Principal Financial Group
711 High Street
Des Moines, IA 50392

VIA EMAIL (attorneygeneral@doj.nh.gov)

May 7, 2020

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of website issue

Dear Attorney General MacDonald:

I am writing to inform you of an issue that occurred regarding personal information of 14 residents. On November 23, 2019, we updated a portion of our website, Principal.com. We later determined that a software coding issue was intermittently resulting in instances where a single webpage containing information related to another Principal® customer's account may have been displayed while a customer was navigating in his or her own account. Information displayed included name, Social Security number and sometimes other identifiable information. New code was installed on January 6, 2020, which fixed the issue.

After receiving a limited number of reports from Principal customers about this issue (as of January 3, 2020, 8 Principal customers had reported seeing information displayed from a different account out of approximately 11 million logins since November 23, 2019), we conducted an investigation to determine if additional instances could be identified after the software update, prior to the fix. Our investigation took substantial time and effort, and we are now confident we have identified the full group of retirement plans and participants that may have had information inadvertently displayed to another customer.

In each occurrence, a single webpage containing personal information was potentially displayed to one Principal customer. To be clear, the individual to whom the webpage was misdirected could not make any changes or initiate any transactions in any other customer's account. Nor could the individual access or navigate within another customer's account. If the individual tried to click on a link or navigate on the webpage, they would have received an error or simply received their own account information. Given the circumstances, we believe it is very unlikely that the displayed data will be misused.

After thorough investigation, we do not believe there was an acquisition of any inadvertently displayed information, nor do we believe there is any likelihood of harm to the individuals whose personal information was displayed. Out of an abundance of caution, however, the retirement plan sponsor whose participants' information was displayed have asked us to notify those participants of the occurrence and offer them credit monitoring services. A copy of the notification letter sent to affected participants is attached. We are correspondingly providing you with this information.

How Discovered – Reports received through our Corporate Contact Center.

Has lost, stolen, or breached information been recovered – N/A

Have individuals involved in the incident (both internal and external) been identified – Yes

Has a police report been filed – No

Type of information lost, stolen or breached – No information was lost, stolen or breached. Information potentially inadvertently displayed included name and Social Security.

Was information encrypted – No

Lost, stolen or breached information covers what period of time – December 16, 2019

How many New Hampshire residents affected – 14

Results of an internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed – All procedures were followed. We conducted a variety of tests before this software was introduced to our website, and we have now updated our testing to account for this exact scenario. However, because this issue was very unique and occurred so infrequently given the volume of activity our website experiences, the issue was not identified during testing.

Regulated entity contact person for the Department to contact regarding the incident – Michele Ramsey, AVP – Chief Privacy Officer.

Please do not hesitate to contact me if you have questions.

Sincerely,

/S/ Michele M. Ramsey

Michele M. Ramsey
AVP - Chief Privacy Officer
Principal Financial Group
Des Moines, Iowa 50392-0300
(515) 248-0406
FAX (866) 496-6527
ramsey.michele@principal.com

Attachment

Principal Financial Group
711 High Street
Des Moines, IA 50392

April 28, 2020

[Participant name]
[Participant address]
[Participant address]

Dear

Keeping your retirement account information safe and secure is a high priority. That's why we're making you aware of an issue that occurred within our website, which involved your personal information.

What happened?

In late 2019, we updated a portion of our website. We later determined that a software coding issue was intermittently resulting in instances where a customer navigating within their own account on our website would inadvertently be shown a single webpage containing information related to another Principal® customer's account. On December 16, 2019, we believe a single webpage that included your personal information was misdirected to a Principal.com user while he was navigating in his own online account. We have since fixed the website code that caused this issue. Our forensics review indicates that the misdirected webpage, if it was displayed at all, was only displayed for a few seconds. In addition, the Principal.com user who received the misdirected webpage has stated that he does not remember ever seeing the information. Out of an abundance of caution, however, we are writing to make sure you are aware that this issue occurred.

What information was involved?
We've identified that your name, Social Security number, and birthdate was among the information misdirected to another customer.

Although a single webpage containing your information may have been displayed to another Principal customer, that individual wasn't able to access or navigate within your account. If the individual tried to click on a link or navigate on the webpage, they would've received an error or simply received their own account information. To be clear, the individual couldn't make any changes or initiate any transactions in your account. Given the circumstances, we believe it's very unlikely that the information will be misused.

Why does Principal have my personal information?
Principal is the recordkeeper for the Knight-Swift Transportation Holdings Inc. Retirement Plan. As the recordkeeper, Principal maintains certain personal information about Knight-Swift's current and former employees. After we learned that this issue had occurred, we contacted the plan administrator. After explaining what had occurred, the plan administrator asked us to notify you.

What are we doing now?
We take the privacy of our customers' account information very seriously.

We realize the expectations you have of us (and rightfully so), so please know that we're confident we've resolved the issue and have the right measures in place to help make sure this doesn't happen again. Additionally, as part of our normal protocols, an independent auditor reviews and evaluates our security measures on an ongoing basis.

We want you to feel comfortable with the security of your account, so we're extending you an offer for a one-year subscription to Equifax Credit Watch (a credit monitoring service)—which alerts you to certain changes or activity in your credit file. (See attachment for additional information.) This service also provides identity theft insurance. Here's how you can sign up for this service (at no cost to you):

- Visit www.myservices.equifax.com/tri
- Enter your activation code: [code]

What can you do?
We believe it's very unlikely your information will be misused, but in addition to the credit monitoring service offered, you may choose to:

- Review your account statements often and report any suspicious activity immediately to the service provider.
- Protect all your accounts with a personal identification number (PIN) or password. Don't use any part of your Social Security number as a PIN or password.
- Update your current passwords for your online accounts.

Protect yourself from identity theft by reviewing and acting upon Federal Trade Commission information, which can be found at www.consumer.gov/idtheft or by calling 1-877-FTC-HELP (1-877-382-4357). If you suspect your identity has been stolen, contact the Federal Trade Commission at 1-877-ID-THEFT (1-877-438-4338).

Questions?
We understand. Here are a few questions you might have:

Was this a cybersecurity attack?
No. This issue was not the result of an attack or infiltration of our network. The issue was due to a portion of code used within our website that caused certain webpage responses to be misdirected.

Was my account information made public to everyone?
No. Your account information was only potentially displayed on one webpage to one Principal customer while he was logged into his own account.

Could the customer who saw my account information take control of my account?
No. That individual wasn't able to access or navigate within your account. If the individual tried to click on a link or navigate on the webpage, they would've received an error or simply received their own account information. To be clear, the individual couldn't make any changes or initiate any transactions.

Did you test the software before it was released?
Yes, we conducted a variety of tests before this software was introduced to our website. And we've updated our testing to account for this exact scenario. However, because this issue was very unique and occurred so infrequently given the volume of activity our website experiences, the issue was not identified during testing.

Your security is our priority and we appreciate the trust you place in us. If you have more questions, please call us at 800-986-3343.

HZ3421B | 1112406-032020 | 03/2020

Other Important Information

Product Information

Equifax® Credit Watch™ Gold with 3-in-1 Credit Monitoring provides you with the following key features:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, Transunion®, and Experian® credit reports
- One Equifax 3-Bureau credit report
- Automatic Fraud Alerts[2] with a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax® credit report
- Up to $1 MM Identity Theft Insurance[3]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/tri

1. **Welcome Page:** Enter the Activation Code provided above 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 Username and Password, review the Terms of Use and then check the box to accept 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 Gold with 3-in-1 Credit Monitoring 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 Activation Code provided above.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.

1. Credit monitoring from Experian® and Transunion® will take several days to begin.

2. The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

3. Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. 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.

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.

There are other steps you can take to further protect yourself against identity theft or other unauthorized use of personal information if you are concerned.

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 90-day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call our 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. Fraud alerts last 90 days unless you manually renew it or use the automatic fraud alert feature within your Credit Watch subscription.

Experian	Equifax	TransUnion
(888) 397-3742	(877) 478-7625	(800) 680-7289
P.O. Box 9532	P.O. Box 740241	P.O. Box 6790
Allen, TX 75013	Atlanta, GA 30374-0241	Fullerton, CA 92834-6790
www.experian.com	www.equifax.com	www.transunion.com

- You can obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or online at: www.annualcreditreport.com. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three major credit reporting agencies. You may want to obtain copies of your credit report to ensure the accuracy of the report information.

- To learn more about protecting yourself from identity theft and to report incidents of identity theft, please contact the following:

Federal Trade Commission
1-877-ID-THEFT (1-877-438-4338)
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft, or www.ftc.gov/credit

Directions for placing a security freeze on your credit report

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
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834

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 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.

Maryland Residents: You may obtain information about preventing identity theft from the Maryland Attorney General's office: Attorney General of Maryland, Attn: Security Breach Notification, 200 St. Paul Place, Baltimore, MD 21202, Toll Free 1-888-743-0023 / TDD: 410-576-6372, idtheft@oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report filed regarding 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 (see details above for placing a security freeze) on their credit reports at no cost to the consumer. 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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, Toll Free 1-877-566-7226 / TDD 916-716-6000, www.ncdoj.gov/.