



June 19, 2017

RECEIVED  
JUN 22 2017  
CONSUMER PROTECTION

Attorney General Joseph Foster  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General Foster:

We are writing to notify you of an unauthorized access or use of personal information involving eleven (11) New Hampshire residents.

**NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS:**

On May 25, 2017, the Santander Bank Fraud Risk group identified an ATM skimming event at a Santander Bank ATM terminal in Billerica MA. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number.

**NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED:**

The incident affected eleven (11) New Hampshire residents. These residents will be receiving notice in a letter scheduled to be mailed on or about June 14, 2017, a sample of which is enclosed.

**STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT:**

This incident was identified by Santander Bank Fraud Risk and Physical Security Departments, escalated to the Bank's Privacy Office, and an investigation was initiated. The investigation revealed that some of the personal information obtained was used for fraudulent purposes. The cards for all impacted individuals were immediately closed and new cards were reissued. The Bank is continuing to monitor Santander Bank ATMs and potentially suspicious transactions.

**CONTACT INFORMATION:**

Santander Bank values the security of its customers' information and regrets this unfortunate incident. Please contact Cassie Kelleher, the Santander Bank Fraud Investigator assigned to this case, directly at 781-462-2983 should you have any questions or require additional information.

Sincerely,

Michelle Guttman  
Chief Privacy Officer

Enclosures: Notification Letter to Affected Resident

Equal Housing Lender. Santander Bank, N.A. is a Member FDIC and a wholly owned subsidiary of Banco Santander, S.A. ©2013 Santander Bank, N.A. Santander and its logo are registered trademarks of Banco Santander, S.A., or its affiliates or subsidiaries in the United States and other countries





DATE: XXXX

Re: Account number ending in -XXXX

Dear <Customer Name>,

Santander Bank is strongly committed to the security of our cardholders' information and strives to let you know about security concerns as soon as possible. We are writing to notify you of a data security incident that occurred at the ATM located at XXXXX on XXXX involving your Santander® Card. As a result of this incident, we have reason to believe the following information was compromised:

- Your name
- Card number
- Personal Identification Number (PIN), and
- Card expiration date.

Here's what you need to know:

1. **We will reissue your card.**
  - a. Your current card has been deactivated.
  - b. Your new card will arrive in an unmarked envelope by XXXX
2. **Upon receipt of your new card, you will need to activate the card by calling 888.875.8074 immediately.**
  - a. Please activate your new card by XXXX otherwise we may close it under the assumption that it has not been received.
3. **If you make automatic payments, you will need to notify merchants of your new card number, expiration date, and security code.**

Furthermore, we are doing our part on a daily basis to ensure that you are protected.

**Santander has placed additional fraud monitoring** on your card that goes above and beyond our standard measures. We will contact you if we suspect any unusual activities related to this incident.

**Your Santander card comes with our Zero Liability policy.** As always, you are not liable for fraudulent charges on your account when you notify us promptly.

**We are just a phone call away.** If you have questions—or if you detect suspicious activity—please report it immediately by calling the number on the back of your card. For customers with hearing impairments, please call 800.428.9121 (TTY/TDD). You may also visit your neighborhood branch for assistance.

In addition to the fraud protection actions Santander has taken on your behalf, you can take precautionary steps to further protect yourself from the risks of fraud and identity theft. We recommend that you remain vigilant over the next 12-24 months, review your statements, monitor free credit reports carefully, and refer to the attached sheet for more information on tools and resources available to all Santander customers.

Please be assured that safeguarding your personal information is a top priority at Santander Bank. We apologize for any inconvenience this situation may cause and are standing by to assist you with any questions or concerns you may have.

Sincerely,

Jason Beaber  
Director, Customer Service Center  
Santander Bank, N.A.

Santander Bank, N.A. is a Member FDIC and a wholly owned subsidiary of Banco Santander, S.A. ©2015 Santander Bank, N.A. | Santander, Santander Bank and the Flame Logo are registered trademarks of Banco Santander, N.A. or its affiliates or subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners.

04/2015 LC-RETB0392-A



## Guide to Monitoring Your Accounts for Fraud and Identity Theft

**Review your account statements.** We recommend that you review your statements carefully and otherwise remain vigilant over the next 12 to 24 months. We will also continue to monitor your accounts for unusual activity. If you notice any suspicious activity or suspect identity theft please contact Fraud Prevention at 877-906-7500 or by calling the number on the back of your card. For customers with hearing impairments, please call 800.428.9121 (TTY/TDD). You may also report suspected incidents of identity theft to local law enforcement or to your state's attorney general.

**Sign up to receive alerts from Santander about your account activity**—a free tool designed to help you monitor your balances, statements, and purchases in real time. Log in to Santander Online Banking, click on the "Credit Cards" tab and choose "Alerts" on the left-hand menu. To change your individual settings, click on "Manage alerts".

**Monitor your credit reports.** To obtain an annual free copy of your credit reports visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 1-877-322-8228, or submit a request via mail. To submit via mail, complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission website ([www.ftc.gov](http://www.ftc.gov)) and mail it to Annual Credit Report Request Service PO Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through these methods. Once you receive your credit reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, or debts on your accounts that you do not recognize. Also make sure to verify the accuracy of your Social Security number, address(es), complete name and employer(s) information. If any information is incorrect, please notify the major credit bureaus directly. Below, we have listed their contact information for you.

**Contact the major credit bureaus** to access useful information about protecting your credit, including information on fraud alerts, security freezes, or other steps you can take to protect yourself from fraud and identity theft. General contact information for the major credit bureaus is:

Equifax  
Consumer Fraud Division  
P.O. Box 740256  
Atlanta, GA 30374  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

Experian  
Credit Fraud Center  
P.O. Box 1017  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
Fraud Victim Assistance Dept.  
P.O. Box 6790  
Fullerton, CA 92834  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

**Enable MasterCard® Identity Theft Alerts.** Santander MasterCard cardholders that enable Identity Theft Alerts will be notified if their personal information has been compromised online. This information is gathered so that they have the opportunity to react quickly and take the necessary steps to protect themselves. If you are a holder of a Santander MasterCard, visit <http://www.mastercard.us/idtheftalerts> to enroll. There is no additional charge for identity theft services offered through MasterCard. For more information on terms and eligibility, please refer to your card agreement, call Santander at the number on the back of your card, and / or contact MasterCard directly at 1-800-MasterCard.

**Access MasterCard® Identity Theft Resolution Services** If you believe you have been a victim of identity theft, contact 1-800-MasterCard for assistance in completing the recommended steps above. There is no limit on the number of claims you may submit, and there is no additional charge for identity theft services offered through MasterCard. For more information on terms and eligibility, please refer to your card agreement, call Santander at the number on the back of your card, or contact MasterCard directly at 1-800-MasterCard.

**The Federal Trade Commission (FTC)** is a government agency that provides information about identity theft and maintains a database of identity theft cases for use by law enforcement. To file a report with the FTC call the Identity Theft Hotline at 1-877-IDTHEFT (438-4338); send a letter to: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W. Washington DC 20580; or visit [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/) to submit a report online. You may also wish to consult the publication, "Take Charge: Fighting Back Against Identity Theft."

**Maryland Residents** can obtain additional information about steps to avoid identity theft by contacting the Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; visiting <http://www.oag.state.md.us>; or calling 1-888-743-0023.



If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; if you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

We also encourage you to consider taking the following steps:

- Regularly check account activity and carefully review your monthly statements;
- Report any suspected incidents of identity theft to local law enforcement and to Santander immediately;
- Request a free credit report annually from each of the three main credit reporting agencies by going online at [www.annualcreditreport.com](http://www.annualcreditreport.com);
- You may also obtain information about fraud alerts and security freezes from the Federal Trade Commission at 877-438-4338, TTY 1-866-653-4261; [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft); 600 Pennsylvania Avenue, NW, Washington, DC 20580.



North Carolina Residents can obtain additional information about steps to prevent identity theft by contacting the Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001; visiting <http://www.ncdoj.com>; or calling (919) 716-6400.