Ameriprise Financial, Inc.
5222 Ameriprise Financial Center
Minneapolis, MN 55474

Ameriprise Financial

February 12, 2010

VIA US MAIL
New Hampshire Attorney General's Office
Department of Justice
33 Capitol 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 the theft of information for one (1) Ameriprise client who is a resident of New Hampshire.

On February 9, 2010, Ameriprise Financial Services sent a notification letter, a copy of which is enclosed, to the client. The letter describes steps Ameriprise is taking internally to help ensure that her accounts are not accessed by unauthorized persons and provides the client with an opportunity to enroll for one year of credit monitoring from Equifax, at Ameriprise's expense. In addition, we have included a copy of the brochure that was also sent to this resident containing information about how to protect against identity theft sent to this resident.

If you have any questions regarding this incident, please contact me at

Sincerely,

Jolene A. Neby, Paralegal
Manager of Legal Affairs
Ameriprise Financial, Inc.

:jan

Enclosures (2)

100%

< DATE >

< CLIENT NAME >
< CLIENT ADDRESS >
< CLIENT ADDRESS >

Dear < CLIENT NAME >:

I am sending this letter to inform you of an incident that occurred. Your REIT application was lost by an express mailing vendor en route to the REIT transfer agent. The application contains your name, address, Social Security Number and date of birth. The transfer agent did open your REIT account as originally intended.

Ameriprise Financial is taking prudent steps to protect your accounts from unauthorized activity.

As an additional precaution, Ameriprise Financial is providing you an opportunity to enroll in an independently operated credit monitoring program for one year. This program, which is offered to you at no cost, is administered by Equifax, one of the three national credit-reporting agencies. This service will provide you with an online solution which provides weekly credit monitoring of your Equifax credit file and one copy of your Equifax Credit Report™.

If you are interested in enrolling in the credit monitoring program Equifax has a simple Internet-based verification and enrollment process.

Visit: www.myservices.equifax.com/silver

1. Consumer Information: complete the form with your contact information (name, address and email address) and click "Continue" button. The information is provided in a secured environment.
2. Identity Verification: complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.
3. Payment Information: During the "check out" process, provide the following promotional code:

   < PROMOTIONAL CODE >

   in the "Enter Promotion Code" box (case sensitive, no spaces). After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)
4. Order Confirmation: – Click "View My Product" to access your Equifax Credit Report.

What other actions can you take to help protect against misuse of your personal information?

I ask that you thoroughly review your account statements and transaction confirmations, as well as any solicitations you receive in the near future. This includes callers who claim to represent Ameriprise Financial. The corporate office will not be calling you about this incident, so do not divulge any information to a caller who claims to be from the corporate office. In addition, you should closely monitor your personal accounts (e.g. checking and savings, credit cards, etc.) to make sure no one is attempting to use your information.

In addition, we are including an educational brochure developed at Ameriprise Financial that gives you resources and actions you can take to protect yourself from Identity Theft.

In the event that you experience fraud or theft as a direct result of this situation, please call the Suspicious Activity Hotline immediately at (800) 862-7919, Option 0, Ext. 16166 and leave an urgent message. One of our fraud investigators will return your call. Ameriprise Financial is committed to helping you address your situation and to pursuing corrective actions, if necessary.

If you have any additional questions please do not hesitate to contact a customer service representatives at 1 (800) 862-7919, Option 0, ext. 68321.

Our clients are top priority and I apologize for any inconvenience this incident may cause you.

Sincerely,

Dan McAskin
Vice President of Operations
Ameriprise Financial Services, Inc.

Enclosure: Ameriprise Financial Identity Theft Brochure

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, 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.

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**.

Protect your Social Security number

- Do NOT provide your Social Security number (SSN) to anyone, without confirming that it's absolutely necessary.
- Do NOT carry your Social Security card with you.
- Do NOT print your SSN (or telephone number) on your checks.
- Do NOT e-mail your SSN to anyone.
- Do NOT store your SSN on your computer.
- Do NOT use your SSN as a password.

What to do if your personal information is lost or stolen

- Contact the fraud department at 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	(800) 525-6285
Experian	(888) 397-3742
TransUnion	(800) 680-7289

- If you suspect or encounter any unauthorized activity on your Ameriprise Financial accounts, call your personal financial advisor or contact Client Service at **(800) 862-7919**.

How Ameriprise Financial protects your information

Ameriprise Financial is dedicated to protecting our clients' assets, personal information and privacy. We restrict access to non-public Client information to persons with a need to know that information. We maintain physical, electronic and procedural safeguards to protect your Client Information. We will not sell your personal information to anyone.

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.
- **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.
- **File a claim with your Identity Theft insurance carrier.** Most credit bureaus and some insurance agencies offer Identity Theft insurance.
- **Seek assistance.** The FTC has created an Identity Theft information packet to assist victims. Request a packet via the contact options below:

  Web: consumer.gov/idtheft
  Phone: (877) ID-THEFT (438-4338)
  or TTY (866) 653-4261

- **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.
- **Place a freeze on your credit report.** Some states have passed regulations allowing residents to place a freeze on their credit report. This prevents any new account (credit card, car lease, credit or savings, etc.) from being opened before "unfreezing" the credit report by personally verifying with the credit bureau. Contact your State Attorney General's office or the state PIRG Consumer Protection Organization's website at **pirg.org** to see if your state has this option available.

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**.
- **Changing Your Address** — Someone redirecting your billing statements to another location, without your consent, by completing a "change of address" form with the U.S. Postal Service or your financial institutions.
- **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.

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: consumer.gov/idtheft
Phone: (877) ID-THEFT (438-4338)
or TTY (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: Check for your local number in the blue pages of your phone book

Ameriprise Financial

260263 A (11/06