



AMERICAS

*Lael E. Bellamy,
Chief Counsel and Chief Privacy Officer
(770) 980-6532
lael.bellamy@us.ing.com*

July 1, 2010

Via Facsimile

410.576.6566

Attorney General Douglas F. Gansler
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Attn: Security Breach Notification

Dear Attorney General Gansler:

Pursuant to MD Code Com. Law, § 14-3501 et seq., we are writing to notify you of an unauthorized access of personal information involving 473 Maryland residents. We do not believe this incident requires notification under Maryland law, however we are notifying as a courtesy and in the interest of full disclosure.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS.

ReliaStar Life Insurance Company (RLIC) is responsible for premium administration for RLIC insurance products purchased by employees of our clients. An encrypted electronic file containing the personal information of one client's employees, including several Maryland resident, was inadvertently made available to another company's Human Resources (HR) department due to an isolated administrative error. The encrypted file included the individual's name and social security number. Our password-based registration encryption system prohibits the wrong addressee from opening an encrypted e-mail. Because the e-mail was addressed to the wrong client, that wrong client was able to open the e-mail.

NUMBER OF MARYLAND RESIDENTS AFFECTED.

Of the individuals affected, 473 were residents of the State of Maryland. The Maryland residents will shortly receive the attached notice through the mail.

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT.

The encrypted file was sent to the incorrect employer. The employer receiving and reading the incorrect file contacted us on June 3, 2010, notifying us the file was not theirs. ING Employee Benefits, a division of ReliaStar Life Insurance Company, worked with the HR and IT Departments of the parties involved to ensure that all data that was inadvertently made available was fully deleted from their systems. The information was not reported to law enforcement, and there is no evidence that the personal information has been or will be used for fraudulent purposes, as the individuals who received personal information that did not belong to them were

5780 Powers Ferry Road, N.W.
Atlanta, GA 30327-4390

Tel.: 770.850.7780
Fax: 770.850.7660

Attorney General Douglas F. Gansler
July 1, 2010
Page 2

HR or benefits professionals in trusted positions who are used to handling similar confidential information. We will offer credit monitoring services to affected consumers.

OTHER NOTIFICATION AND CONTACT INFORMATION.

Should you have additional questions or concerns, please do not hesitate to contact me at 770-980-6532. Thank you.

Sincerely yours,

Lael E. Bellamy /RK

Lael E. Bellamy

LEB/tah
Attachment

**COMPLIANCE**

Judith K. Ginter
Chief Compliance Officer, Employee Benefits

July 1, 2010

NAME
Street
City, MD

Dear:

This letter is to inform you that an electronic file containing your personal information was inadvertently made available to another company's Human Resources (HR) department due to an isolated administrative error which has been resolved. The file included your name and social security number. Upon discovery of the error, ING worked with the HR and IT Departments of the parties involved to assure that all data that was inadvertently made available was fully deleted from their systems.

Please be assured that we have safeguards in place to protect against improper disclosure of personal data. Strict guidelines exist to instruct our personnel on how personal information is to be gathered, stored and used. This protection also includes technologies that guard the confidentiality of our customer databases. In the instance that personal information is improperly disclosed, it is our policy to immediately take steps necessary to minimize the impact.

Although we believe the risk to you of identity theft is low, we are offering you one year of free credit monitoring and identity fraud coverage at our expense. We have arranged with Equifax, a leading credit reporting agency, to enroll you in this program if you are interested. If you wish to participate in the complimentary Equifax program, we have included a participant code for you to do so. Additional information regarding the Equifax service is included with this letter.

In the unlikely event that you find any suspicious activity, please contact us immediately so that we may further our investigation. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports, credit card statements and financial accounts periodically for unauthorized activity. In addition, you should review you credit card or other financial accounts for any suspicious and/or unauthorized activity.

Because of the increasing number of incidents of identity theft in the United States, the FTC has made available excellent advice on how you can protect yourself against such fraud. You should consider reviewing the identity theft materials posted for consumers on the FTC's Web site, www.ftc.gov/bcp/edu/microsites/idtheft/ and particularly, the posted copy of the FTC's booklet, "Take Charge: Fighting Back Against Identity Theft." You may also write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580 or call the FTC's toll-free Identity Theft helpline at 1-877-ID-THEFT (1-877-438-4338) (TTY: 1-866-653-4261).

20 Washington Ave. S. - Route 7781
Minneapolis, MN 55401

Tel: (612) 372-1108
Fax: (612) 342-3695
E-Mail: Judie.Ginter@us.ing.com

Insurance products issued by ReliaStar Life Insurance Company, ReliaStar Life Insurance Company of New York, members of ING.

Additional information on protecting yourself from identity theft is also available from the Maryland Attorney General's office. You should consider reviewing the identity theft materials posted for consumers on the Maryland Attorney General's Web site, <http://www.oag.state.md.us/idtheft/index.htm>. You may also contact the Maryland Attorney General's ID theft unit at 410-576-6491, idtheft@oag.state.md.us or 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

The Maryland Attorney General's office recommends that you review your credit report from each of the three credit reporting agencies twice per year. You can stagger them so you are looking at a fresh report every two months. Under Maryland and federal law, you are entitled to two FREE credit reports from each of the Credit Reporting Agencies each year. Go to www.annualcreditreport.com or call 1-877-322-8228 to access your report through the federal Fair Credit Reporting Act. You must contact each of the three Credit Reporting Agencies individually to access your credit report under Maryland law:

Equifax:

Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
Email to: security.dataadministration@equifax.com
1-800-685-1111

Experian:

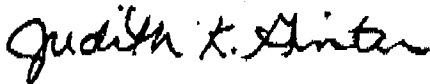
Consumer Fraud Assistance
P.O. Box 9556
Allen, TX 75013
Email to: businessrecordsvictimassistance@experian.com
1-888-397-3742

TransUnion:

Consumer Relations & Fraud Victim Assistance
1561 E. Orangethorpe Ave.
Fullerton, CA 92831
Email to: FVAD@Transunion.com
1-800-680-7289

We regret this incident and apologize for any inconvenience this may have caused you. We stand ready to answer your questions and are prepared to take any additional steps necessary to ensure your personal, confidential information is secure. Please call 1-800-748-4017 if you have any questions about this incident or need additional information.

Sincerely,



Judith K. Ginter

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

Equifax Credit Watch provides you with the following benefits:

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

How to Enroll

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

1. Consumer Information: complete the form with your contact information (name, address and e-mail address) and click “Continue” button. The information is provided in a secured environment.
2. Identity Verification & Payment Information: complete the form with your Social Security Number, date of birth, telephone numbers, create a User Name and Password, agree to the Terms of Use and *enter the promotion code provided at the top of your letter* in the “Enter Promotion Code” box and click “Continue” button. This code eliminates the need to provide a credit card number for payment. The system will ask you up to four security questions. This is the Equifax Identity Verification Process.
3. Order Summary: click “Continue” button.
4. Order Confirmation: – Click “View My Product” to access your 3-in-1 Credit Report and other 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. Promotion Code: You will be asked to enter your promotion code as provided at the top of your 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 our auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

To take advantage of Equifax
services, please use the
following promotional code:
CODE NUMBER