



Fax

To: <i>Office of A/C</i>	From: <i>K. Dedembeck</i>
Fax: <i>605 2236202</i>	Phone:
Date: <i>11/10/15</i>	Pages: <i>7</i>

Urgent Per Your Request For Review Please Reply

Comments:

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



November 10, 2015

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301
Fax: (603) 223-6202

Re: Information Security Breach Notification

Dear Sir or Madam:

This letter is for the purpose of that Columbia Threadneedle Investments had a data breach incident involving (2) Columbia Threadneedle Investments clients who are residents of New Hampshire. Specifically, on October 12, 2015, a scanning error occurred with our vendor and our clients' Future Scholar paperwork was inadvertently scanned and uploaded to a different investment advisory firm. The investment advisory firm reported the error to our mutual vendor and they immediately corrected the error.

At the same time that this letter is being sent, Columbia Threadneedle Investments will also be sending a notification letter to the affected residents, a copy of which is enclosed. The letter describes steps Columbia Threadneedle Investments 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 from Equifax, at Columbia Threadneedle Investments' expense. In addition, we have included a copy of a brochure containing information about how to protect against identity theft.
notifying your office

If you have any questions regarding this incident, please contact me at (248) 205-5817.

Sincerely,

A handwritten signature in cursive script that reads "Kathleen A. Dedenbach".

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

KAD:jaw

Enclosures





<<Mail Date>>

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

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

I am writing to make you aware of a situation involving your personal information. On October 12, 2015, a scanning error occurred with our vendor and your Future Scholar paperwork was inadvertently scanned and uploaded to a different investment advisory firm. The investment advisory firm reported the error to our mutual vendor and they immediately corrected the error. We believe this situation poses an extremely low risk, however, the personal information that may have been viewed included your name and Social Security number.

As a precaution, we are providing you with 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. 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. The last page of this letter details out the instructions and promotional code you need to enroll for one free year of coverage.

You also may consider taking the following actions to help protect against the potential misuse of your personal information:

- 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.
- Read the enclosed brochure with resources and tips to help protect against identity theft.
- Review any solicitations you receive in the near future, including calls from someone who claims to represent Columbia Threadneedle. If you have any doubts about the caller, hang up and call us to verify the validity of the call.

In the event that you experience fraud or theft as a direct result of this situation, or if you have questions, please call us at (888) 244-5674. Our representatives are available Monday through Friday from 8 a.m. until 8 p.m. Eastern Time and will be happy to assist you.

Sincerely,

Veronica Seaman
Vice President
Columbia Threadneedle Investments

Enclosure: Columbia Threadneedle Identity Theft Brochure



Activation Code: <<INSERT Credit Monitoring Code>>

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:

- o Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian, and TransUnion** credit reports
- o Wireless alerts and customizable alerts available (available online only)
- o One 3-in-1 Credit Report and access to your Equifax Credit Report™
- o Up to \$1 million in identity theft insurance¹ with \$0 deductible, at no additional cost to you
- o 24 by 7 live 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.
- o 90 day Fraud Alert² 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 enrollment process. Note that all credit reports and alerts will be sent 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 provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order 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). Please allow up to 10 business days to receive this 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 activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow 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 and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of 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 LLC



FUTURE SCHOLAR
529 COLLEGE SAVING PLAN



Your success. Our priority.

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. If this happens, you can take steps to help limit the damages and restore your good name.

How does identity theft happen?

<p>Dumpster diving</p>	<p>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 (SSN).</p>
<p>Phishing</p>	<p>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 Columbia Threadneedle Investments, please send your message to service.inquiries@columbiathreadneedle.com.</p>
<p>Social engineering</p>	<p>Someone may pretend to offer you a job or an apartment and ask you to send personal information to qualify. The misuse of a legitimate business, calling or sending emails that attempt to trick you into revealing personal information.</p>
<p>Theft</p>	<p>Stealing or finding lost wallets and purses, as well as mail items such as bank and credit card statements, preapproved credit offers, new checks or tax information. Thieves may also work for businesses, medical offices or government agencies and steal information on the job.</p>

How we protect your information

We are 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 information. We will not sell your personal information to anyone.

REDUCE YOUR RISK OF 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 and phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the message.

■ **Guard your SSN**

Do not give your SSN to people or companies that you do not know. Do **not** provide your SSN to anyone, without confirming that it's absolutely necessary.

■ **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 preapproved 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 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 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. Register for access to your accounts at columbiathreadneedle.com/us and regularly review your account activity. Report any errors or questions you have on your accounts to your financial professional or contact our shareholder call center at 888.244.5674.

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 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.

Credit bureaus

- Equifax: 800.525.6285
- Experian: 888.397.3742
- TransUnion: 800.680.7289
- If you suspect or encounter any unauthorized activity on your accounts with us, call your financial professional or our shareholder call center at 888.244.5674.

**REDUCE YOUR RISK
OF IDENTITY THEFT****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 your other financial institutions**
They may be able to provide additional security measures to protect your account.
- **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**
Check your policy or carrier to determine if you have identity theft insurance protection. If applicable, consider filing a claim.
- **Contact the financial institution and close any accounts you suspect are fraudulent or have fraudulent transactions.**
- **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: 877.ID.THEFT (438.4338)
 - 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 and consider a credit monitoring service.**

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: 877.ID.THEFT (438.4338)

TTY: 866.653.4261

OnGuard Online

Web: onguardonline.gov

Privacy Rights Clearinghouse

Web: privacyrights.org

Phone: 619.298.3396

U.S. Postal Inspection Service

Web: usps.com/postalinspectors

Phone: 877.876.2455

U.S. Secret Service

Web: secretservice.gov

Social Security Administration

Web: ssa.gov/oig

Phone: 800.269.0271

(Fraud hotline)

**Your local Department of
Motor Vehicles****Federal Government
Information Center**

Web: usa.gov

For passport concerns

Web: travel.state.gov

Phone: 877.487.2778

Identity Theft Resource Center

Web: idtheftcenter.org

Phone: 888.400.5530

To find out more, call 888.244.5674
or visit columbiathreadneedle.com/us
blog.columbiathreadneedle.us

Not FDIC Insured • No bank guarantee • May lose value

Columbia Management Investment Distributors, Inc., member FINRA, is the distributor and underwriter for the Columbia Management Future Scholar 529 College Savings Plan Financial Advisor Program. The Office of State Treasurer of South Carolina (the State Treasurer) administers the Program and has selected Columbia Management Investment Advisers, LLC and Columbia Management Investment Distributors, Inc. (Columbia Management) as Program Manager. Columbia Management and its affiliates are responsible for providing certain administrative, recordkeeping and investment services, and for the marketing of the Program. Columbia Management is not affiliated with the State Treasurer.

Columbia Threadneedle Investments (Columbia Threadneedle) is the global brand name of the Columbia and Threadneedle group of companies.

Columbia funds are distributed by Columbia Management Investment Distributors, Inc., member FINRA, and managed by Columbia Management Investment Advisers, LLC.

Columbia Management Investment Distributors, Inc., 225 Franklin Street, Boston, MA 02110-2804

© 2015 Columbia Management Investment Advisers, LLC. All rights reserved.

