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

Ameriprise Financial

December 18, 2018

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. had a data breach incident involving information for (9) Ameriprise clients who are residents of New Hampshire.

Specifically, on November 11, 2018, a TIN Mismatch file was inadvertently emailed to an unsecure Gmail account. The email contained client name and social security number.

At the same time this letter is being sent, Ameriprise Financial will also be sending 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 through EZ Shield, 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

1632 <<Client ID>> <<Check Digit>> 001

NOTICE OF A DATA BREACH

Ameriprise Financial

<<Mail Date>>

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

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

What Happened?

I am writing to inform you of an incident involving your personal information. On November 11, 2018, an Ameriprise Financial employee inadvertently, emailed a list of client information to his personal email account. Upon discovery of the error, the employee's leaders watched as the employee deleted the email from his personal email account. Unfortunately, the list of information included your personal information. It is a violation of our internal policies, and disciplinary action has been taken. While there was no intent for misuse and the data has been deleted, Ameriprise Financial does not have a confidentiality agreement with the personal email provider, and we wanted to take the precaution of notifying you.

What Information Was Involved?

Name and Social Security Number.

What We Are Doing.

We have 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 EZ Shield, Inc. The services include resolution assistance by certified fraud experts, Internet Monitoring, and credit monitoring to keep you informed of changes to your information within the Experian credit bureau. To obtain these services, please go to https://myidentity.ezshield.com/protection and insert code: <<[redacted]>>

What You Can Do.

None of us like to hear about incidents involving our personal information. And in situations like this, taking a few prudent steps can further protect you against the potential misuse of your information. That's why we recommend the following actions:

- Register a Fraud Alert or Security Freeze with the three major credit bureaus listed below:

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

- Thoroughly review your account statements and transaction confirmations.

- Closely monitor all of your personal accounts (e.g. checking and savings, credit cards, etc) to make sure there is no unauthorized activity.
- Review any solicitations you receive in the near future.
- 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 your advisor to verify the validity of the call.
- Read the enclosed educational brochure which provides resources and measures to help protect against identity theft.
    - Additional information is available on ameriprise.com/privacy-security-fraud/
- The Federal Trade Commission also has many resources available to help protect against identity theft. Contact them at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 438-4338
identitytheft.gov

For More Information.

If you have questions, or notice any unusual activity, contact us at (800) 862-7919 and say "Privacy and Security" in the phone menu. We are here to help.

Please accept my sincere apology regarding this situation and any inconvenience it may cause you.

Sincerely,

Erik Langhus

Erik Langhus
Vice President
Ameriprise Financial, Inc.

Enclosure: Ameriprise Financial Identity Theft Brochure

1632 <<Client ID>> <<Check Digit>> 001

Residents of Iowa, Maryland, North Carolina and Oregon:

The Identity Theft Unit in your state gives you step-by-step advice on how to protect yourself and help you to address some of the issues that identity theft causes. Report suspected identity theft to your local law enforcement, the Attorney General and the Federal Trade Commission. Below are the mailing address, website, and phone number for the Office of the Attorney General of your state.

Iowa	Office of the Attorney General of Iowa Crime Victim Assistance Division Lucas State Office Building 321 East 12th Street Des Moines, IA 50319 (515) 281-5044 (800) 373-5044 iowaattorneygeneral.gov
Maryland	Office of the Attorney General of Maryland 200 St. Paul Place Baltimore, MD 21202 (410) 576-6491 oag.state.md.us
North Carolina	Consumer Protection Division of the Attorney General's Office Old Education Building 114 W. Edenton Street Raleigh, NC 27602 (919) 716-6400 ncdoj.com
Oregon	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (503) 378-4400 doj.state.or.us

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 popup 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 is phishing, forward it to spam@uce.gov and the legitimate company impersonated in the email. For any phishing e-mail 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

263283 K (04/16)

Ameriprise Financial

Reduce your risk of identity theft

What is Identity Theft?

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

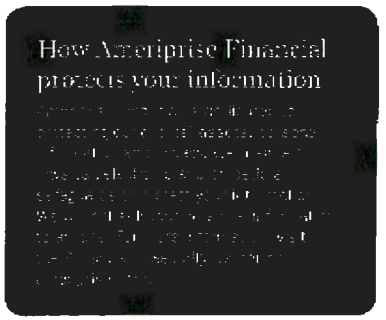
- Unauthorized charges on your bank, credit card or other accounts
- Mistakes on the explanation of medical benefits from your health plan
- Your regular bills and account statements don't arrive on time
- Bills or collection notices for products or services you never received
- Calls from debt collectors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