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

Ameriprise Financial®

December 21, 2016

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

Fax: (603) 271-2110

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 (13) Ameriprise clients who are residents of New Hampshire. Specifically, on December 6, 2016, it was discovered that an external hard drive maintained by a franchise advisor's office was accessible via the internet. This was an isolated incident pertaining only to information this advisor maintained. The hard drive contained back-ups of financial documents, including names, addresses, dates of birth, account and Social Security numbers. While the information was not easily accessible and would require a person to search specifically for the port that contained the hard drive, it was immediately taken offline upon discovery.

After this letter was sent to your office, Ameriprise Financial also sent a notification letter to the affected residents, a copy of which is enclosed. The letter describes steps Ameriprise Financial is taking to help ensure that these individuals' 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,

Kathleen A. Dedenbach

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

KAD:jaw
Enclosures

1632 Client ID

Ameriprise Financial

<<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 December 6, 2016, it was discovered that an external hard drive maintained by my franchise office was accessible via the internet. This is an isolated incident pertaining only to information I maintained. The hard drive contained back-ups of financial documents, including names, addresses, dates of birth, and account and Social Security numbers. While the information was not easily accessible and would require a person to search specifically for the port that contained the hard drive, we immediately took it offline upon discovering the issue.

We take the security of your information very seriously and apologize for this incident. We have taken steps to protect your accounts from unauthorized activity, including 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 also 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 (508) 775-2399. Please accept my sincere apology regarding this situation and any inconvenience it may cause you.

Sincerely,

John Pupa
Financial Advisor

Enclosure: Ameriprise Financial Identity Theft Brochure

EQUIFAX®

1632 Client ID

Activation Code: INSERT Credit Monitoring Code

About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product	Equifax Credit Watch provides you with the following key features and benefits:
Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. Note: You must be over age 18 with a credit file in order to take advantage of the product.	o Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian,** and **TransUnion** credit reports o Wireless alerts and customizable alerts available (available online only) o One 3-in-1 Credit Report and access to your Equifax Credit Report™ o Up to $1 million in identity theft insurance [1] with $0 deductible, at no additional cost to you o 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. o 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	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. 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. 5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.	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 (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

How does identity theft happen?

- **Dumpster Diving**
  Rummaging through trash looking for bills or other documents with personal information — your name, address, phone number, utility service account numbers, credit card numbers and your Social Security number.
- **Phishing**
  Phone calls, spam emails or pop-up messages where criminals impersonate financial institutions or companies to persuade you to reveal personal information. For example, you may receive an email asking you to "update" or "confirm" your information and direct you to a website that looks identical to the legitimate organization's site. The phishing site is a phony site designed to trick you into divulging your personal information so the operators can steal your identity.

  If you believe a message to be phishing, forward it to spam@uce.gov and the legitimate company impersonated in the email. For any phishing email impersonating Ameriprise Financial, please send your message to anti.fraud@ampf.com.
- **Social Engineering**
  The misuse of a legitimate business by calling or sending e-mails that attempt to trick you into revealing personal information. For example, someone calls pretending to offer you a job and asks for your personal information, such as your Social Security number, to see if you "qualify" for the position.
- **Theft**
  Stealing or finding lost wallets and purses, as well as mail items such as bank and credit card statements, pre-approved credit offers, new checks or tax information. Thieves may also work for businesses, medical offices or government agencies, and steal information on the job.

Resources

You can find resources and information online and from government agencies about scams and crimes that can lead to identity theft.

Federal Trade Commission
Web: ftc.gov/idtheft
Phone: 1.877.ID-THEFT (438.4338)
or TTY 1.866.653.4261

OnGuard Online
Web: onguardonline.gov

Privacy Rights Clearinghouse
Web: privacyrights.org
Phone: 619.298.3396

US Postal Inspection Service
Web: usps.com/postalinspectors
Phone: 1.877.876.2455

US Secret Service
Web: secretservice.gov

Social Security Administration
Web: oig.ssa.gov
Phone-Fraud Hotline: 1.800.269.0271

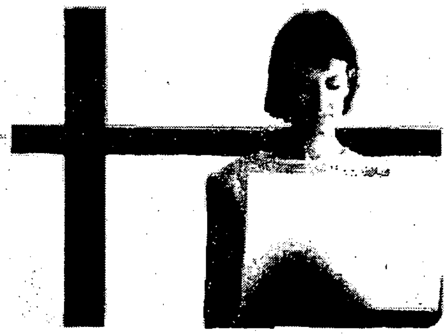
US Government Information and Services
Web: usa.gov
Phone: 1.844.872.4681

Identity Theft Resource Center
Web: idtheftcenter.org
Phone: 1.888.400.5530

Ameriprise Financial Services, Inc.
738 Ameriprise Financial Center, Minneapolis, MN 55474
ameriprise.com

200263 K (04/16)

Ameriprise Financial



Reduce your risk of identity theft

What is Identity Theft?

[illegible]

Protect your identity

- **Keep your information private.** Before disclosing any personal information, ensure you know why it is required and how it will be used.
  - Don't respond to email, text or phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the message.
- **Guard your Social Security number.** Do not give your Social Security number to people or companies you do not know.

  Request to see a privacy policy. A legitimate business requesting your Social Security number should have a privacy policy explaining why personal information is collected, how it's used, and who will have access to it.
- **Destroy old documents.** Shred information you no longer need that contains personally identifiable information and account numbers. For example, credit card receipts, billing statements and pre-approved credit offers should be shredded before you discard them.
- **Safeguard your mail from theft.** Promptly remove incoming mail from your mailbox or consider a locking mailbox, and place outgoing mail in post office collection boxes.
- **Carry only the essentials.** Do not carry extra credit cards, your birth certificate, passport or your Social Security card with you, except when necessary.
- **Review your credit report.** The law requires the three major credit bureaus — Equifax, Experian and TransUnion — to provide a free copy of your credit report once per year.
  - Visit annualcreditreport.com or call 1.877.322.8228 to order your free credit reports each year.
  - Consider staggering your credit report requests from each agency throughout the year. Look for inquiries and activity on your accounts that you can't explain.
- **Review your statements.** Carefully and promptly review all transaction confirmations, account statements and reports. Regularly review your account(s) by logging into the secure site at www.ameriprise.com. If you suspect or encounter any unauthorized activity on your Ameriprise Financial accounts, call your personal financial advisor or contact Client Service at 1.800.862.7919.

Protect yourself online

- Be wary of any unsolicited emails and offers that seem too good to be true. Never click on a link sent in an unsolicited email.
- If you are in doubt, don't reply. Call the institution at a known number.
- Use only secure websites when entering personal information or making online purchases. Secure websites can be recognized by the prefix https:// and a padlock icon in the status bar of the web browser.
- Avoid accessing your financial accounts online from public computers at libraries, hotel business centers or airports. These are prime target areas for thieves using keystroke monitoring tools to steal your usernames and passwords.
- Create unique passwords and personal identification numbers (PINs) using letters, characters and numbers.
- Use firewalls, anti-spyware and anti-virus software to protect your home computer and regularly update these programs.
- Educate yourself. There are educational materials about many of the online scams at onguardonline.gov.
- Limit the personal information you make public on social media sites, including information about leaving for vacation or information about your routines.

Red flags of identity theft

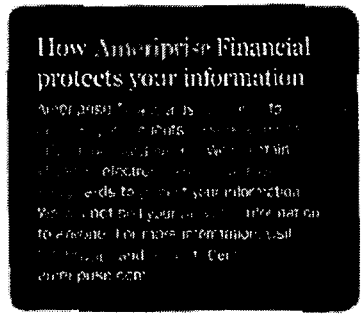
- Unauthorized charges on your bank, credit card or other accounts
- Mistakes on the explanation of medical benefits from your health plan
- Your regular bills and account statements don't arrive on time
- Bills or collection notices for products or services you never received
- Calls from debt collectors about debts that don't belong to you
- You are turned down unexpectedly for a loan or a job

What to do if your personal information is lost or stolen

- Contact one of the three major credit bureaus and request that a "fraud alert" is placed on your file. The alert instructs creditors to verify your identity via phone before opening any new accounts or making changes to your existing accounts.

Credit Bureaus	
Equifax	P.O. Box 740241 Atlanta, GA 30374 (800) 525-6285 equifax.com
Experian	P.O. Box 9554 Allen, TX 75013 (888) 397 3742 experian.com
TransUnion	2 Baldwin Place P.O. Box 1000 Chester, PA 19022 (800) 680 7289 transunion.com

- If you suspect or encounter any unauthorized activity on your Ameriprise Financial accounts, call your personal financial advisor or contact Client Service at 1.800.862.7919.



What to do if you are the victim of identity theft

If you discover that someone has used your personal information to open accounts or pursue unauthorized activity:

- **Contact a credit bureau.** Inform one of the three major credit bureaus that you are a victim of identity theft.
- **Place a freeze on your credit report.** Consider a credit monitoring service.
- **Contact your other financial institutions.** They may be able to provide additional security measures to protect your account. Close any accounts you suspect are fraudulent or have fraudulent transactions.
- **File a police report.** Identity theft is a crime and most creditors require a law enforcement report as proof of the theft.
- **Report the crime to the Federal Trade Commission (FTC).** Your report will aid law enforcement officials across the country in their investigations.
- **Seek assistance.** The FTC has created an identity theft information packet to assist victims. Request a packet via the contact options below:

  Web: ftc.gov/idtheft

  Phone: 1.877.ID-THEFT (438.4338)
  or TTY 1.866.653.4261
- **File a claim with your insurance carrier.** Check your policy or carrier to determine if you have identity theft insurance protection. If applicable, consider filing a claim.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police report, copies of disputed bills and any correspondence. Keep a log of your conversations with creditors, law enforcement officials and other relevant parties. Follow up all phone calls in writing and send correspondence via certified mail, return receipt requested.