

June 2, 2006

The Hon. Jim Poolman
Commissioner of Insurance
600 East Blvd.
Bismarck, ND 58505

HUMANA
when you need it most

Dear Commissioner Poolman:

Michael B. McCallister asked that I respond promptly to your May 31, 2006 letter regarding personal information that may have been compromised as the result of a theft from an automobile.

First, let me state that we understand the gravity of this situation and sincerely apologize for the error on our part of not notifying your Department. We are working to prevent errors such as this in the future, and we will keep you promptly apprised of such events and related follow up activities.

Forty-four North Dakota residents were identified by GoldenCare USA, Inc., the general agency contracted with Humana to sell insurance policies. On May 5, 2006, GoldenCare USA, Inc. notified Humana that an employee's car had been broken into and copies of Humana Medicare applications were included in the computer briefcase that was stolen. This briefcase also included a laptop which did not have access to Humana systems nor did it contain any Humana applicant or policyholder information. The employee filed a police report on said theft (Attachment #1) with the Brooklyn Park Police Department on May 5, 2006.

Humana's Privacy Office was notified on the next business day, Monday May 8, 2006 of the above incident, and we immediately began our investigation. Humana requested a complete list of the affected Humana beneficiaries. It took the agency some time to recreate an accurate list of the applications involved in the incident. We began to contact them by telephone beginning on May 17, 2006 to advise them of the incident and inform them that we would be sending them a letter and offering free credit monitoring to any affected beneficiary who so desired. A mailed notice was completed by May 19, 2006 and included a toll-free number to call to have any questions answered (Attachment #2).

At the same time we were notifying the beneficiaries, we addressed corrective actions with GoldenCare USA, Inc. Humana confirmed that GoldenCare USA, Inc., which has a business associate agreement with Humana, has a privacy policy in place to address such issues and that all GoldenCare USA, Inc. employees based in Plymouth, Minnesota received privacy training. The employee involved in the incident received disciplinary counseling on the appropriate safeguarding and storage of personal information of all clients. Further, reminder educational sessions were held on May 8, 2006 with all GoldenCare USA, Inc. agency employees. We will be sending a reminder to all of our contracted agency and staff on the handling of applicant information as a result of this incident.

Humana has also reviewed all our current internal policies regarding the safeguarding of personal information of all Humana members and applicants. Our privacy policy is attached (Attachment #3). We are also investigating any additional contractual or training requirements we may want to put into place with our vendors and agents. We will provide you with an update as soon as that work is completed.

Humana's privacy policies and procedures comport with both Gramm-Leach-Bliley privacy and security requirements and HIPAA privacy and security requirements. Our investigation and remediation were conducted pursuant to such implementation. GoldenCare USA, Inc. is an authorized non-affiliated party to whom we can make disclosures.

Included below are our responses to your questions:

1. Specifically, how many North Dakota consumers have had their personal/private information compromised? Please provide the names to this Department, so we may communicate with them independently.

Forty-four (44) North Dakota residents were affected. Please see Attachment #4 for a password-protected file. We will communicate the password in another communication.

2. How many consumers outside of North Dakota have had their personal/private information breached?

Two hundred twenty-four (224) residents of three other states (Minnesota, Iowa and Nebraska) were affected, and we are communicating to officials in those states.

3. What is the security policy of Humana in storing this information?

Our privacy policy is included in Attachment #3. We do have a Business Associate Agreement with GoldenCare USA, Inc. which states our requirements to safeguard the Protected Health Information they create, store and transfer as they perform functions on our behalf. We have conducted an investigation of the situation and requested and received a corrective action plan from GoldenCare USA, Inc. that included consultation with the individual who removed the documents from the office as well as supplementary training for all employees in the office.

4. What is Humana's policy in accepting applications for policies and transferring that information?

Please refer to Humana's Privacy Policy, Attachment #3. In addition, Golden Care USA, Inc. has its own policies concerning the handling of Protected Health

Information. Humana is also in the process of developing more specific guidance for our employees and business associates regarding the transportation and storage of member personal information.

5. What are the details of the theft?

Please see details on pages 1-2 of this letter and the attached police report. We will contact this law enforcement agency if we obtain any reports of this information being used inappropriately to aid in their investigation and protect the affected individuals.

6. What assurances can you give to policyholders that there is a thorough investigation taking place to retrieve the information lost?

The investigation into the stolen information is currently being conducted by the Brooklyn Park Minnesota Police Department. We are requesting that we be informed as soon as any of the stolen documents are recovered. At that time we will notify our members and your office of any recovery.

7. What other procedures does Humana employ to protect affected policyholders?

In an incident such as this where a policyholder's personal information has been stolen, the immediate concern is to assist the individual in protecting him or herself from identity theft. That is the reason we offer a comprehensive credit monitoring service. The service we offer to affected policyholders (free of charge) includes:

- Comprehensive credit file monitoring including daily notification of key changes to Equifax, Experian and TransUnion credit files
- Online enrollees have access to a 3 in 1 credit report and unlimited copies of their Equifax credit report
- \$20,000 Identity Fraud Expense Coverage with a \$0 deductible
- Access to Equifax Premium Customer Care 24 hours a day, 7 days a week.

Finally, my office is available to answer questions and provide guidance in this area as needed.

8. How will you respond to currently unaffected Humana policyholders who now might be concerned with the security of their information?

We are preparing scripts as well as frequently answered question documents for our customer service representatives to respond to basic questions that policyholders may have. If questions from the policyholder are more detailed the

customer service personnel will consult Humana's Privacy Office regarding the response.

9. Who, specifically, can consumers contact by toll-free number to discuss their concerns?

Consumers affected by the incident can utilize the toll free number we provided in our letter. Questions requiring follow up and or any privacy related complaints are referred to our Privacy Office.

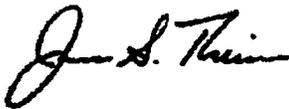
10. Provide to me weekly reports of any contacts with North Dakota policyholders regarding this issue.

We will do this.

Again, we understand the gravity of this situation. We have already taken significant steps to alert consumers, are dealing with the agency and are evaluating processes and training improvements. Humana is ready to respond to any additional questions. We will be in contact with your office shortly to follow-up on this letter.

Thank you.

Sincerely,



Chief Privacy Officer
Humana Inc.
502-580-4322
jtheiss@humana.com

Attachments

-----MAY 30 '06 01:55PM INSURANCE OFFICE----- P.2/4
 Date: 5/23/06 BROOKLYN PARK POLICE DEPARTMENT Page:
 Time: 17:40:12 Offense Report Program: CM53012

 Case Number : 1-06-022180 Class Code : THEFT FROM AUTO
 Seat Assignment: 51P230 ATHLETIC COMPLEX
 District : 51NW
 Street Number : [REDACTED]
 City : [REDACTED], MN 55445
 How Received : Radio Primary Officer: CUDD, C.
 Date Reported : 5/05/06 17:15 Incd Occur From: 5/04/06 22:45
 Incd Occur To : 5/05/06 7:15 Incident : THEFT FROM AUTO
 Location Type : SINGLE FAMILY RESIDENCE
 Bias Motivation: No Attachments : NO
 Case Status : Inactive Case Status Dt : 5/15/06
 Transcribed By : LBITSCHUH, D. 5/12/06 Rpt. Coded By : RIVARD, J. 5/12/06

***** ADDITIONAL TIMES *****
 Time Dispatched: 17:15 Time Arrived : 17:15
 Time Cleared : 17:35

***** CASE MANAGEMENT INFORMATION *****
 Dept Class : THEFT FROM AUTO Case Status : Inactive
 Case Status Dt : 5/15/06 Investigator : INCIDENT REVIEW,,

ASSIGNMENT HISTORY
 Dept Unit : Investigations Investigator : INCIDENT REVIEW,
 Assignment Date: 5/15/06 Reviewed by : NELSON, E.

***** OFFENSE REPORT # 1 *****
 Federal Class : Larceny - From Motor Vehicle(not 21
 GOC : Not Applicable
 Statute/Ordin : 609-52-2 IC15S
 UCR Disposition: Open/Pending
 Statute Desc : THEFT-501-2500-FE-MOTOR VEH-OTH PRO

***** COMPLAINANT INFORMATION - #.1 *****
 Prompt valid in: [REDACTED] Birth Date : 1/13/1941 65
 Adult / Juvenil: ADULT
 Street Number : [REDACTED]
 City : BROOKLYN PARK, MN 55445
 Home Phone No. : [REDACTED] Business Phone : [REDACTED]
 Other Phone Nbr: 763/000-0000 Sex : Female
 Race : Unknown Dangerous Pers?: No

***** NARRATIVE # 2 *****
 Summary Reported By: CUDD, C. 5/05/06

Theft from auto. Laptop computer and other items stolen from
 unlocked vehicle. No suspect info.

***** NARRATIVE # 3 *****
 Original Report Reported By: CUDD, C. 5/05/06

REPORT NARRATIVE:

On 5/5/06 at 1715 hours, I, Officer Cudd was dispatched to a phone
 call report regarding a theft from auto.

Date: MAY 30 2006 01:55AM INSURANCE OFFICE----- P.3/4
Time: 17:40:12 BROOKLYN PARK POLICE DEPARTMENT Page: 2
Offense Report Program: CMS301L

1-06-022180 (Continued)

I contacted the complainant, verbally identified as [REDACTED],
Date of Birth: 01/13/41. She stated that:

- She had parked her vehicle outside her house on 5/4/06 at 1045 p.m.
- She had left the vehicle unlocked.
- When she came back out to the vehicle at 715 a.m. this morning, she realized that her black nylon briefcase was missing.
- The briefcase contained a laptop computer, as well as several papers from National Independent Brokers, the company she works for, that are rather important to the company.
- She did not see who had done it, nor did she have any idea who might have done it.
- The computer was a Dell 2500 computer, with a service number of (see stolen property narrative).
- The computer had an express service code of (see stolen property narrative).
- She did not have the serial number for the computer.
- The silver Dell emblem is missing from the top of the computer.
- On the rear of the computer, there is a door, which has tape over it.
- The computer is about 4 years old, and it was bought for \$1400.00.
- The case was a black nylon laptop carrying case with a handle, valued at about \$50.00.
- As the vehicle was unlocked, there was no forced entry into the vehicle.

I provided [REDACTED] with the case number for the report. I also advised her to try and obtain the serial number for the computer and provided her with my voicemail number so that she could contact me if she found it. I advised her to call if she had any further information. No further action taken by this officer.

DISPOSITION:

Theft from auto. Laptop computer and other items taken from unlocked vehicle. No suspect information. No further action taken by this officer.

Dictated by: Officer C. Cudd, Badge #182, Squad #1518

HUMANA

Fax:5025802249

Jun 2 2006 15:09

P.03

HUMANA

Fax:5025802249

Jun 1 2006 8:27

P.06

----- MAY 30 '06 01:55PM INSURANCE OFFICE P.4/4 -----
 Date: 5/23/06 BROOKLYN PARK POLICE DEPARTMENT Page: 3
 Time: 17:40:12 Offense Report Program: CMS301L

1-06-022180 (Continued)

***** N A R R A T I V E # 4 *****
 STOLEN PROPERTY Reported By: CUDD, C. 5/05/06

STOLEN PROPERTY

CASE NUMBER: 06-22180

- Dell 2600 laptop computer. Black in color. Dell emblem missing off of top of the computer. Door to the rear of computer has tape over it. Service code CPSHP11. Express service code 270-376-043-41. Purchased four years ago for approximately \$1400.00.

- A black nylon laptop carrying case with handle. Valued at around \$50.00.

- Paperwork from the complainant's place of employment, National Independent Brokers, which bare importance for the company.

Dictated by: Officer C. Cudd, Badge #182

***** END OF REPORT *****

[Date]

[Humana logo]

[Name]

[Address]

[Address]

[City, State ZIP]

Dear [Member Name]:

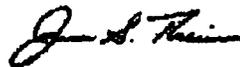
Since you are a valued Humana member, we need to tell you about a recent situation. We were recently notified that a copy of your Humana Medicare enrollment application was stolen. Unfortunately, this application contains your personal information including such items as your name, address, Social Security #, and bank routing information, if indicated on the application.

We regret this unfortunate situation and want to assure you that Humana takes all privacy incidents seriously. While Humana has policies and procedures in place to maintain the security of each member's personal information, at this time we are taking additional steps to assist in protection of your information.

We do not expect this issue to create future problems for you. However, we have set up a free credit monitoring service with Equifax for your use for one year. If you would like to put this protection in place, please follow the instructions enclosed. You can sign up for this service online, or you can simply complete and mail or fax the enclosed enrollment form.

Again, we regret this possible exposure of personal information. Your continued satisfaction and confidence in the protection of your information is of great importance to us. If you have any questions or need further assistance, please send an e-mail to PrivacyOffice@Humana.com or contact Customer Service at 1-800-281-6918. If you have a speech or hearing impairment and use a TDD, call 1-800-833-3301.

Sincerely,



James S. Theiss
Chief Privacy Official

For your added protection ...

Humana has arranged free credit monitoring services with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you. The steps to follow:

1. Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection service.
2. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two credit reporting agencies

Equifax Credit Watch™ Gold with 3-in-1 Monitoring

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 credit reporting agencies. The key features and benefits are listed below.

Equifax Credit Watch Gold with 3-in-1 Monitoring provides you with a one-year membership service:

- Comprehensive credit files monitoring, with daily notification of key changes to your Equifax, Experian and Trans Union credit files.
- Automatic notification of key changes to your credit files from any of the three agencies.
- If you enroll online, you have access to one 3-in-1 Credit Report and unlimited copies of your Equifax Credit Report™. If you enroll by U.S. mail, you receive quarterly updates to your Equifax Credit Report.
- Up to \$20,000 Identity Fraud Expense Coverage with \$0 deductible at no additional cost to you. Certain limitations and exclusions apply.†
- Premium Customer Care 24 hours a day, 7 days a week, to assist you in understanding the content of your credit information.

How to Enroll

Use the enclosed enrollment form, or go to www.myservices.equifax.com/monitor_order to enroll online.

In the Promotion Code box, insert this code:

If you choose to enroll online, just follow these steps:

- **Step 1 – Registration:** Complete the form with your contact information (name, address, telephone #, Social Security Number, date of birth, e-mail address). The information is provided in a secured environment.

- **Step 2 - Verify Your Identity:** Equifax will verify your identity by asking you up to two security questions
- **Step 3 - Order Summary:** During the "check out" process, insert your Promotion Code, exactly as noted above, in the box labeled "Enter Promotion Code." This code eliminates the need to provide a credit card number for payment.
- **Step 4 - Go to the Member Center:** Under "Product List," select Credit Watch Gold with 3-in-1 Monitoring to access the product features.

Fraud Alert

A fraud alert is a consumer statement added to your credit file that lasts 90 days. Once the fraud alert statement is added to your credit file, it alerts creditors of possible fraudulent activity and requests that they contact you before establishing a credit account in your name. To place a fraud alert on your Equifax credit file, you may contact Equifax's 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.

ENROLLMENT DEADLINE IS
(specify date)

† Insurance underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Nothing stated herein affects the terms, conditions and coverages of any insurance policy issued by St. Paul Travelers, nor does it imply that coverage does or does not exist for any particular claim or type of claim under any such policy.



enlighten | enable | empower

ATTACHMENT

EQUIFAX CREDIT WATCH™ with 3-in-1 MONITORING
ENROLLMENT INSTRUCTIONS

Use this form only if you are enrolling by mail or fax

Complete the information shown below and mail or fax this form to receive your Equifax Credit Watch™ with 3-in-1 Monitoring via U.S. mail.

- YES, I would like my complimentary Equifax Credit Watch™ with 3-in-1 Monitoring subscription delivered via U.S. mail.

Name (First, Middle Initial, Last)

Address (House #, Street Name)

City State ZIP Code

Date of Birth (MM/DD/YYYY) Gender (M/F) Daytime Phone Number

□□□ — □□ — □□□□ HMA-_____
Social Security Number (required to obtain a credit file) Promotional Code (MUST FILL IN NUMBERS)

Fair Credit Reporting Act

I authorize Equifax Consumer Services, Inc. ("Equifax") to obtain my credit report and monitor my credit file at one or more consumer reporting agencies, as necessary for me to receive Equifax Credit Watch™ (the "Service"). I understand that Equifax cannot accept authorization from any person other than the individual joining the service and confirm that I am at least 18 years of age and I am requesting my own personal information. I understand that there will be additional terms and conditions included in the Service materials that I will receive, including without limitation additional provisions regarding cancellation rights, and limitations on Equifax's liability, and I will be bound by those terms and conditions unless I immediately cancel the Service upon receipt of the complete terms and conditions.

Signature (Required) Date E-Mail Address (Optional)

HUMANA

Fax:5025802249

Jun 2 2006 15:13

P.05

HUMANA

Fax:5025802249

Jun 1 2006 8:28

P.13

EQUIFAX

enlighten | enable | empower

Please return this form by either:

FAX: 1-800-437-4675 (toll-free)

OR

MAIL: Equifax Consumer Services

P.O. Box 105496

Atlanta, GA 30348

June 12, 2006

The Honorable Jim Poolman
Commissioner
North Dakota Department of Insurance
600 East Boulevard
Bismarck, ND 58505



Dear Commissioner Poolman:

Thank you for your letter dated June 6, 2006 responding to the communication we sent to your office regarding the theft of paper copies of Medicare applications. We understand your frustration and are working hard to remedy this situation as completely and as quickly as we can.

As a result of this incident, Humana has re-examined our internal employee policies and procedures relating to protecting the personal information of our members and the same policies and procedures as they relate to contracted insurance agencies with which we hold Business Associate Agreements. While this review is not accomplished quickly, we want you to know we have taken immediate steps to put all our contracted insurance agencies on notice that safeguarding member information is a priority and they should treat this information with care and protect it accordingly (please see response to Question #6 below).

Below please find our responses to your information requests.

- 1. An explanation of why the subsequently stolen applications were allowed to be removed from GoldenCare USA's office.**
 - A. The stolen applications were taken home by an administrative assistant of GoldenCare USA to remain current in her workload. The employee received disciplinary counseling on the appropriate safeguarding and storage of personal information of all clients. In addition, GoldenCare USA updated their privacy rule memorandum to specifically address this issue by prohibiting the removal of this information from their offices (please see response to Question #3 for further detail).

- 2. Specific information regarding GoldenCare USA's privacy training for employees prior to the breach, including: Training materials; records of training meetings; attendance records at these meetings; and any other specifics relating to the training.**
 - A. GoldenCare USA's HIPAA Privacy Training took place on February 28, 2003. Subsequent training sessions are handled by the management team of each

department and when new employees are hired. We have included in Attachment #1, training materials from GoldenCare USA as you requested.

- 3. A copy of training materials distributed at the May 8, 2006 educational session for all GoldenCare USA employees.**
 - A. Attachment #2 is a copy of the document that was updated on May 8, 2006 by GoldenCare USA to further clarify that all customer and agent information must remain on their premises. **This memorandum was distributed to and signed by all employees of GoldenCare USA. (waiting for confirmation)**

- 4. A copy of GoldenCare USA's corrective action plan referred to in response to number (3) of your letter of July 2, 2006.**
 - A. Attachment #3 contains a copy of the GoldenCare USA's corrective action plan. GoldenCare USA provided a draft copy of their corrective action plan which was viewed as insufficient by Humana. We forwarded to GoldenCare USA a proposed corrective action plan which is page three of Attachment #3. Humana is awaiting response from GoldenCare USA at this time. Humana will review the revised corrective action plan as well as our ongoing relationship with GoldenCare USA. All options remain open. We will forward a final copy of the disposition of the corrective action plan and our relationship as soon as it has been finalized.

- 5. A more specific description of the 'disciplinary counseling' provided for the GoldenCare USA employee involved in the incident.**
 - A. The disciplinary actions taken by GoldenCare USA with the associate are described in Attachment #4.

- 6. A copy of the reminders sent to all contracted agencies regarding the handling of applicant information as a result of this incident.**
 - A. The reminder that was issued on June 2, 2006 to all contracted agencies regarding the handling of personal information. The communication was sent from Humana's National Director of Delegated Sales. The text of the communication is below:
 - "Dear Valued Partner:
Humana has recently been made aware of several breaches of protected health information (PHI) of Medicare beneficiaries. Given the current climate, it would be wise to review your own internal safeguards as it relates to the PHI of not only Humana members, but any individual you may possess information on. You may wish to review Exhibit A in the GPA contract, "HIPAA Business Associate Requirements" that outlines

what your obligations are to protect Humana member information as a Business associate of ours.

Humana is reviewing its current policies and privacy practices for both internal and external partners. Assuring proper handling of enrollment applications and the physical safeguards for any data storage and protection of the same information is of critical importance and will be closely monitored. As a valued partner of Humana, we intend to work closely with you to ensure those protections are in place for the sake of everyone involved.

In the near future, we will provide additional guidance and procedures that will continue to assure we maintain and protect this data.

Thank you in advance for your cooperation.”

7. An update regarding additional contractual or training requirements Humana Inc. put into place with its vendors and agents.

- A. A detailed audit plan to audit all delegated agents regarding compliance with our Group Producing Agent Contract is being developed with a projected implementation date of June 26, 2006. Materials are under development and are not available at this time. We will be in contact with your office when the final documents are completed.

8. An explanation of how Humana Inc. can be confident that there were no more than 44 North Dakota policyholders affected.

- A. GoldenCare USA was able to identify the copies of the paper applications by having a GoldenCare USA associate with direct knowledge of the workflow process between GoldenCare USA and Humana. This associate was able to determine which applications had been received by their office with the assistance of daily application receipt information provided by the local Humana office. The GoldenCare USA associate was then able to eliminate applications sold by other agents. GoldenCare USA is confident that they accurately identified the copies of applications.

9. The names and addresses of any North Dakota policyholders involved in a privacy breach in which the personal information of approximately 17,000 Humana policyholders was found on a computer available to the public in a Baltimore, Maryland hotel.

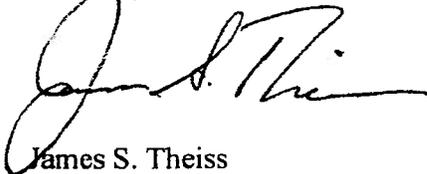
- A. Attachment #5 is a password-protected spreadsheet of the names and addresses of 82 North Dakota members who were impacted by the recent situation of member information being left in a temporary file of the hotel business service computer in Baltimore. We are attaching the two letters used to notify these individuals. Attachment #6 is the letter that was sent to actively enrolled Humana members

and Attachment #7 is the letter that was sent to formerly enrolled Humana members. This notification was sent to 17,657 individuals.

The protection of our members' personal information is a priority for Humana. Therefore, we are reviewing the length of time these affected members will have access, free of charge, to a credit monitoring service. We will also be re-contacting affected members who have not elected coverage to encourage them to take advantage of this service. In addition, we are revising our initial letter to more clearly encourage affected members to take advantage of this service.

We truly understand the gravity of this situation and are working hard to remedy this very unfortunate incident. We appreciate and welcome your continued involvement and look forward to working with you to resolve this situation.

Sincerely,



James S. Theiss

June 13, 2006

The Honorable Jim Poolman
Commissioner
North Dakota Department of Insurance
600 East Boulevard
Bismarck, ND 58505

HUMANA
... When you need it most

RE: Response to June 7, 2006 Letter

Dear Commissioner Poolman:

This letter is in response to your communication on June 7, 2006 regarding the discovery of a file containing personal member information located on a public access hotel computer. As we noted in our June 9, 2006 notice letter to your office, the document in question was a temporary file that was not deleted due to a technical software error in Humana's Web mail system. We regret that this information did not reach your office before our letter to affected members began to arrive.

Since we have exchanged a number of communications in the last week regarding the Minnesota and Maryland incidents, I have included references to information contained in prior responses in parentheses following the answer to the question. I hope this format makes it easy for you and your staff to locate the information.

Below please find our responses to your information requests.

- 1. Why has Humana, Inc. , yet again, failed to notify the North Dakota Insurance Department of this second serious violation?**
 - A. We again apologize for the delay in our communication regarding the Maryland incident. On June 9, 2006, we sent your office a letter by e-mail (Attachment #1) that provided background on this incident, steps we had taken to notify member, and our efforts to address the security issue. That correspondence included a copy of our communication to affected members. (Humana's June 12, 2006 response to your office includes both versions of the affected member letter in our response to question 9 as Attachments 6 & 7.)

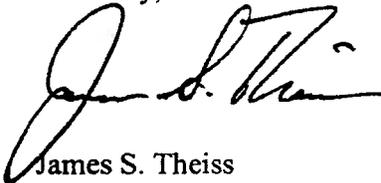
- 2. How many total consumers from North Dakota and outside North Dakota have had their personal/private information exposed in this latest incident?**
 - A. Eighty-two North Dakota members were impacted by the Maryland incident. We notified a total of 17,657 individuals, including the 82 North Dakota members, affected by the Maryland incident. (Humana's June 12, 2006 letter includes the same information in a response to question 9.)

- 3. Provide me names and addresses of all North Dakota consumers whose personal/private information has been compromised, so we may communicate with these policyholders independently.**
 - A. This list was provided with our June 12, 2006 letter to your office as password protected electronic file labeled Attachment #5.

- 4. Provide me weekly reports on any contacts with these North Dakota policyholders regarding this incident, as well as with the 44 North Dakota consumers affected by the prior breach.**
 - A. Humana will keep your office updated on our policyholder contacts for both the Minnesota and Maryland incidents (Humana's May 31, 2006 letter includes the same response in the answer to question #10.) For the week ending June 9th, we have received 4 inbound calls from North Dakota members affected by both incidents. All of these calls sought more information about the incident or about the free credit monitoring service being offered.

We truly understand the gravity of this situation and continue to work hard to remedy these very unfortunate incidents. We would welcome the opportunity to meet with you to discuss our responses to the specific questions or review the steps we have taken to address these security issues.

Sincerely,



James S. Theiss
Chief Privacy Officer
Humana, Inc.