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

Ameriprise Financial

July 13, 2017

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301
Phone: (603) 271-3643
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. [illegible] a data breach incident involving the theft of information for (1) Ameriprise client who is a resident of New Hampshire. Specifically, on February 10, 2017, a copy of an advisor's client [illegible] was uploaded to their personal email account as part of their transition to Ameriprise Fi[illegible] The client list included personal information. While there was no intent for misuse, it is [illegible] Ameriprise Financial policy to use unapproved email applications for documents containi[illegible] client information. The document has since been deleted from the personal email account.

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,

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

KAD:jaw

Enclosures

Ameriprise Financial

Date: July 14, 2017

<<First Name>> <<Last Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>

NOTICE OF A DATA BREACH	
What Happened?	I am writing to make you aware that on February 10, 2017, a copy of Jim Warren's client list was uploaded to his personal email account as part of his transition to Ameriprise Financial. The client list included personal information. While there was no intent for misuse, it is against Ameriprise Financial policy to use unapproved email applications for documents containing client information. The document has since been deleted from the personal email account. Out of an abundance of caution, I wanted to notify you of this issue.
What Information Was Involved?	The list contained your name, account and Social Security Numbers.
What We Are Doing.	As a precaution, we are 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. The last page of this letter includes the features of the Equifax Service and the promotional code you need to use to enroll for our free year of coverage.
What You Can Do.	• 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.
For More Information.	Please contact Jim Warren at (949) 462-9751 for any questions. I apologize for any inconvenience. Sincerely, Jennifer Swihart Sr. Investigator, Privacy Office Ameriprise Financial, Inc.

Activation Code: <<GIFT CODE>>

EQUIFAX®

About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product

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.

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

- Comprehensive credit file monitoring and autom alerts of key changes to your Equifax, Experia **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] wi deductible, at no additional cost to you
- 24 by 7 live agent Customer Service to ass understanding the content of your Equifa information, to provide personalized iden victim assistance and in initiating an investiga 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.
5. Order Confirmation: This page shows you your 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 enrollmen process. Note that all credit reports and alerts will s 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 p Equifax with your permission to access and to monitor your file. Without your Equifax cannot process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation th receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Custome Care letter with further instructions (if your identity can not be verified using the information provide Please allow up to 10 business days to receive 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 ac within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the frau added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud a on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and foll 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 a informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, cond 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 L.C

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

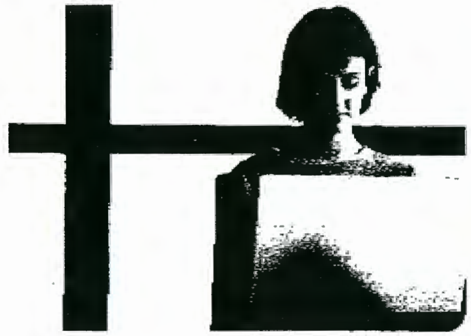
Identity Theft Resource Center
Web: idtheftcenter.org
Phone: 1.888.400.5530

Financial Planning | Retirement | Investments | Insurance

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

260253 K (04/16)

Ameriprise Financial



Reduce your risk of identity theft

What is Identity Theft?

Identity theft occurs when someone uses your name or personal information such as your Social Security, driver's license, credit card, telephone or other account number without your permission. Identity thieves use this information to open credit card and telephone service accounts, and make major purchases or withdrawals — all in your name. Information can be used to take over your existing accounts or open new accounts. Identity theft can result in damage to your credit rating and denials of credit and job offers. If this happens you can take steps to help undo the damages and restore your good name.

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 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

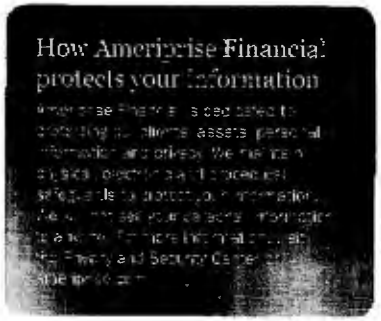
- Unauthorized charges on your bank, credit card or other accounts
- Mistakes on the explanation of medical benefits from your health plan
- Your regular bills and account statements don't arrive on time
- Bills or collection notices for products or services you never received
- Calls from debt collectors 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.