Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

June 22, 2018

VIA EMAIL (attorneygeneral@doj.nh.gov)

New Hampshire Attorney General
33 Capitol St.
Concord, NH 03301

RE: Breach Incident Notification - Humana, Inc. [HU1800314]

Dear Attorney General:

The purpose of this letter is to notify your office of a recent incident that has occurred impacting a resident of your state.

What Happened?

On June 3, 2018 Humana was the target of a sophisticated cyber spoofing attack that occurred on Humana.com. A NH resident/Humana member's personal information on the website may have been accessed by the attackers.

On June 3, 2018 Humana became aware of a significant increase in the number of secure log in errors that were the result of numerous attempts to log into Humana.com from foreign countries. Humana Cyber Security Operations blocked the offending foreign Internet Protocol (IP) addresses from the website on June 4, 2018.

The volume of log in attempts to Humana.com on June 3, 2018 and June 4, 2018 suggested that a large and broad-based automated attack had been launched. This was evidenced by the volume of log in attempts coming from a foreign country. The nature of the attack and observed behaviors indicated the attacker had a large database of user identifiers (IDs) and corresponding passwords that were being inputted with the intention of identifying which might be valid on Humana.com. The excessive number of log in failures strongly suggests the ID and password combinations did not originate from Humana. Humana blocked the foreign addresses by June 4, 2018

Based on the facts, Humana has determined this to be an identity spoofing event. Identity spoofing refers to the action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal, such as use of stolen / spoofed authentication credentials to impersonate a user.

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

What Information Was Involved?

A NH resident/Humana member's Humana account may have been compromised during these attacks. We would like to stress that their Social Security Number was not disclosed as a result of this incident as it is not available for display in Humana web portals. The attackers may have gained access to their information on humana.com, which includes medical, dental and vision claims, spending account information.

Information potentially viewed/accessed on Humana.com could have included:

- Medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc.
- Spending account information such as health saving account spending and balance information, and

What We Are Doing?

Humana has implemented controls such as forcing a password reset, deploying new alerts of successful and failed logins and locked accounts as well as deploying a series of technical controls to enhance web portal security.

Humana has determined there is no evidence that any data was removed from Humana systems and Humana Cyber Security Operations continues to monitor the situation.

We encourage our members to review other websites where they have log in accounts and consider changing their password for those accounts. We also encourage them to vary their log in ID and password across all their web and mobile application accounts.

On June 21, 2018, a notification letter was sent to one (1) New Hampshire resident who were impacted by this situation. Attached you will find a copy of the letter that includes an offer for free credit monitoring and free identity theft protection.

We deeply regret this incident, but want to assure you that Humana has various safeguards to protect individual information including policies, procedures and technical safeguards. Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

If you have any questions about the information received in this letter or require additional information, please do not hesitate to reach out to me.

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

Sincerely,

Stacey Glennon
Senior Privacy & Ethics Professional
Humana Inc.
800-664-4140 x5801190
sglennon@humana.com

Enclosures

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

<Date>

<Member Name>
<Address>
<City, State Zip>

RE: HU1800314

NOTICE OF DATA BREACH

Equifax Activation Code:

Dear <Member Name>;

We are writing to notify you, a valued member, of a recent incident involving some of your personal information.

What Happened?

On June 3, 2018 Humana was the target of a sophisticated cyber spoofing attack that occurred on Humana.com. Your personal information on the website may have been accessed by the attackers.

On June 3, 2018 Humana became aware of a significant increase in the number of secure log in errors that were the result of numerous attempts to log into Humana.com from foreign countries. Humana Cyber Security Operations blocked the offending foreign Internet Protocol (IP) addresses from the website on June 4, 2018.

The volume of log in attempts to Humana.com on June 3, 2018 and June 4, 2018 suggested that a large and broad-based automated attack had been launched. This was evidenced by the volume of log in attempts coming from a foreign country. The nature of the attack and observed behaviors indicated the attacker had a large database of user identifiers (IDs) and corresponding passwords that were being inputted with the intention of identifying which might be valid on Humana.com. The excessive number of log in failures strongly suggests the ID and password combinations did not originate from Humana. Humana blocked the foreign addresses by June 4, 2018

Based on the facts, Humana has determined this to be an identity spoofing event. Identity spoofing refers to the action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal, such as use of stolen / spoofed authentication credentials to impersonate a user.

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

What Information Was Involved?

Your Humana account may have been compromised during these attacks. We would like to stress that your Social Security Number and bank account numbers were not disclosed as a result of this incident as it is not available for display in Humana web portals. The attackers may have gained access to your information on humana.com and/or go365.com, which includes medical, dental and vision claims, spending account information and biometric screening information.

Information potentially viewed/accessed on Humana.com could have included:

- Medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc.
- Spending account information such as health saving account spending and balance information, and

What We Are Doing?

Humana has implemented controls such as forcing a password reset, deploying new alerts of successful and failed logins and locked accounts as well as deploying a series of technical controls to enhance web portal security.

Humana has determined there is no evidence that any data was removed from Humana systems and Humana Cyber Security Operations continues to monitor the situation.

We encourage you to review other websites where you have log in accounts and consider changing your password for those accounts. We also encourage you to vary your log in ID and password across all your web and mobile application accounts.

We know that you may be worried about what took place.

At our expense, to safeguard your information from potential misuse, we have partnered with Equifax® to provide its Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, $1 million Identity Fraud Expense Coverage and access to your credit report. We strongly encourage you to enroll for this free service to protect yourself from the potential misuse of your information.

What You Can Do

We want you to know that at Humana we take seriously our responsibility to ensure the security of your information. We regret any concern this incident may have caused. You have privacy rights under a Federal law that protects your health information. It is important for you to know you can exercise these rights, ask questions about them, and file a complaint if you think Humana has not taken adequate steps to protect your health information.

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

Humana respects your right to file a complaint with us or with the Department of Health and Human Services through the Office of Civil Rights at:

Office for Civil Rights Region IV
U.S. Department of Health and Human Services
Atlanta Federal Center, Suite 3B70
61 Forsyth Street, S.W.
Atlanta, GA 30303-8909

You have the right to obtain any police report filed in regard to 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.

In addition, the Federal Trade Commission suggests the following steps if you believe your identity has been stolen.

1. **Place a fraud alert on your credit reports and review your credit reports**. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two companies.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241 Atlanta, GA 30374-0241 **1-800-525-6285** www.equifax.com	P.O. Box 9532 Allen, TX 75013 **1-888-EXPERIAN or 1-888-397-3742** www.experian.com	Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19016 **1-800-680-7289** www.transunion.com

Once you place the fraud alert, you are entitled to order free copies of your credit reports. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Services, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georiga, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

2. **Carefully review your credit reports**. Look for inquiries from companies that you haven't contacted, accounts that you did not open, and debts on your accounts that you can't explain. Be aware that some companies may bill under names other than their store names.

3. **Close any accounts that you know, or believe, have been tampered with or opened fraudulently.**

4. **File your concern with the Federal Trade Commission.** This important information helps law enforcement agencies track down identity thieves. You can contact the Federal Trade Commission at 1-877-ID-THEFT, (1-877-438-4338) or by visiting the Federal Trade Commission website at www.ftc.gov/idtheft or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year.

For residents of Maryland: You may also obtain information about identity theft prevention from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about identity theft prevention from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may also obtain information about identity theft prevention from the North Carolina Rhode Island Attorney General's Office:

Office of the Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400, consumers@riag.ri.gov

We are asking that you remain vigilant. Check for any medical bills that you do not recognize on your credit reports. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. If you are a **California resident**, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

Fraud Alerts: You can place an initial alert or an extended alert on your credit report to put your creditors on notice that you may be a victim of fraud:. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed above.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. You may also incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law also allows consumers to place a security freeze on their credit reports. 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.
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 up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

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	**Experian Security Freeze**	**Trans Union Security Freeze**
P.O. Box 105788 Atlanta, GA 30348	P.O. Box 9554 Allen, TX 75013	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

In order 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;

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

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 either 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.

To remove the security freeze, you must send a written request to each of the three credit bureaus 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. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Reporting of identity theft and obtaining a police report:

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, the Oregon Attorney General.

For More Information

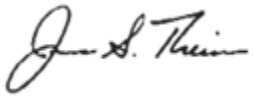
If you have any questions or need any help with anything mentioned in this letter, please contact us at **1-866-4ASSIST** (1-866-427-7478). If you have a speech or hearing impairment and use a TTY, call **1-800-833-3301**. In addition, please notify our Privacy Office Office at privacyoffice@humana.com if you believe your information is being used (e.g. identity theft) by another party so that we can work with you and law enforcement officials to promptly investigate the matter.

Again, please accept our sincere apology for this incident. We value your membership and work hard to protect your information.

Sincerely,

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com



Jim Theiss
Chief Privacy Officer
Humana, Inc.

Enclosures

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

Discrimination is against the law

Humana Inc. and its subsidiaries comply with applicable federal civil rights laws and do not discriminate on the basis of race, color, national origin, age, disability, or sex. Humana Inc. and its subsidiaries do not exclude people or treat them differently because of race, color, national origin, age, disability, or sex.

Humana Inc. and its subsidiaries provide: (1)free auxiliary aids and services, such as qualified sign language interpreters, video remote interpretation, and written information in other formats to people with disabilities when such auxiliary aids and services are necessary to ensure an equal opportunity to participate; and, (2) free language services to people whose primary language is not English when those services are necessary to provide meaningful access, such as translated documents or oral interpretation.

If you need these services, call **1-877-320-1235** or if you use a **TTY**, call **711**.

If you believe that Humana Inc. and its subsidiaries have failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with Discrimination Grievances, P.O. Box 14618, Lexington, KY 40512-4618.

If you need help filing a grievance, call **1-877-320-1235** or if you use a **TTY**, call **711**.

You can also file a civil rights complaint with the **U.S. Department of Health and Human Services**, Office for Civil Rights electronically through the Office for Civil Rights Complaint Portal, available at **https://ocrportal.hhs.gov/ocr/portal/lobby.jsf**, or by mail or phone at **U.S. Department of Health and Human Services**, 200 Independence Avenue, SW, Room 509F, HHH Building, Washington, DC 20201, **1-800-368-1019**, **800-537-7697 (TDD)**.

Complaint forms are available at **https://www.hhs.gov/ocr/office/file/index.html**

Multi-Language Interpreter Services

ATTENTION: If you do not speak English, language assistance services, free of charge, are available to you. Call **1-877-320-1235 (TTY: 711)**.... ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al **1-877-320-1235 (TTY: 711)**.... 注意 : 如果您使用繁體中文 , 您可以免費獲得語言 援助服務。請致電 **1-877-320-1235 (TTY: 711)** 。... CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số **1-877-320-1235 (TTY: 711)**.... 주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. **1-877-320-1235 (TTY: 711)**번으로 전화해 주십시오.... PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa **1-877-320-1235 (TTY: 711)**.... Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните **1-877-320-1235 (телетайп: 711)**.... ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele **1-877-320-1235 (TTY: 711)**.... ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le **1-877-320-1235 (ATS: 711)**.... UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer **1-877-320-1235 (TTY: 711)**.... ATENÇÃO: Se fala português, encontram- se disponíveis serviços linguísticos, grátis. Ligue para **1-877-320-1235 (TTY: 711)**.... ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero **1-877-320-1235 (TTY: 711)**... ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: **1-877-320-1235 (TTY: 711)**.... 注意事項 : 日本語を話される場合、無料の言語支援をご利用いただけます。**1-877-320-1235 (TTY: 711)**まで、お電話にてご連絡ください。... فارسی گفتگو می کنید، تسهیالت زبانی بصورت رایگان برای شما فراهم می باشد. با تماس بگیرید. تووجه: اگر به زبان **(TTY: 711)1-877-320-1235**. D77baaak0n7n7zin:D77saadbeey1n7[ti'goDinéBizaad,saadbee1k1'1n7da'1wo'd66', t'11jiik'eh, 47 n1 h0l=, koj8' h0d77lnih **1-877-320-1235 (TTY: 711)**....**1-877-320-1235** اتصل برقم الللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. **711)رقم هاتف الصم والبكم:** ملحوظة: إذا كنت تتحدث اذكر

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com

EQUIFAX®

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:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian**, and **TransUnion** credit reports
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to $1 million in identity theft insurance [1] with $0 deductible, at no additional cost to you
- 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.
- 90 day Fraud Alert [2] 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

Humana

Privacy Office
101 E. Main Street
Louisville, KY 40202
Humana.com