Russell Investments

1301 Second Avenue
Seattle, WA 98101

tel 206-505-7877
fax 206-505-3495
toll-free 800-426-7969

www.russellinvestments.com

March 7, 2017

The Honorable Bob Ferguson
The Washington State Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Via Email: SecurityBreach@ATG.wa.gov

Dear Mr. Attorney General Ferguson:

We are writing to notify you of a breach of security with respect to personal information involving 1,291 Washington residents.

On February 22, 2017, Russell Investments discovered that it experienced a data breach when a Russell Investments employee sent files containing personal information to a personal Gmail account and downloaded those files to a personal computing device. This file transfer triggered a security monitoring alert indicating the breach of personal information. Forensic analysis indicates the personal information relates to certain Russell Investments' U.S.-based employees and certain of their dependents.

One thousand two hundred and ninety-one individuals residing in Washington were affected by this incident. Shortly after this notification to you, the 1,291 individuals residing in Washington who are affected by this incident will receive in writing, via U.S. mail, one of three types of Data Breach Notices. These notices will offer credit monitoring services to the affected individuals. Individuals who are enrolled in a Premera health insurance plan will receive credit monitoring services through Premera, while all other affected individuals will receive similar services from Equifax. These notices are identical except with respect to the provider of the credit monitoring services being offered, and in the case where Equifax is the provider, those notices are further divided into a notice for adults and a notice applicable to minors. A sample copy of the forms of notice are attached to this notification.

Immediately following the security monitoring alert on February 22, 2017, Russell Investments' Information Security and Incident Response team investigated and mitigated the data breach. After discovery of this issue, the primary objectives were reducing the risk of misuse of the personal information; removing the personal information from non-Russell Investments managed devices and cloud accounts; ascertaining the exact personal information involved and which people were affected by the breach of personal information; and rotating the privileged credentials and keys. Russell Investments successfully achieved these objectives.

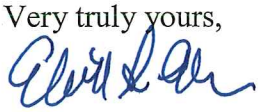
Since Russell Investments swiftly discovered the data breach, understood exactly what happened, where the breached personal information resided, and obtained the full cooperation of

the employee who caused the data breach in successfully remediating the breach, we did not need to involve any law enforcement agencies in this incident. While Russell Investments believes that there is limited risk that the personal information could be compromised and misused, we are providing each person affected by this data breach with two years of no-cost credit monitoring services and informing them of other steps that these persons can take to prevent identity theft.

In an effort to avoid any similar data breach in the future, Russell Investments is considering: revisions to human resources' policies; revisions to IT polices related to privileged systems access by employees; implementing new data loss prevention functionality in our computer systems; blocking access to unapproved online storage services; and enhancements to our virtual private network used for remote access to employees' work environments.

If you have any questions or concerns, please contact me at (206) 505-4516 or ecohen@russellinvestments.com.

Very truly yours,



Elliot S. Cohen
Associate General Counsel
Russell Investments

Attachments

On Russell Investments Letterhead

DATE

NAME
ADDRESS
ADDRESS

RE: NOTICE OF DATA BREACH

Dear NAME:

This notice concerns a recent data security incident that involved your information. While we do not believe your information has or is likely to be used inappropriately, we sincerely apologize for this incident and share the following details.

WHAT HAPPENED

On February 22, 2017, Russell Investments discovered that it experienced a data breach when a Russell Investments associate sent files containing personally identifiable information ("PII") to a personal Gmail account and downloaded those files to a personal computing device. This file transfer triggered a security monitoring alert indicating the breach of PII. Forensic analysis indicates the PII relates to certain Russell Investments' U.S.-based associates and certain of their dependents.

In the days following the data breach Russell Investments' Information Security and Incident Response team met daily; identified the breached PII and where it could see to have been stored or saved outside of Russell Investments' systems; recovered the breached PII from the associate who caused the data breach; deleted all known copies of the breached PII stored outside of Russell Investments' systems; and took other steps to remediate the situation including, but not limited to, resetting key passwords and other credentials to reduce the risks of potential misuse of the PII.

Since Russell Investments swiftly discovered the data breach, understood exactly what happened, where the breached PII resided, and obtained the full cooperation of the associate who caused the data breach in successfully remediating the breach, we did not need to involve any law enforcement agencies in this incident.

WHAT INFORMATION WAS INVOLVED

The PII is distributed among many different data files. Taken together, the PII consists of the first and last names of the affected individuals along with one or more of that individual's: social security number, date of birth, address, phone number, gender, health insurance group number, employment data (e.g., salary), and personal email address. While not every affected individual experienced the breach of each of these data elements, you are receiving this notice because your name, combined with whichever of these data elements that do apply to you consists of a breach

of your PII. Regardless of which type of your PII was breached and although we do not believe your information is likely to be used inappropriately, Russell Investments is offering you a comprehensive approach to reducing your risk of identity theft or other misuse of your PII.

WHAT ARE WE DOING

Immediately following the security monitoring alert indicating the breach of PII on February 22, 2017, Russell Investments' Information Security and Incident Response team investigated and mitigated the data breach. After discovery of this issue, the primary objectives were reducing the risk of misuse of the PII; removing the PII from non-Russell Investments managed devices and cloud accounts; ascertaining the exact PII involved and which people were affected by the breach of PII; and rotating the privileged credentials and keys. Russell Investments successfully achieved these objectives.

In an effort to avoid any similar data breach in the future, Russell Investments is considering: revisions to human resources' policies; revisions to IT polices related to privileged systems access by associates; implementing new data loss prevention functionality in our computer systems; blocking access to unapproved online storage services; and enhancements to our virtual private network used for remote access to associates' work environments.

While we believe that there is limited risk that your PII could be compromised and misused, at no cost to you we are providing you with tools to monitor, over the next two years, your credit and the credit of anyone else in your family that is affected by this data breach. You can activate this credit monitoring by going to www.myservices.equifax.com/silver and:

1. Welcome Page: Enter this ACTIVATION CODE 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.

WHAT YOU CAN DO

Remain vigilant, protect your personal information, and alert law enforcement and your state attorney general immediately if you suspect that anyone is misusing your PII or that you are a victim of identity theft. Here are proactive steps that you can take to protect your identity:

1) Obtain More Information to Protect Yourself

Visit any of the three U.S. Credit Bureau websites (see below) for general information regarding protecting your identity. The Federal Trade Commission provide information on-line at www.ftc.gov/idtheft and maintains an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261.

2) Place a 90-Day Fraud Alert on Your Credit file

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

3) Order Your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4) Manage Your Personal Information

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

5) Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

FOR MORE INFORMATION

If you have further questions, or would like help from a Russell Investments representative, please contact Russell Investments at 206-505-5656.

For more information on credit reporting, obtaining free credit reports or identity theft protection:

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013

Phone: (888) 397-3742
www.experian.com

Equifax
U.S. Consumer Services
Equifax Information Services, LLC.
Fraud Hotline: (877) 478-7625
www.equifax.com

TransUnion:
P.O. Box 6790
Fullerton, CA 92834
Fraud Hotline: (800) 680-7289
www.transunion.com

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
(877)-FTC-HELP (382-4357)
Website: www.ftc.gov

For California Residents: You can obtain information from, the California Office of the Attorney General about steps you can take to help prevent identity theft.

California Attorney General
1300 I St., Ste. 1740
Sacramento, CA 95814
(916) 445-9555
Website: https://oag.ca.gov/idtheft

For Massachusetts Residents: If you are the victim of identity theft, you have a right to file a police report and request a copy of it. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you to temporarily lift, or permanently remove a security freeze.

For North Carolina Residents: You can obtain information from, the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Attorney General's consumer Hotline toll-free within North Carolina at 877-5-NO-SCAM or 919-716-6000.

Sincerely,
Russell Investments

On Russell Investments Letterhead

DATE

NAME
ADDRESS
ADDRESS

RE: NOTICE OF DATA BREACH

Dear NAME:

This notice concerns a recent data security incident that involved your information. While we do not believe your information has or is likely to be used inappropriately, we sincerely apologize for this incident and share the following details.

WHAT HAPPENED

On February 22, 2017, Russell Investments discovered that it experienced a data breach when a Russell Investments associate sent files containing personally identifiable information ("PII") to a personal Gmail account and downloaded those files to a personal computing device. This file transfer triggered a security monitoring alert indicating the breach of PII. Forensic analysis indicates the PII relates to certain Russell Investments' U.S.-based associates and certain of their dependents.

In the days following the data breach Russell Investments' Information Security and Incident Response team met daily; identified the breached PII and where it could see to have been stored or saved outside of Russell Investments' systems; recovered the breached PII from the associate who caused the data breach; deleted all known copies of the breached PII stored outside of Russell Investments' systems; and took other steps to remediate the situation including, but not limited to, resetting key passwords and other credentials to reduce the risks of potential misuse of the PII.

Since Russell Investments swiftly discovered the data breach, understood exactly what happened, where the breached PII resided, and obtained the full cooperation of the associate who caused the data breach in successfully remediating the breach, we did not need to involve any law enforcement agencies in this incident.

WHAT INFORMATION WAS INVOLVED

The PII is distributed among many different data files. Taken together, the PII consists of the first and last names of the affected individuals along with one or more of that individual's: social security number, date of birth, address, phone number, gender, health insurance group number, employment data (e.g., salary), and personal email address. While not every affected individual experienced the breach of each of these data elements, you are receiving this notice because your name, combined with whichever of these data elements that do apply to you consists of a breach

of your PII. Regardless of which type of your PII was breached and although we do not believe your information is likely to be used inappropriately, Russell Investments is offering you a comprehensive approach to reducing your risk of identity theft or other misuse of your PII.

WHAT ARE WE DOING

Immediately following the security monitoring alert indicating the breach of PII on February 22, 2017, Russell Investments' Information Security and Incident Response team investigated and mitigated the data breach. After discovery of this issue, the primary objectives were reducing the risk of misuse of the PII; removing the PII from non-Russell Investments managed devices and cloud accounts; ascertaining the exact PII involved and which people were affected by the breach of PII; and rotating the privileged credentials and keys. Russell Investments successfully achieved these objectives.

In an effort to avoid any similar data breach in the future, Russell Investments is considering: revisions to human resources' policies; revisions to IT polices related to privileged systems access by associates; implementing new data loss prevention functionality in our computer systems; blocking access to unapproved online storage services; and enhancements to our virtual private network used for remote access to associates' work environments.

While we believe that there is limited risk that your PII could be compromised and misused, at no cost to you we are providing you with tools to monitor, over the next two years, your credit and the credit of anyone else in your family that is affected by this data breach. You can activate this credit monitoring by going to www.myservices.equifax.com/minor and:

1. Please login using the username and password you created when enrolling in your product
2. Select the button for "$29.95 for 12 months", you will not be charged any money and your credit monitoring will operate for 2 years.
3. Enter this ACTIVATION CODE in the box labeled "Promotion Code" to order the first minor product and click "apply code". This will zero out the price of the product. **Do not enter credit card information.**
4. Check the box to agree to the Terms of Use.
5. Next, click the "Submit Order" button.
6. You will then see the Order Confirmation. Please note that since you did not enter credit card information you **WILL NOT** be billed.
7. Click "View my Product" which will take you to your Member Center.
8. Click the orange button "Enroll Child" to enter your child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from monitoring the account. You may then re-enroll the minor with the correct SSN.
9. Check the box confirming you are the child's parent or guardian.
10. Click "Submit" to enroll your child.
11. If you are enrolling multiple minors, please log out, then repeat the above process to add another minor.

WHAT YOU CAN DO

Remain vigilant, protect your personal information, and alert law enforcement and your state attorney general immediately if you suspect that anyone is misusing your PII or that you are a victim of identity theft. Here are proactive steps that you can take to protect your identity:

1) Obtain More Information to Protect Yourself

Visit any of the three U.S. Credit Bureau websites (see below) for general information regarding protecting your identity. The Federal Trade Commission provide information on-line at www.ftc.gov/idtheft and maintains an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261.

2) Place a 90-Day Fraud Alert on Your Credit file

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

3) Order Your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4) Manage Your Personal Information

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

5) Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

FOR MORE INFORMATION

If you have further questions, or would like help from a Russell Investments representative, please contact Russell Investments at 206-505-5656.

For more information on credit reporting, obtaining free credit reports or identity theft protection:

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Phone: (888) 397-3742
www.experian.com

Equifax
U.S. Consumer Services
Equifax Information Services, LLC.
Fraud Hotline: (877) 478-7625
www.equifax.com

TransUnion:
P.O. Box 6790
Fullerton, CA 92834
Fraud Hotline: (800) 680-7289
www.transunion.com

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
(877)-FTC-HELP (382-4357)
Website: www.ftc.gov

For California Residents: You can obtain information from, the California Office of the Attorney General about steps you can take to help prevent identity theft.

California Attorney General
1300 I St., Ste. 1740
Sacramento, CA 95814
(916) 445-9555
Website: https://oag.ca.gov/idtheft

For Massachusetts Residents: If you are the victim of identity theft, you have a right to file a police report and request a copy of it. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you to temporarily lift, or permanently remove a security freeze.

For North Carolina Residents: You can obtain information from, the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Attorney General's consumer Hotline toll-free within North Carolina at 877-5-NO-SCAM or 919-716-6000.

Sincerely,
Russell Investments

On Russell Investments Letterhead

DATE

NAME
ADDRESS
ADDRESS

RE: NOTICE OF DATA BREACH

Dear NAME:

This notice concerns a recent data security incident that involved your information. While we do not believe your information has or is likely to be used inappropriately, we sincerely apologize for this incident and share the following details.

WHAT HAPPENED

On February 22, 2017, Russell Investments discovered that it experienced a data breach when a Russell Investments associate sent files containing personally identifiable information ("PII") to a personal Gmail account and downloaded those files to a personal computing device. This file transfer triggered a security monitoring alert indicating the breach of PII. Forensic analysis indicates the PII relates to certain Russell Investments' U.S.-based associates and certain of their dependents.

In the days following the data breach Russell Investments' Information Security and Incident Response team met daily; identified the breached PII and where it could see to have been stored or saved outside of Russell Investments' systems; recovered the breached PII from the associate who caused the data breach; deleted all known copies of the breached PII stored outside of Russell Investments' systems; and took other steps to remediate the situation including, but not limited to, resetting key passwords and other credentials to reduce the risks of potential misuse of the PII.

Since Russell Investments swiftly discovered the data breach, understood exactly what happened, where the breached PII resided, and obtained the full cooperation of the associate who caused the data breach in successfully remediating the breach, we did not need to involve any law enforcement agencies in this incident.

WHAT INFORMATION WAS INVOLVED

The PII is distributed among many different data files. Taken together, the PII consists of the first and last names of the affected individuals along with one or more of that individual's: social security number, date of birth, address, phone number, gender, health insurance group number, employment data (e.g., salary), and personal email address. While not every affected individual experienced the breach of each of these data elements, you are receiving this notice because your name, combined with whichever of these data elements that do apply to you consists of a breach

of your PII. Regardless of which type of your PII was breached and although we do not believe your information is likely to be used inappropriately, Russell Investments is offering you a comprehensive approach to reducing your risk of identity theft or other misuse of your PII.

WHAT ARE WE DOING

Immediately following the security monitoring alert indicating the breach of PII on February 22, 2017, Russell Investments' Information Security and Incident Response team investigated and mitigated the data breach. After discovery of this issue, the primary objectives were reducing the risk of misuse of the PII; removing the PII from non-Russell Investments managed devices and cloud accounts; ascertaining the exact PII involved and which people were affected by the breach of PII; and rotating the privileged credentials and keys. Russell Investments successfully achieved these objectives.

In an effort to avoid any similar data breach in the future, Russell Investments is considering: revisions to human resources' policies; revisions to IT polices related to privileged systems access by associates; implementing new data loss prevention functionality in our computer systems; blocking access to unapproved online storage services; and enhancements to our virtual private network used for remote access to associates' work environments.

While we believe that there is limited risk that your PII could be compromised and misused, at no cost to you we are providing you with tools to monitor, over the next two years, your credit and the credit of anyone else in your family that is affected by this data breach. You can activate this credit monitoring by:

- Go to www.premera.com in your internet browser and click the "Log in" button in the upper right hand corner of the Premera home page.
- If you have not already registered for an account with Premera:
    - Register for a new Premera account by clicking on "Create Account" and following the instructions.
    - After creating your account click "Login" and log into your Premera account and follow the instructions to finish setting up your account.
    - Login to your account.
    - Click "sign up today" under the box that says "Free Credit Monitoring" and follow the instructions.
- If you have an account with Premera:
    - Login to your account.
    - Click "sign up today" under the box that says "Free Credit Monitoring" and follow the instructions.

WHAT YOU CAN DO

Remain vigilant, protect your personal information, and alert law enforcement and your state attorney general immediately if you suspect that anyone is misusing your PII or that you are a victim of identity theft. Here are proactive steps that you can take to protect your identity:

1) Obtain More Information to Protect Yourself

Visit any of the three U.S. Credit Bureau websites (see below) for general information regarding protecting your identity. The Federal Trade Commission provide information on-line at www.ftc.gov/idtheft and maintains an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261.

2) Place a 90-Day Fraud Alert on Your Credit file

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

3) Order Your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4) Manage Your Personal Information

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

5) Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

FOR MORE INFORMATION

If you have further questions, or would like help from a Russell Investments representative, please contact Russell Investments at 206-505-5656.

For more information on credit reporting, obtaining free credit reports or identity theft protection:

Experian
Experian Security Assistance
P.O. Box 72

Allen, TX 75013
Phone: (888) 397-3742
www.experian.com

Equifax
U.S. Consumer Services
Equifax Information Services, LLC.
Fraud Hotline: (877) 478-7625
www.equifax.com

TransUnion:
P.O. Box 6790
Fullerton, CA 92834
Fraud Hotline: (800) 680-7289
www.transunion.com

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
(877)-FTC-HELP (382-4357)
Website: www.ftc.gov

For California Residents: You can obtain information from, the California Office of the Attorney General about steps you can take to help prevent identity theft.

California Attorney General
1300 I St., Ste. 1740
Sacramento, CA 95814
(916) 445-9555
Website: https://oag.ca.gov/idtheft

For Massachusetts Residents: If you are the victim of identity theft, you have a right to file a police report and request a copy of it. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you to temporarily lift, or permanently remove a security freeze.

For North Carolina Residents: You can obtain information from, the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Attorney General's consumer Hotline toll-free within North Carolina at 877-5-NO-SCAM or 919-716-6000.

Sincerely,
Russell Investments