15521

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

<<Mail Date>>

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

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

I am writing to inform you of an incident involving your personal information. Your advisor, [redacted] recently started employment at a franchise office of Ameriprise Financial Services, Inc. When changing firms, [redacted] was allowed by her previous firm to retain information regarding her clients. That information was shared inappropriately with Ameriprise Financial on <<DATE>> to set up a client profile without your written consent. The data shared to set up the client profile included your name, address, date of birth, Social Security number and email address. Due to the sensitive nature of this information, I wanted to notify you of this incident.

While it is very unlikely that you will be a victim of identity theft as a result of this incident, as a precaution, Ameriprise Financial is providing you an opportunity to enroll in an independently operated credit monitoring program for two years at no expense to you. This program is administered by EZ Shield, Inc. The services include resolution assistance by certified fraud experts, Internet Monitoring which will alert you if your information is being traded on the dark web, 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: **<<GIFT CODE>>**

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

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze at no charge on their credit reports. 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.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze	Experian Security Freeze	Trans Union Security Freeze
P.O. Box 105788 Atlanta, GA 30348 www.freeze.equifax.com (800) 685-1111	P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze (888) 397-3742	P.O. Box 2000 Chester, PA 19022-2000 www.freeze.transunion.com (888) 909-8872

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

- 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

If you have any questions, please do not hesitate to contact me at (781) 849-9939. Please accept my sincere apology regarding this situation and any inconvenience it may cause you.

Sincerely,

Catherine Johnson
Registered Principal / Financial Advisor
Ameriprise Financial Services, Inc.

Enclosure: Ameriprise Financial Identity Theft Brochure

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

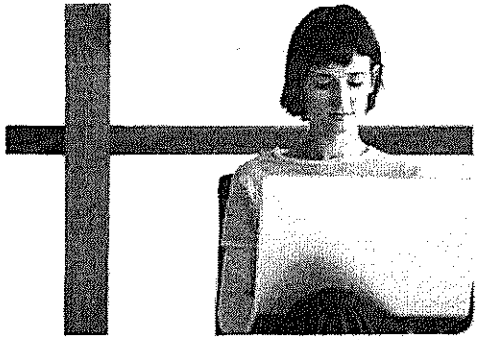
Identity Theft Resource Center
Web: idtheftcenter.org
Phone: 1.888.400.5530

Financial Planning | Retirement | Investments | Insurance

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

260263 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, bank account number, without your permission. Identity thieves use this information to open credit, bank 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 will take steps to help limit 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 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.

How Ameriprise Financial protects your information

Ameriprise Financial is dedicated to protecting our clients' assets, personal information and privacy. We maintain physical, electronic and procedural safeguards to protect your information. We will not sell your personal information to anyone. For more information, visit the Privacy and Security Center at ameriprise.com.

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.