

March 27, 2018

VIA OVERNIGHT DELIVERY

Attorney General Gordon J. MacDonald
Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, New Hampshire 03301

RECEIVED
MAR 28 2018
CONSUMER PROTECTION

RE: Data Incident Notification

Dear Attorney General MacDonald:

Our firm represents The Retirement Advantage, Inc. (“TRA”), a Wisconsin corporation. Our client hereby formally submits notification of a recent data incident, pursuant to N.H. Rev. Stat. Ann. §359-C:20. TRA reserves the right to supplement this notice with any new significant details learned subsequent to this submission. By providing this notice, TRA does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire notification of security breach statute, all other laws or personal jurisdiction.

Applied Plan Administrators (“APA”), a division of TRA, recently fell victim to a phishing attack which resulted in unauthorized access to one APA email account. On February 12, 2018, TRA became aware of potentially suspicious activity in that APA email account and promptly took responsive action to resolve the threat at that time. Promptly thereafter, TRA engaged our firm as legal counsel and a third party forensics firm to investigate the incident. On February 23, 2018, the forensics firm determined that there was unauthorized access to the single APA account from February 10, 2018 through February 12, 2018. The forensics firm did not find any evidence that other APA email accounts or APA systems were affected. Furthermore, the forensics firm uncovered no evidence that personally identifiable information was accessed or acquired as a result of this incident.

Out of an abundance of caution, however, TRA has decided to notify potentially affected residents of New Hampshire -- via letter to be mailed on or about March 29, 2018 -- that their personal information could have been accessed given that the APA email account in question contained files that included personal information such as, names, addresses, social security numbers, dates of birth, and financial information such as account numbers. Please see a sample customer notification letter, attached hereto as Exhibit A.

TRA will be notifying approximately eight (8) New Hampshire residents and will be offering free credit monitoring to each individual for a twelve (12) month period. TRA will also

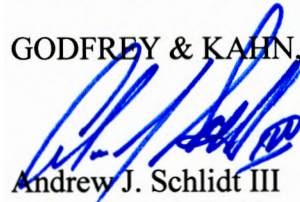
March 27, 2018
Page 2

provide a dedicated call center that potentially affected individuals may call with questions regarding the incident. Furthermore, TRA will continue to work with its consultants to identify and implement measures to further mitigate future threats.

Please do not hesitate to contact me if you have any questions regarding this matter.

Very truly yours,

GODFREY & KAHN, S.C.



Andrew J. Schlidt III
Attorney Shareholder

AJS:

EXHIBIT A

Sample Customer Notification Letter



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name1>>
<<Address1>>
<<Address2>>
<<Address3>>
<<City>>, <<ST>> <<ZIP>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name>>:

Securing and protecting the data of our customers is a top priority for The Retirement Advantage, Inc. ("TRA"). TRA is or was previously the third party administrator for your current or prior employer's 401(k) retirement plan. Regrettably, we are contacting you to let you know of a recent incident at Applied Plan Administrators ("APA"), a division of TRA, which may have involved the unauthorized disclosure of your personal information.

WHAT HAPPENED?

On February 12, TRA noticed suspicious activity on an APA employee's email account and immediately secured the account. Shortly thereafter, TRA engaged counsel and an outside forensic consulting firm to investigate the suspicious activity. On February 23, 2018, the forensic firm determined that a third party gained unauthorized access to one APA employee's email account on February 10, 2018, using a phishing attack. The forensic firm uncovered no evidence that the attacker accessed or acquired specific records in the employee's email account containing personally identifiable information. Furthermore, TRA has not been notified of any fraud arising from this incident. Nonetheless, TRA is providing you notification of this incident to ensure that you can take precautionary measures to the extent that you wish to do so. Please note this incident was limited to unauthorized access to an APA email account. This incident did not involve unauthorized access to your 401(k) account as administered through your employer's 401(k) retirement plan.

WHAT INFORMATION WAS INVOLVED?

The personally identifiable information potentially involved includes your name, address, Social Security number, financial institution information and other similar personal financial information.

WHAT WE ARE DOING

We take this incident, and the security of your information, very seriously. In addition to immediately securing the affected email account, we are taking additional measures designed to ensure another incident does not happen again, including reviewing our existing security practices and procedures. To help relieve concerns and restore confidence following this incident, we have arranged for you to enroll, **at no cost to you**, in an online credit monitoring service *myTrueIdentity* for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

Complimentary Credit Monitoring Service

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space "Enter Activation Code", enter the following 12-letter Activation Code <<Insert Unique 12- letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

WHAT YOU CAN DO

In addition to signing up for *myTrueIdentity*, we encourage you to review the information below for ways to further protect your identity.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely for the next 12 – 24 months. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to <http://www.IdentityTheft.gov> or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Take Advantage of Additional Free Resources on Identity Theft

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; <http://www.IdentityTheft.gov>; 1-877-ID THEFT (1-877-438-4338); and TTY: 1-866-653-4261. A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.

The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General.

Consider a Security Freeze on Your Credit File

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
<http://transunion.com/freeze>
1-888-909-8872

1. Your name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
2. Your Social Security Number
3. Your date of birth (month, day and year)
4. Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
5. If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees or Security Freeze services. Forms of payment are check, money order, or

credit card, or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are the victim of identity theft and are eligible for free Security Freeze Services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.

For New Mexico Residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have the right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Rhode Island Residents: If you are the victim of identity theft, the placement, temporary lifting, and removal of a credit freeze is free. If you are not a victim of identity theft, the placement and temporary lifting of a credit freeze is \$10.00, removing the credit freeze is free.

ADDITIONAL INFORMATION

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at <http://www.transunion.com/childidentitytheft> to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this incident.

For Maryland Residents: Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

For Rhode Island Residents: Rhode Island residents may obtain additional information about identity theft by contacting the Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400, or online at <http://www.riag.ri.gov>. Approximately seven (7) Rhode Island residents were potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud.

For North Carolina Residents: North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

For California and Wyoming Residents: This notice has not been delayed as a result of a law enforcement investigation.

FOR MORE INFORMATION

TRA sincerely apologizes for any inconvenience and concern this incident may cause you. If you have additional questions, please contact us at 888-715-9279, Monday through Friday, 6:00 a.m. to 6:00 p.m. PST.

Sincerely,

Michelle Zentner
Director of Operations
The Retirement Advantage, Inc. (TRA)