor the effects of the security incident and take appropriate actions. We apologize for any inconvenience this situation may cause. If you have any questions about this notice, please allow our Customer Service Center to assist you at (800) 850-5000.

Sincerely,



Steven Belt  
VP, Customer Experience Director

The incident date(s) are believed to be 7/15/2019 – 7/10/2020. The nature of the incident is that the residents' personal information was acquired or used by an unauthorized person and there is a substantial risk of identity theft or fraud involving unauthorized card use. We received knowledge of this incident via Visa Alert Services. The incident appears to have involved a potential breach of security at a third party merchant or processor of customer information exposing Visa payment account data to a possible compromise. Preliminary investigation indicates that the categories of personal information involved in this incident are as follows: name, address, debit card number, CVV, and expiration date. The personal information that was the subject of this incident is believed to be in electronic form.

We believe 12 MA residents have been affected by this incident. These residents have received notice (attached) in accordance with M.G.L. c. 93H by letter. Letters were sent on 10/23/2020.

OPEN - When we became aware of this incident on 10/23/2020, we implemented measures to protect the impacted MA residents and to help ensure that similar incidents do not occur in the future. In addition to notifying the impacted resident, we cancelled the compromised card number, reissued a new card, and will reimburse consumers that are impacted by unauthorized transactions, if any, in accordance with Federal Reserve Regulation E. We did not report the incident to law enforcement. We do not have evidence that the personal information has been used for fraudulent purposes.

CLOSED - When we became aware of this incident on 10/23/2020, we researched and determined that we had already implemented measures to protect the impacted MA residents and to help ensure that similar incidents do not occur in the future. We had previously cancelled the compromised card numbers, reissued new cards, and will reimburse consumers that are impacted by unauthorized transactions, if any, in accordance with Federal Reserve Regulation E. We also notified the impacted residents. We did not report the incident to law enforcement. We do not have evidence that the personal information has been used for fraudulent purposes.