

Theodore P. Augustinos  
860.541.7710  
fax 888.325.9082  
taugustinos@eapdlaw.com

January 4, 2010

*Via Federal Express*

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

Re: Lincoln Financial Securities Corporation and  
Lincoln Financial Advisors Corporation  
Notification under N.H. Rev. Stat. 359-C:20

Dear Attorney General Delaney:

We write to advise you of a recent discovery of a vulnerability that existed in a portfolio information system used by our clients Lincoln Financial Securities Corporation ("LFS") and Lincoln Financial Advisors Corporation ("LFA"), which are broker-dealer subsidiaries of Lincoln National Corporation ("LNC"). Certain records involving approximately 1,200,000 individuals, of which approximately 18,900 are New Hampshire residents, could have been accessed because of the vulnerability. It is important to note that a forensic review by outside forensic consultants engaged in connection with this matter revealed no evidence or reason to believe that this vulnerability has subjected these individuals' personal information to acquisition or misuse, and LFS and LFA have taken several immediate and important steps to eliminate the potential of unauthorized access to personal information on the system.

The portfolio information system used by LFS and LFA integrates portfolio accounting and performance reporting to deliver a concise, single view of a customer's assets. It consolidates, on a daily basis, customer account data from hundreds of disparate sources, including proprietary, brokerage, insurance sponsors, retirement, managed accounts, alternatives and mutual funds. This system is not used to transfer funds or effect trades, but only for reporting and analysis of accounts. The customer data available through the portfolio information system includes the following information: names, addresses, Social Security numbers, account numbers, account registration, transaction details, account balances and, in some cases, dates of birth and email addresses.

**Learning about the Incident.** On August 17, 2009, LFS was advised by the Financial Industry Regulatory Authority ("FINRA") that FINRA had received from an unidentified source a username and password that provided access to the portfolio information system. This username

and password had been shared among certain employees of LFS and employees of affiliated companies. The sharing of usernames and passwords is not permitted under the LNC security policy. FINRA declined to inform LFS whether it had received the common username and password from a current employee of LFS or some other party. It was also discovered that LFA used shared usernames and passwords to access the portfolio information system.

**Investigating the Incident.** Immediately upon learning of the vulnerability in the security of the portfolio information system created by the use of shared usernames and passwords, LFS and LFA began an in-depth assessment to determine whether the system was accessed by any unauthorized individuals. LFS and LFA engaged the assistance of our law firm, Edwards Angell Palmer & Dodge LLP, as outside counsel. We engaged Kroll Ontrack, Inc. ("Kroll") to conduct a forensic investigation to determine the following:

- (i) Usage of shared usernames and passwords;
- (ii) Level of access that had taken place using the shared usernames and passwords;
- (iii) Consumer and employee records accessed with those shared usernames and passwords; and
- (iv) The identities of people who obtained access to the system using the shared usernames and passwords.

In investigating this vulnerability, it was discovered that, between LFS and LFA, there were a total of six shared usernames and passwords, which were created as early as 2002. These had all originally been created and distributed by the system administration team to certain home office and support staff to perform administrative functions, respond to registered representative inquiries and review client account activity. Other than FINRA, LFS and LFA have no knowledge that (i) anyone other than LFS, LFA or employees of affiliated companies had access to these shared usernames and passwords, (ii) that any employee ever used these usernames and passwords other than in the performance of their duties, or (iii) that any former employee used any such username and password after leaving LFS or LFA.

Kroll's forensic investigation revealed no evidence indicating that any access using shared usernames and passwords was unauthorized. There is, however, no evidence to support a conclusive determination that no such unauthorized access occurred.

To date, LFS and LFA have no evidence or reason to believe that this vulnerability has subjected customer personal information to acquisition or misuse. LFS and LFA also are unaware of any reported instance of identity theft or fraud related to this vulnerability. There is also no indication that use of shared usernames and passwords has compromised the security, confidentiality or integrity of the customers' personal information. LFS and LFA have therefore determined that this incident does not constitute a breach of security as defined under New Hampshire law. Nevertheless, LFS and LFA are voluntarily providing this notice and taking the precautionary measures as described below.

**Precautionary Measures Taken.** To address the vulnerability described above, LFS and LFA have taken several immediate and important steps to eliminate the potential of unauthorized access to personal information on the portfolio information system, including the following:

- (i) All shared usernames and passwords have been discontinued. LFS and LFA have heightened their enforcement of the existing LNC policy that prohibits shared usernames and passwords.
- (ii) Individuals whose personal information was exposed to this vulnerability will receive voluntary notification, and the offer of free credit monitoring.

The voluntary notices to potentially affected individuals will alert them of the vulnerability to their information out of an abundance of caution and enable them to take immediate steps to protect themselves against possible identity theft or other monetary damage. The voluntary notification will be provided in the form enclosed as Exhibit A, by first-class mail on or about January 6, 2010. The letter will, among other things, advise the affected individuals to remain vigilant by reviewing account statements and monitoring credit reports.

The notification will also describe the various services LFS and LFA have made available free of charge to affected individuals through Kroll. LFS and LFA have engaged Kroll to provide affected individuals toll-free access to its Consumer Solutions Center, along with free credit monitoring services and identity theft restoration services. Kroll will also provide free access to a credit report to affected individuals who enroll for the service. In addition, the enrolled individual's credit file will be monitored for critical changes, including address changes, inquiries, new trade-lines, derogatory notices and appearance 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 restoration services, will provide the affected individual with a toolkit of resources to address issues encountered.

As noted above, while LFS and LFA have not determined that a breach of security as defined by New Hampshire law has occurred, they have elected, on a voluntary basis, to notify your office and affected individuals of the vulnerability described above. They do so out of an abundance of caution and with full reservation of their rights in all respects. In addition, LFS and LFA are conducting a comprehensive review of their client information systems for similar vulnerabilities. Should additional similarly situated clients be identified, LFS and LFA will notify the affected individuals and offer the Kroll services as described above.

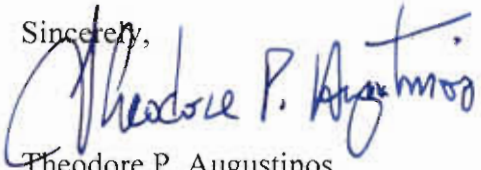
Attorney General Michael J. Delaney

January 4, 2010

Page 4

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 additional questions or if we may be of further assistance.

Sincerely,



Theodore P. Augustinos

Enclosure

cc: David Booth  
President, Lincoln Financial Securities Corporation  
Senior Vice President, Lincoln Financial Advisors Corporation

Christine Frederick  
Vice President and Associate General Counsel, Lincoln Financial Group



URGENT — Please Open Immediately.

<<FirstName>> <<MiddleName>> <<LastName>> <<Suffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<StateProvince>> <<PostalCode>>  
<POSTNET BARCODE>

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

Member Services: 1-866-XXX-DR1A, Monday through Friday  
If you have questions or feel you may have an identity theft issue,  
please call ID TheftSmart member services.

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

Safeguarding the privacy of our customers' information is a top priority at Lincoln Financial Securities Corporation ("LFS"). We are committed to protecting your information and recognize your need to know should it ever be compromised. The purpose of this letter is to inform you that LFS recently discovered that a portfolio information system used by LFS, which contains information including your name, Social Security number and financial account numbers, was potentially vulnerable to unauthorized access. We have no evidence or reason to believe that your information has been acquired or misused by an unauthorized person. We are notifying you out of an abundance of caution to make you aware of the circumstances and to inform you of the steps that LFS has taken to rectify the situation.

The portfolio information system integrates accounting and performance reporting of customer assets. This system is not used to transfer funds or effect trades, but only for reporting and analysis of accounts.

It is important to note that there is no indication that this vulnerability has compromised the security, confidentiality or integrity of your information. We have engaged outside forensic consultants, who conducted an in-depth investigation of the vulnerability related to the portfolio information system. We have also taken specific actions to improve our data security, as well as investigate other LFS client information systems for any vulnerabilities of this nature. We are continually strengthening our computer security policies and procedures across all of our information technology platforms.

Because securing your personal information is so important to us, and as a precautionary measure to help safeguard you against any possible misuse of your information, we have also engaged Kroll Inc. to provide its ID TheftSmart™ service. Kroll's service, offered at no cost to you for one year, includes Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration. Information about this service, and how you may take advantage of it at our expense, is enclosed.

Please note that to be eligible for the credit monitoring service, you need to be over the age of 18 with credit established in the U.S., have a Social Security number issued in your name, and have a U.S. residential address associated with your credit file.

To receive online credit services, please visit [www.idintegrity.com](http://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*. Note, however, 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.

If you have any questions about the incident, would like to speak with someone to clarify or discuss the contents of this letter, or feel you may have an identity theft issue, call [1-866-XXX-DRIA](tel:1-866-XXX-DRIA), 9:00 a.m. – 6:00 p.m. (Eastern Time), Monday through Friday.

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

Sincerely,

A handwritten signature in black ink, appearing to read 'D Booth', with a long horizontal stroke extending to the right.

David Booth  
President, Lincoln Financial Securities Corporation

## 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, Georgia 30374  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19022  
1-800-888-4213  
[www.transunion.com](http://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](http://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](http://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/](http://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 complaint 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 of 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](http://www.equifax.com)

#### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

#### **TransUnion (FVAD)**

P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)



URGENT — Please Open Immediately.

<<FirstName>> <<MiddleName>> <<LastName>> <<Suffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<StateProvince>> <<PostalCode>>  
<POSTNET BARCODE>



<<FirstName>> <<MiddleName>> <<LastName>>

Membership Number: <<MembershipNumber>>

Member Services: 1-866-XXX-DR1A

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.

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

Safeguarding the privacy of our customers' information is a top priority at Lincoln Financial Advisors Corporation ("LFA"). We are committed to protecting your information and recognize your need to know should it ever be compromised. The purpose of this letter is to inform you that LFA recently discovered that a portfolio information system used by LFA, which contains information including your name, Social Security number and financial account numbers, was potentially vulnerable to unauthorized access. We have no evidence or reason to believe that your information has been acquired or misused by an unauthorized person. We are notifying you out of an abundance of caution to make you aware of the circumstances and to inform you of the steps that LFA has taken to rectify the situation.

The portfolio information system integrates accounting and performance reporting of customer assets. This system is not used to transfer funds or effect trades, but only for reporting and analysis of accounts.

It is important to note that there is no indication that this vulnerability has compromised the security, confidentiality or integrity of your information. We have engaged outside forensic consultants, who conducted an in-depth investigation of the vulnerability related to the portfolio information system. We have also taken specific actions to improve our data security, as well as investigate other LFA client information systems for any vulnerabilities of this nature. We are continually strengthening our computer security policies and procedures across all of our information technology platforms.

Because securing your personal information is so important to us, and as a precautionary measure to help safeguard you against any possible misuse of your information, we have also engaged Kroll Inc. to provide its ID TheftSmart™ service. Kroll's service, offered at no cost to you for one year, includes Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration. Information about this service, and how you may take advantage of it at our expense, is enclosed.

Please note that to be eligible for the credit monitoring service, you need to be over the age of 18 with credit established in the U.S., have a Social Security number issued in your name, and have a U.S. residential address associated with your credit file.

To receive online credit services, please visit [www.idintegrity.com](http://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*. Note, however, 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.



If you have any questions about the incident, would like to speak with someone to clarify or discuss the contents of this letter, or feel you may have an identity theft issue, call **1-866-XXX-DRIA**, 9:00 a.m. – 6:00 p.m. (Eastern Time), Monday through Friday.

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

Sincerely,

Sincerely,

A handwritten signature in black ink, appearing to read 'D Booth', with a horizontal line extending to the right.

David Booth  
Senior Vice President, Lincoln Financial Advisors Corporation

## 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, Georgia 30374  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19022  
1-800-888-4213  
[www.transunion.com](http://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](http://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](http://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/](http://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 complaint 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 of 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](http://www.equifax.com)

#### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

#### **TransUnion (FVAD)**

P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)