#14285

DATE

Name and Address

Dear Customer: RE: card number ending in XXX

Dedham Savings was recently notified of a possible security incident (card breach) at an undisclosed location. The data exposed was debit card numbers, cardholder names, PIN data, Security Code (CVC number) and expiration dates. Please note that no personal information linked to debit card numbers, such as checking or savings account numbers was disclosed. It has been determined that your debit card was among those that were reported to Dedham Savings.

Although certain card data may have been compromised in the incident, it does not necessarily mean that your card data was involved. It is important to note that "compromised" simply means that typically secure information may have been revealed to an unauthorized person. Please be assured that Dedham Savings is closely monitoring all potentially compromised cards. Our internal fraud detection systems have not detected fraud on customers' affected cards.

As a precautionary measure, we have reduced your daily limit to $300.00 for debit card purchases (signature transactions) on your existing card. We will also be issuing a new card for you with your existing Personal Identification Number (PIN). We anticipate that new card will arrive within 7 to 10 business days in an unmarked envelope. During the interim, you will continue to have limited access on your current card until you receive your new debit card. **Your current card will be restricted by XXXX or upon activation of your new debit card, whichever comes first. Once you receive your new card, please;**

- **Activate your new card immediately so you may continue making transactions without interruption. To activate your card contact our 24 Hour Telephone Banking System at 1-888-252-0760 Option 6,2 or by performing a PIN based transaction.**
- **Destroy your old card and start using your new card with your current Personal Identification Number (PIN).**
- **If you have set up recurring payments with a store or service provider, provide those companies with your new card number and expiration date.**

Dedham Savings' cardholders should continue to diligently monitor their account activity. You may use our 24 hour Telephone Banking system, BankLine, at 1-888-252-0760 or view your account history online with Your Link. To enroll in Your Link, visit our website at www.dedhamsavings.com. Once you have enrolled, you can have instant access to your account history.

We are providing a notice on the back of this letter that is currently required by federal and state law that outlines certain actions and recommendations that you may take to protect yourself as a consumer. Each consumer should read the notice and make a determination on what steps make sense for you. If you need further assistance, please contact the bank at the number provided below.

If you notice that your card has been used for any unauthorized transaction, please contact our **Electronic Banking Department immediately at (781)-329-6700 or 1-800-462-1190**. Please be assured that you will not be held responsible for any fraudulent activity associated with this incident. We will continue to monitor the effects of this security incident and want to ensure that you are aware of the resources available to you.

We value your patronage and appreciate you for making Dedham Savings "Your Bank".

Sincerely,

Justin Magnan

Justin Magnan
Electronic Banking Department

Customer Notice

Under Federal and Massachusetts law, businesses and state and local government agencies must notify you if your personal information was compromised by a security breach because it may place you at greater risk of identity theft.

What is a Security Breach?

A security breach occurs when data or records containing personal information such as Social Security numbers, bank account numbers or driver license numbers are lost, stolen or accessed improperly. This kind of information can be used by criminals to commit identity theft.

Being notified that your information was part of a security breach does not necessarily mean you will become a victim of identity theft. However, you are at an increased risk and need to take steps to protect yourself.

STEP 1: Review Your Account Statements

Over the next 12-24 months, you should closely review your account statements and notify us immediately of any suspicious activity.

STEP 2: Notify the Credit Bureaus

You may contact the fraud departments of the three major credit reporting agencies to discuss your options. You should review your credit report and may obtain your report by contacting any of the credit reporting agencies listed below. You may also receive a free annual credit report at www.annualcreditreport.com. You have the right to place a free 1 year fraud alert on your credit file and an extended fraud alert up to seven years if you have been a victim of identity theft. A fraud alert lets creditors know to contact you before opening new accounts. It also may delay your ability to obtain credit. To place a fraud alert on your credit report, contact the three credit reporting agencies below.

Experian	Equifax	TransUnion
(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 30374-0241	Fullerton, CA 92834-6790
www.experian.com	*www.equifax.com*	*www.transunion.com*

STEP 3: Learn More (EDUCATE YOURSELF)

You may wish to learn more about identity theft. The Federal Trade Commission has on-line guidance about the steps that consumers can take to protect themselves against identity theft. You can call 1-877-ID-THEFT (1-877-438-4338) or visit the Federal Trade Commission's website at *www.ftc.gov*, or *www.consumer.gov/idtheft* to obtain additional information. We also encourage you to report suspected identity theft to the Federal Trade Commission.

STEP 4: Consider a Security Freeze

You have a right to place a security freeze on your consumer credit report, free of charge. The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer report without your express authorization. A security freeze may be requested by sending a request by certified mail, overnight mail or regular stamped mail 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. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent credit request or application you make regarding new loans.

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number and date of birth;
2. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
3. Proof of current address, such as a current utility bill or telephone bill;
4. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
5. 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 credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send a written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. There is no fee to place, lift or remove a security freeze.

Step 5: Notify Law Enforcement

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.