

Ameriprise Advisor Services, Inc.
 719 Griswold
 Suite 1700
 Detroit, MI 48226
 Tel: 313.628.1200
 Fax: 313.628.1583

July 14, 2010

YIAKATISPIRIE
 Office of the Attorney General
 Attn: Security Breach Notification
 200 St Paul Place
 Baltimore, MD 21202

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 three (3) Ameriprise clients who are residents of Maryland. A back-up hard drive used in an independent contractor's business was stolen. The hard drive contained historical Ameriprise Financial electronic files that listed the clients' names, social security numbers, and other financial information.

Ameriprise Financial Services will also be sending a notification letter to the clients, a copy of which is enclosed. The letter describes steps Ameriprise is taking internally 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's expense. In addition, we have included a copy of the identity theft brochure, which is also sent to the clients, containing information about how to protect against identity theft.

If you have any questions regarding this incident, please contact me at (313) 628-1200.

Sincerely,

Kevin A. Dedent
 Kevin A. Dedent, Counsel
 General Counsel's Organization
 Ameriprise Financial, Inc.

KAD:jo

Enclosures (3)



• Mail Item •

• First Name • Last Name •

• Street Address 1 •

• City, State, ZIP •

• First Name • Last Name •

I am writing to make you aware that a back-up hard drive I used in my practice was recently stolen. Unfortunately, the hard drive contained Ameriprise Financial electronic files which listed your name, address, Social Security Number, Ameriprise Financial account number, and other financial information that you provided to me. I want to let you know what we are doing to address the situation.

Ameriprise Financial is working closely with local law enforcement authorities in an effort to recover the stolen equipment. We have also taken steps to protect your accounts from unauthorized activity, which includes instructing our service associates to use extra caution when verifying calls and to confirm the signature on written requests related to your accounts. You will be prompted to provide an additional confidential phrase for authentication purposes. This will be sent to you in a separate mailing. Be sure to keep this information in a secure location for future reference.

As an additional 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 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 third page of this letter includes the features of the Equifax Service and the promotional code you need to use to enroll in one free year of coverage.

I request 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.

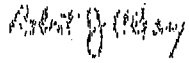
In addition, as a resident of Maryland, the Identity Theft Unit in your state gives you step-by-step advice on how to protect yourself and help you to address some of the issues that identity theft causes. Below is the mailing address, website, and phone number for the Office of the Attorney General of Maryland if you have any questions regarding identity theft in your state.

Office of the Attorney General of Maryland
 700 St. Paul Street
 Baltimore, MD 21202
 (410) 576-6471
 Website: www.oag.state.md.us

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 (610) 834-7385. Please accept my sincere apology regarding this situation and any inconvenience it may cause you.

Sincerely,



Robert Cloney

Senior Financial Advisor with Ameriprise Financial Services, Inc.

Equifax Credit Watch provides you with a 1 year membership service:

- Comprehensive credit file monitoring of your Equifax, Experian, and TransUnion credit reports with daily notification of key changes to your credit files from any of the three agencies.
- Weekly alerts and customizable alerts available
- One Free Credit Report and unlimited access to your Equifax Credit Report™
- \$20,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- 24 hr 7 day 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.

Please choose one of the Enrollment Options below:

Option 1: Online Enrollment: Equifax has a simple Internet-based verification and enrollment process. You will need to complete the below steps for each promotional code provided.

Visit www.equifax.com/eqwatch

1. **Registration Information:** complete the form with your contact information (name, address and e-mail 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:

<CONSENT PROMOTIONAL CODE>>

to the "Enter Promotion Code" box. (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.)

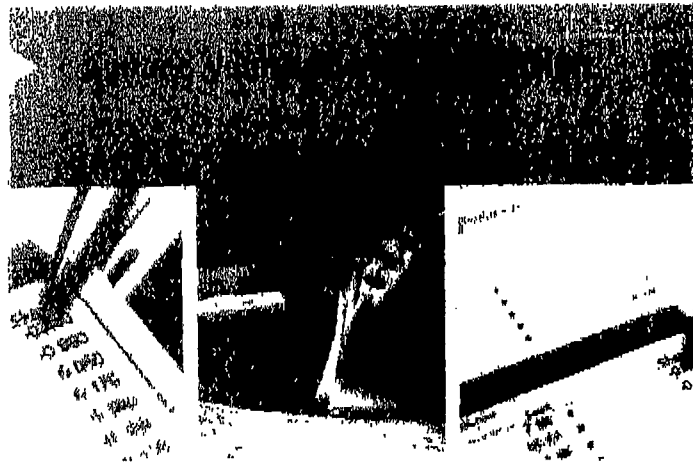
1. **Make Confirmation:** Click "View My Product" to access your 3-in-1 Credit Report.

Option 2: Home Enrollment for US Mail delivery of the alerts and credit reports

Use 1-800-927-8432 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. **Promotional Code:** You will be asked to enter your promotion code as shown above (no spaces)
2. **Contacting Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Eligible Resident:** 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. **Make 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).

† Equifax is not an insurer. This is a Personal Auto Master Policy underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates. Equifax is not an insurer. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on our underwriting qualifications and state regulations. Coverage not available for residents of New York.



What is Identity Theft?

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.

Protect your Identity

- **Keep your information private.**
Before disclosing any personal information, you know why it is required and how it will be used.
- **Check your Social Security number.**
Do not give your Social Security number to companies that you do not know.
- **Destroy old documents.**
Shred information you no longer need that potentially identifies information and Social Security numbers. For example, credit card receipts, statements and pre-approved credit offers should be shredded before you discard them.
- **Stop your mail from theft.**
Promptly remove incoming mail from your mailbox or postoffice or holding mailbox, and place outgoing mail in post office collection boxes.
- **Carry only the essentials.**
Do not carry your credit cards, your birth certificate, passport or your Social Security card with you, except when you need it.
- **Review your credit report.**
The law requires the three major credit bureaus -- Equifax, Experian and Trans-Union -- to provide a free copy of your credit report once per year.
- Visit annualcreditreport.com or call (877) 839-8228 to order your free credit reports each year.
- Cancel or registering your credit report requests from each agency throughout the year. Look for irregular and activity on your accounts that you can't explain.
- **Review your statements.**
Carefully and promptly review all transaction confirmations, account statements and reports. Register on the My Financial Accounts website at myfinancialaccounts.com and regularly review your account activity. Report any errors or questions you have on your accounts to your Ameriprise financial advisor or contact Client Services at (800) 862-7919.

Protect yourself online

- Be wary of any unsolicited emails that seem too good to be true. Never click on links in an unsolicited email.
- If you are in doubt, don't reply. Call the number in 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 your 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, numbers, characters and symbols.
- 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" be 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.



- Equifax (800) 685-1235
- 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) 667-7019.

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.

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

