



24513

November 5, 2021

Dear Customer,

IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION

A security incident occurred at a merchant that may involve your personal information. Investigation determined that data may have been exposed on transactions conducted between November 1, 2020, and November 4, 2021. Salem Five has reason to believe that your name 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 regarding 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 or 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 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. 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

Equifax
www.equifax.com

TransUnion
www.transunion.com

210 Essex Street | Salem, MA 01970 | 800.850.5000 | 978.745.5555 | mail@salemfive.com | salemfive.com

Member FDIC | Member DIF

V.2021.03.10

(888) 397-3742
P.O. Box 9532
Allen, TX 75013

(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374

(800) 680-7289
P.O. Box 6790
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 1-888-298-0045 <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

Visa Confidential CAMS

Terri Murphy

Case Number: EU-2021-0615a-RE

Date: November 4, 2021

Entity Type: Other

Data Elements at Risk:

- Cardholder Name
- CVV2
- Expiration Date
- PAN

PIN Transaction: Unknown

Exposure Window: Unknown

Visa's Fraud and Breach Investigations have been provided the following at-risk account numbers by [VI_TO_FILL_IN]. The account numbers were recovered from [VI_TO_FILL_IN] with the above data elements at risk. Please be advised that there is an ongoing investigation, and Visa may provide additional information if it becomes available.

Please review your listed accounts at gvo1.visaonline.com and take the necessary steps to prevent fraud and safeguard your cardholders. While assessing the appropriate action to take, you may want to review the compromised account best practices document located in the HELP section of Visa Risk Manager.

Disclaimer Information: This information is provided as an advisory service only and is intended solely for the addressee. Access to this information by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution is prohibited and may be unlawful. The author and Visa Inc. accept neither responsibility for the accuracy of this information nor any subsequent investigative action or otherwise taken by any individual member based on the information provided herein. This advisory may be based on information provided to Visa Inc. by merchants, acquirers, third party processors and/or law enforcement. Visa Inc. accepts no responsibility for the information and advises Visa members to do their own verification to determine the accounts provided are at risk. Any action(s) taken by a Visa member based on this information is entirely at the member's own discretion.

Visa Confidential

CAMS	Terri Murphy
------	--------------

Email Attachment(s)

Number of Accounts 4

CANCEL