16101

SalemFive

October 8, 2019

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 an unknown date and October 7, 2019. 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 policy report having been field 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* 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	Equifax	TransUnion
www.experian.com	www.equifax.com	www.transunion.com
(888) 397-3742	(877) 478-7625	(800) 680-7289
P.O. Box 9532	P.O. Box 740241	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

Butts, Nicholas A (SCA)

From: Melissa.LeFave-Willis@salemfive.com
Sent: Monday, November 25, 2019 12:52 PM
To: Breaches, Data (SCA)
Subject: FW: Security Breach Notification - AMENDMENT

I would like to amend a previously submitted form. The ACTUAL person in custody of PI when breach occurred is UNKNOWN.

Person in custody of personal information when breach occurred. If multiple persons were in custody of personal information, select the relationship of the primary person: Current Employee

Kind regards,
Melissa

Melissa LeFave-Willis
AVP, ERM Manager I

SalemFive
Salem Five Bank | 210 Essex Street | Salem, MA 01970
tel. 978.720.5362 | melissa.lefave-willis@salemfive.com

We're Listening On:

From: Carito, Diana <Diana.Carito@salemfive.com>
Sent: Monday, November 25, 2019 11:33 AM
To: LeFave-Willis, Melissa <Melissa.LeFave-Willis@salemfive.com>
Subject: FW: [EXTERNAL] - Security Breach Notifications

Kind regards,
Diana

OUT OF OFFICE: Refer to my calendar which is current.

Diana L. Carito
Senior Vice President & Director Enterprise Risk Management

SalemFive
Salem Five Bank | 210 Essex Street, 2nd Floor | Salem, MA 01970
tel: 978.720.5816 | fax: 978.744.8351 | diana.carito@salemfive.com

From: Data Breaches <noreply+63308160d0553ecb@formstack.com>
Sent: Monday, November 25, 2019 11:28 AM
To: Carito, Diana <Diana.Carito@salemfive.com>
Subject: [EXTERNAL] - Security Breach Notifications

Thank you for using the Security Breach Online Notifications Form. The following information has been submitted

Submission Time: Nov 25, 2019 11:28 AM

Section 1: Organization and Contact Information

Business Name: Salem Five Cents Savings Bank
Business Address:
Company Type: Banks & Credit Unions
Your Name: Diana Carito
Last Name: Carito
Title: SVP & Director ERM
Contact Address: 210 Essex Street
Salem, MA 01970
Telephone Number: (978) 720-5816
Ext: 5816
Email Address: Diana.Carito@salemfive.com
Relationship to Org: Current employee

Section 2 Breach Information

Breach Type: Electronic

Date Data Breach Was Discovered: 10/07/2019

Number of Massachusetts Residents Affected: 29

Person in custody of personal information when breach occurred. If multiple persons were in custody of personal information, select the relationship of the primary person: Current Employee

Please give a detailed explanation of how personal information was protected at the time of the breach, and state the means used (for example, locks/encryption methods): The incident date(s) are believed to be 10/7/2019 – 10/7/2019. 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, debit card number, CVV, and expiration date. The personal information that was the subject of this incident is believed to be in electronic form. Incident

did not involve our systems.

Please select the types of personal information that was included in the data breach: *Credit/Debit Card Number = Selection(s)*

Please check all of the boxes that apply to your breach: The breach was a result of a malicious/criminal act. = Selection(s)

Section 3 Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data: N/A

Date of last review of written security program:

Physical access to systems containing personal information was restricted to authorized personnel only: N/A

Network configuration of breached system: N/A For breaches involving electronic systems, complete the following:N/A = Selection(s)

Section 4 Remediation

The company has notified all Massachusetts residents affected by the breach: Yes

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply): Option2 | US Mail
Option5 | Other

Please explain your answer of other above: Phone calls also made to residents.
Date notices were first sent to Massachusetts residents: 10/08/2019
Your company offered complimentary credit monitoring services to Massachusetts residents affected by the breach: No

Law enforcement has been notified of this data breach: No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring: We believe 29 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 10/8/2019. When we became aware of this incident on 10/7/2019, 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.

Attached file 1:

Attached file 2:

Attached file 3:

Attached file 4: