



July 5, 2016

RECEIVED  
OFF OF THE ATTY GENERAL

2016 JUL 12 P 5:38

Attorney General Brian Frosh  
Maryland Attorney General  
200 St. Paul Place  
Baltimore, MD 21202

Dear Mr. Frosh:

We are writing to notify you of an unauthorized access or use of personal information involving one (1) Maryland resident.

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

On June 23, 2016 the Santander Bank Fraud Card Detection group discovered suspicious ATM withdrawals. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the ATM vestibule door of our ATM located at 901 West Park Avenue, Ocean, New Jersey. After reviewing video surveillance footage, it was determined that the device had been placed on the ATM vestibule door on May 6, 2016 and removed May 8, 2016. Furthermore, a camera device was installed in the ATM Light Lens. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number.

**NUMBER OF MARYLAND RESIDENTS AFFECTED:**

The incident affected one (1) Maryland resident. This resident will be receiving notice in a letter scheduled to be mailed on or about July 5, 2016. Enclosed, please find a sample of the letter that will be mailed to the affected resident.

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

This incident was identified by the Santander Bank Fraud Card Detection Department, 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 working closely with the United States Secret Service and continuing to monitor Santander Bank ATMs and vestibule doors and suspicious customer electronic transactions.

**CONTACT INFORMATION:**

Santander Bank values the security of its customers' information and regrets this unfortunate incident. Please contact James Massa, the Santander Bank Fraud Investigator assigned to this case, directly at (718) 355-6975 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**

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 <ATM Location> on <Month> <Day>, <Year> 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 <Month1> <Day1>, <Year1>.
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 <Month2> <Day2>, <Year2>; 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,

Helen Mazzitelli  
Executive Vice President, Director of Customer Experience  
Santander Bank, N.A.

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