

EDWARDS ANGELL PALMER & DODGE LLP

20 Church Street Hartford, CT 06103 | 860.525.5065 fax 860.527.4198 eapdlaw.com

August 15, 2011

Federal Express

Attorney General Michael A. Delaney
New Hampshire State Attorney General's Office
33 Capitol Street
Concord, NH 03301

Re: The Lincoln National Life Insurance Company
Lincoln Life & Annuity Company of New York

Notification pursuant to N.H. Rev. Stat. § 359-C.20

Dear Attorney General Delaney:

On behalf of our clients, The Lincoln National Life Insurance Company and Lincoln Life & Annuity of New York (collectively referred to as the "Company"), we hereby notify you of the discovery of an incident that potentially exposed certain personal information (identified below) to unauthorized access. This incident involved approximately 91,763 individuals, of whom 1,204 are New Hampshire residents. It is important to note that an investigation conducted by the Company's Information Technology and Security teams, which was completed on August 3, 2011, revealed no evidence or reason to believe that customer information has been misused, and the Company has taken several immediate and important steps to eliminate the potential of further unauthorized access to personal information.

The incident involves a database maintained by the Company that contains information, including names and Social Security numbers, of former and current participants in retirement plans to which the Company provides products and services. Certain employees of the plan sponsors (*i.e.*, the employers of plan participants) have access to this database for the purpose of administering the plans. To assist the administrators to perform their duties, the database has a search function that administrators can use to search for and find specific participants. Recently, the Company learned that a programming issue would have returned search results that were not limited to an administrator's plan. Therefore, if an administrator searched a participant's name (or last name), the search results would have included participants of all plans bearing the same last name, and displayed their names and Social Security numbers. No other information, including no information concerning participants' beneficiaries, was available to administrators of other plans. As a result of this programming issue, however, the names and Social Security numbers of plan participants may have been exposed to plan administrators of other plans.

Learning about the Incident. On July 18, 2011, the Company was notified by a plan administrator that the search function on the database showed the names and Social Security numbers of employees who were not part of the administrator's plan. Although the names and Social Security numbers of individuals appeared as results of the search function, administrators were denied access to the complete files of participants other than participants in the administrator's plan.

Upon learning of the incident, the Company disabled the log on credentials of the plan administrator and disabled the search function. Once the problem was investigated and identified, the administrator's credentials were restored and participants' Social Security numbers were truncated. The search feature will not be restored, however, until an appropriate programming solution is identified, tested, and implemented.

Investigating the Incident. Upon discovery of this issue, the Company diligently investigated the incident and took actions to protect the personal information of individuals in the database.

The Company determined that the programming problem in the search function for the plan database began in 2009. Due to the comprehensive logging capabilities, the Company's Information Technology and Security teams were able to determine there was no pattern or any suspicious activity that would indicate individuals with access to the database were intentionally viewing the Social Security numbers of plan participants. There is also no indication that the results of database searches were printed, downloaded, or exported.

To date, the Company has no evidence or reason to believe that personal information of plan participants was subjected to misuse. The Company is unaware of any reported instance of identity theft or fraud related to this incident.

Remedial Measures. The Company has taken several important steps to protect personal information of its customers and to prevent this type of incident from occurring in the future, including the following:

- (1) The database search function was disabled and will remain disabled until an appropriate solution is identified, tested, and implemented; and
- (2) Plan participants will receive notification in the form enclosed as Exhibit A, by first class mail on or about August 17, 2011, and the offer of free credit monitoring.

The notice to plan participants will alert them of the incident and enable them to take immediate steps to protect themselves against possible identity theft or other monetary damage.

The notification will also describe the various services the Company has made available free of charge to affected individuals through Kroll, Inc. The Company engaged Kroll to provide affected individuals toll-free access to its Customer Solutions Center, along with free credit

EDWARDS ANGELL PALMER & DODGE LLP

Attorney General Michael A. Delaney

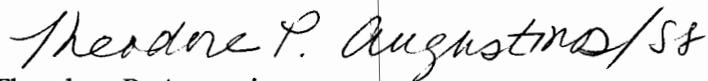
August 15, 2011

Page 3

monitoring services and identity theft consultation and restoration services. The enrolled individual's credit file will be monitored for critical changes, including address changes, inquiries, new trade-lines, derogatory notices and appearances of certain public records. Individuals will be informed of such changes by either postal or electronic mail. If a person suspects or discovers fraudulent activity, Kroll, as part of the identity theft restoration services, will assist the person with restoring their identity.

We trust that this letter and its enclosures provide you with all the information required to assess this matter. Please let us know if you have any additional question or if we may be of further assistance.

Sincerely,



Theodore P. Augustinos

Enclosure

cc: Paula Mango
Privacy Officer, Lincoln Financial Group



URGENT — Please Open Immediately.

<<FirstName>> <<MiddleName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<StateProvince>> <<PostalCode>>
<INTELLIGENT MAIL BARCODE>

<<Date>> (Format: Month Day, Year)

RE: Notification of disclosure of non-public personal information

Dear <<FirstName>> <<MiddleName>> <<LastName>>,

The purpose of this letter is to inform you that as a current or former employee of a retirement plan sponsor that has used the products and services of The Lincoln National Life Insurance Company or Lincoln Life and Annuity Company of New York (together referred to as "Lincoln") your personal information, consisting of your name and Social Security number, may have inadvertently been available to certain employees of other plan sponsors that have used products and services offered by Lincoln. Individuals that may have been able to see your information would have been limited to those authorized to access our secure website for purposes of administering their employer's plan. Although your information may have been exposed to administrators of other plans since October 2009, we have no evidence or reason to believe that your personal information has been misused by an unauthorized person. Upon discovery of this programming error on July 18, 2011, we notified the Lincoln Corporate Privacy Office and took immediate steps to remedy this situation to prevent further potential exposure.

While we have no indication that this inadvertent disclosure has resulted in the misuse of your information, out of an abundance of caution, we have engaged Kroll Inc. to provide its ID TheftSmart™ service for a 12-month period to help you detect any possible misuse of your data. Please see the attached information to assist you in enrolling in this service, which includes Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration services. In order to expedite delivery, this packet was prepared and mailed on behalf of Lincoln, from Kroll's secure print facility in Georgia.

To receive online credit services, please visit www.idintegrity.com to complete your authorization. If you would prefer to order and receive your credit services through the mail, please fill out and return the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form*. Please be aware that if you fill out and return the authorization form to receive credit services through the mail, you cannot sign up online.

Kroll's ID TheftSmart is one of the most comprehensive programs available to help protect against identity theft. We encourage you to take the time to review the safeguards made available to you. As always, we recommend that you review your statements and credit reports regularly. Please note that an enclosure to this letter contains certain information required to be provided to residents of certain states.

If you have any questions about the incident, would like to speak with someone to clarify or discuss the contents of this letter, or believe you may have an identity theft issue related to this incident, contact Kroll at 1-866-XXX-LFCus, Monday through Friday, 9:00am – 6:00pm Eastern Time.

<<ClientDef1>>(If you wish to speak to a Lincoln representative, please call our Customer Contact Center at 1-800-341-0441, Monday through Friday, 8:00am – 8:00pm Eastern Time.)

930F54-0811

We take our obligation to protect client information seriously, and deeply regret any inconvenience or concern that this incident may cause you. Again, we have no evidence or reason to believe that your personal information has been misused by any unauthorized person. We remain committed to maintaining your privacy and to making the protection of your information a key priority.

Sincerely,



Michelle Booth
Vice President
Defined Contribution Client Services

Enclosure

Kroll Inc. is not an affiliate of Lincoln National Corporation.

Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates. Affiliates are separately responsible for their own financial and contractual obligations.

PAD1108-0567 EMBC0811-2716

ID TheftSmart™

<<FirstName>> <<MiddleName>> <<LastName>>
Membership Number: <<MembershipNumber>>

Member Services: 1-866-XXX-LFCus
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday
If you have questions or feel you may have an identity theft issue,
please call ID TheftSmart member services.

U.S. State Notification Requirements

For residents of Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-888-4213 www.transunion.com
--	---	---

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take to avoid identity theft.

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	North Carolina Office of the Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com	Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/bcp/edu/microsites/idtheft/
---	--	--

For residents of Massachusetts and West Virginia:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or compliant with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse is a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348 www.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion (FVAD) P.O. Box 6790 Fullerton, CA 92834-6790 www.transunion.com
---	---	---