



STATE OF NH
DEPT OF JUSTICE
2015 NOV -5 AM 11:43

November 2, 2015

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 two (2) New Hampshire residents.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS:

The incident was the result of improper use of customer information by a former employee, whereby it appears this individual inappropriately accessed customer information during the period between June and July 2015 for the purpose of selling the information to a third party. The former employee was discovered to have accessed electronic information and she may have printed out documents containing personal information. Multiple customers contacted the Santander Bank Fraud Prevention group during the timeframe July 2015 through September 2015 to dispute debit card transactions on their accounts. In each instance, it was determined through investigation that an unknown individual contacted the Customer Contact Center, provided data to the Bank to subvert existing authentication protocol, and changed the customer address and ordered a debit card for accounts accessed by the former employee. The personal information compromised included the customer's name, address, Social Security number, date of birth, and account numbers for any account relationship with the Bank.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED:

The incident affected two (2) New Hampshire residents. These residents were deemed to potentially be at risk for identity theft and/or fraud by our Fraud Prevention group because their accounts were viewed by the former employee on her last day of employment, July 24, 2015. Enclosed, please find a sample of the letter that will be mailed to the affected residents on or about November 4, 2015.

STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT:

This incident was identified by the Santander Bank Fraud Prevention group, escalated to the Bank's Privacy Office, and an investigation was initiated. By the time Fraud Prevention linked the employee to this incident, she was no longer employed by Santander Bank. She had given a two week notice in July 2015 and on her last day of employment the Bank terminated her for leaving work before her scheduled end time. We have evidence that the personal information was used for fraudulent purposes. The Bank is working closely with Rhode Island law enforcement, as well as continuing to monitor activities of its employees. The letter to the affected residents indicates that the Bank is offering one (1) year credit monitoring free of charge.

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



CONTACT INFORMATION:

Santander Bank values the security of its customers' information and regrets this unfortunate incident. Please contact Todd Swoyer, the Santander Bank Internal Investigations Manager, directly at (610) 208-6473 should you have any questions or require additional information.

Sincerely,

A handwritten signature in black ink that reads "Michelle Guttman".

Michelle Guttman
Chief Privacy Officer

Enclosures: Notification Letter to Affected Residents



<DATE>

<Name>

<Address>

<Address>

Dear <Customer Name>:

We are writing to inform you of a potential compromise of your personal information at Santander Bank. The categories of information could potentially include name, address, social security number, date of birth, and account information.

We sincerely apologize for any inconvenience or concern this situation may have caused and are ready to assist you in resolving any related issues. Santander Bank's Fraud Prevention and Security Department is working in conjunction with local law enforcement to investigate this incident.

To help protect your identity, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert (see attachment for details). This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. This is a service designed to help you monitor your Credit Reports and includes monthly updates of any inquiries or derogatory information being reported to your files. We also strongly recommend that you consider the Consumer Protective Measures described in the enclosed document (details included in the attachment).

For additional resources and information, you may also visit the Santander Identity Theft Center website at <https://www.santanderbank.com/us/personal/banking/online-and-mobile-banking/security-center/santander-identity-theft-assistance-center>.

Please be assured that we take the security of your information very seriously. If you have any questions about this letter, please visit your nearest branch or contact Fraud Prevention at 877-906-7500.

Sincerely,

A handwritten signature in black ink that reads "Helen Mazzitelli".

Helen Mazzitelli
Executive Vice President
Director of Customer Experience

CONSUMER PROTECTIVE MEASURES

In addition to our complimentary one-year membership of Experian's® ProtectMyID® Alert, we encourage you to consider taking the following steps:

- If you are a Santander checking customer regularly check your account activity by using Online Banking and by carefully reviewing your monthly statements;
- Report any suspected incidents of identity theft to local law enforcement and to Santander Bank immediately;
- Request a free credit report annually from each of the three main credit reporting agencies by going online at www.annualcreditreport.com;
- You may also contact the credit reporting agencies to place a Fraud Alert or a Security Freeze on your credit.
 - ✓ Equifax: 1-877-322-8228; www.equifax.com; Security Freeze, P.O. Box 105788, Atlanta, GA 30348
 - ✓ Experian: 1-888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
 - ✓ TransUnion: 1-888-909-8872; www.transunion.com; P.O. Box 6790, Fullerton, CA 92834
- 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; 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You can obtain information from these sources about the steps you can take to avoid identity theft. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy. You may want to consider placing a "Fraud Alert" or "Security Freeze" on your credit reports.

A Fraud Alert is a cautionary flag which is placed on your credit file to notify lenders and others that they should take special precautions to ensure your identity before extending credit. When you place a Fraud Alert, you can provide a mobile or other phone number for lenders to contact you to verify that the party applying for credit is actually you, not a fraudster. The three major credit reporting companies will share Fraud Alert information, so if you put a Fraud Alert on your credit report with any one, it will be recognized by the others and applied to your files. An initial Fraud Alert lasts for 90 days and may be renewed. Fraud Alerts are available at no charge to consumers who believe they may be victims.

A Security Freeze (also known as a Credit Freeze) is a more drastic step to protect your credit. A Security Freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a Security Freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. With a Security Freeze in place, even you will need to take special steps when you wish to apply for any type of credit. Because of more stringent security features, you will need to place a Security Freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files. A Security Freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services. For more information, go online and type "security freeze" into the search box on each site.





CREDIT MONITORING

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll By: XX/XX/2015 (Your code will not work after this date.)
2. VISIT the ProtectMyID Web Site to enroll: <http://protectmyid.com/redeem>
3. PROVIDE Your Activation Code: <code>

If you have questions or need an alternative to enrolling online, please call Experian at 888-451-6554 (toll-free) for calls made from within the U.S. or 479-573-7373 for calls made from outside of the U.S.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- Free copy of your Experian credit report
- Surveillance Alerts for:
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
 - **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 888-451-6554 (toll-free) for calls made from within the U.S. or 479-573-7373 for calls made from outside of the U.S.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.