

Ameriprise Financial, Inc.
1441 W. Long Lake Road, Suite 250
Troy, MI 48098



STATE OF NH
DEPT OF JUSTICE
2015 NOV 30 PM 12:19

November 25, 2015

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301

Re: Information Security Breach Notification

Dear Sir or Madam:

This letter is for the purpose of notifying your office that Ameriprise Financial Services, Inc. had a data breach incident involving information for (1) Ameriprise client who is a resident of New Hampshire. Specifically, On October 13, 2015, an advisor had problems with their computer and allowed a third party to connect to it to fix the issue. The connection allowed access to the files on their computer. Unfortunately, business files on the advisor's computer contained client names, address, dates of birth, Social Security and account numbers. There is no evidence to indicate that this client's information was accessed by the third party.

At the same time that this letter is being sent, Ameriprise Financial will also be sending a notification letter to the affected resident, a copy of which is enclosed. The letter describes steps Ameriprise Financial is taking to help ensure that this individual's accounts are not accessed by unauthorized persons and provides them with an opportunity to enroll for one year of credit monitoring from Equifax, at Ameriprise Financial's expense. In addition, we have included a copy of a brochure containing information about how to protect against identity theft.

If you have any questions regarding this incident, please contact me at (248) 205-5817.

Sincerely,

A handwritten signature in blue ink that reads "Kathleen A. Dedenbach".

Kathleen A. Dedenbach
Vice President & Group Counsel
Chief Privacy Officer
General Counsel's Organization
Ameriprise Financial, Inc.

KAD:jaw

Enclosures





<<Mail Date>>

<<First Name>><<Last Name>>
 <<Client Address 1>>
 <<City>>, <<ST>> <<ZIP>>

Dear<<First Name>> <<Last Name>>:

I am writing to make you aware of an incident involving your personal information. On October 13, 2015, I had problems with my computer and allowed a third party to connect to my computer to fix the issue. The connection allowed access to the files on my computer. Unfortunately, business files on my computer contained your name, address, date of birth, Social Security and account numbers. There is no evidence to indicate that your information was accessed by the third party, however, I wanted to take the precaution of notifying you.

We have also taken steps to protect your accounts from unauthorized activity, which includes instructing our service associates to use extra caution when verifying callers and to confirm the signature on written requests related to your accounts.

As a precaution, Ameriprise Financial is providing you an opportunity to enroll in an independently operated credit monitoring program for one year at no expense to you. This program is administered by Equifax, one of the three national credit reporting agencies. Equifax Credit Watch will provide you with an "early warning system" which alerts you to any changes to your credit file. The last page of this letter includes the features of the Equifax Service and the promotional code you need to use to enroll for one free year of coverage.

I recommend you take the following actions to help protect against the potential misuse of your personal information such as:

- Thoroughly review your account statements and transaction confirmations.
- Review any solicitations you receive in the near future.
- Closely monitor all of your personal accounts (e.g. checking and savings, credit cards, etc) to make sure there is no unauthorized activity.
- Read the enclosed educational brochure which provides resources and measures to help protect against identity theft.
- Be vigilant if you receive a call from someone who claims to represent Ameriprise Financial. If you have any doubts about the caller, hang up and call me to verify the validity of the call.

In the event that you experience fraud or theft as a direct result of this situation, please call the Ameriprise Financial Suspicious Activity Hotline immediately at (800) 862-7919, Ext. 11208 to speak with a fraud investigator.

If you have any questions, please do not hesitate to contact me at (315) 363-7701. Please accept my sincere apology regarding this situation and any inconvenience it may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Robert Tarry".

Robert Tarry, CFP
 Financial Advisor

Enclosure: Ameriprise Financial Identity Theft Brochure



Activation Code: **INSERT Credit Monitoring Code**

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian, and TransUnion** credit reports
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to \$1 million in identity theft insurance ¹ with \$0 deductible, at no additional cost to you
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert ² placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/tri

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.

Order Confirmation: This page shows you your under 18 years of age)

2 - The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

5. completed enrollment. Please click the “View My Product” button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided at the top of this letter.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

1 - Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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. This product is not intended for minors (

Red Flags of Identity Theft

- mistakes on your bank, credit card, or other account statements
- mistakes on the explanation of medical benefits from your health plan
- your regular bills and account statements don't arrive on time
- bills or collection notices for products or services you never received
- calls from debt collectors about debts that don't belong to you
- a notice from the IRS that someone used your Social Security number
- mail, email, or calls about accounts or jobs in your minor child's name
- unwarranted collection notices on your credit report
- businesses turn down your checks
- you are turned down unexpectedly for a loan or job

IDENTITY THEFT



WHAT TO KNOW



WHAT TO DO



Taking Charge:

What To Do If Your Identity Is Stolen

Available online at ftc.gov/idtheft

Order free copies at bulkorder.ftc.gov

FEDERAL TRADE COMMISSION
FTC.GOV/IDTHEFT
1-877-ID-THEFT (438-4338)

FEDERAL TRADE COMMISSION
FTC.GOV/IDTHEFT

What is Identity Theft?

Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:

- go through trash cans and dumpsters, stealing bills and documents that have sensitive information.
- work for businesses, medical offices, or government agencies, and steal personal information on the job.
- misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
- pretend to offer a job, a loan, or an apartment, and ask you to send personal information to “qualify.”
- steal your wallet, purse, backpack, or mail, and remove your credit cards, driver’s license, passport, health insurance card, and other items that show personal information.

How to Protect Your Information

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months.
To order, go to annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn’t come on time, contact the business.
- Shred all documents that show personal, financial, and medical information before you throw them away.
- Don’t respond to email, text, and phone messages that ask for personal information. Legitimate companies don’t ask for information this way. Delete the messages.
- Create passwords that mix letters, numbers, and special characters. Don’t use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has “https” at the beginning of the web address; “s” is for secure.
- If you use a public wireless network, don’t send information to any website that isn’t fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Set your computer’s operating system, web browser, and security system to update automatically.

If Your Identity is Stolen...

1 Flag Your Credit Reports

Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.

Equifax 1-800-525-6285
Experian 1-888-397-3742
TransUnion 1-800-680-7289

2 Order Your Credit Reports

Each company’s credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

3 Create an Identity Theft Report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- file a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

The two documents comprise an Identity Theft Report.

