

Good Morning,

Pursuant to MD Code Commercial Law §14-3504, I am writing to notify you of an incident that may have caused the personal information of 204 Maryland residents to be subject to unauthorized access. Lincoln Financial Securities Corporation ("Lincoln") recently determined that an independent financial professional was the victim of a malware attack which resulted in unauthorized access to his computer for a period of time from July 31, 2021, to September 17, 2021.

When Lincoln learned of the access, Lincoln assisted the financial professional in securing the computer and initiated a forensic investigation into the unauthorized access. Outside counsel, working with a security firm, was then engaged to review the compromised computer. When the security firm's findings were reviewed by Lincoln on December 17, 2021, it was determined that the Maryland residents' personal information, such as name, address, date of birth, Social Security number, driver's license number, bank account information, credit card number and PIN, financial account number and/or medical information may have been exposed.

Attached is a draft notification which will be mailed to Maryland residents on or around January 14, 2022, and will include an offer for a complimentary, one-year membership in a credit and identity monitoring service provided by Kroll. We continue to work diligently to minimize the impact of this incident and enhance our cybersecurity posture, as appropriate.

Please let me know if you have any additional questions, or if I may be of further assistance.



Sara Borghesi
Sr. Compliance Consultant
Privacy

Lincoln Financial Group
LincolnFinancial.com

860-202-2791 Mobile



Notice of Confidentiality: **This E-mail and any of its attachments may contain Lincoln National Corporation proprietary information, which is privileged, confidential, or subject to copyright belonging to the Lincoln National Corporation family of companies. This E-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this E-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this E-mail is strictly prohibited and may be unlawful. If you have received this E-mail in error, please notify the sender immediately and permanently delete the original and any copy of this E-mail and any printout. Thank You.**

Notice of Confidentiality: **This E-mail and any of its attachments may contain Lincoln National Corporation proprietary information, which is privileged, confidential, or subject to copyright belonging to the Lincoln National Corporation family of



Lincoln Financial Securities Corporation
130 N. Radnor-Chester Road
Radnor, PA 19087-5221
www.lincolnfinancial.com

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to inform you of an incident that may have affected some of your personal information.

What Happened

Lincoln Financial Securities Corporation ("Lincoln") recently determined that Michael Mooney, an independent financial professional, was the victim of a malware attack that resulted in unauthorized access to his computer for a period of time from July 31, 2021, to September 17, 2021. We have also determined that your personal information may have been exposed due to this unauthorized access. Your personal information was provided to Michael Mooney as an owner, insured, annuitant, or beneficiary associated with a financial account.

What Information Was Involved

Based on the facts known to Lincoln at this time, the personal information affected by this unauthorized access may have included a combination of your <<b2b_text_1(name, data elements)>>. At this time, we have no evidence that your information has been misused.

What We Are Doing

We take our obligation to protect the information we receive seriously. Once the incident was discovered we quickly took action to minimize risks, including securing the compromised computer and initiating a forensic investigation regarding the unauthorized access.

What You Can Do

We have arranged to provide you with a complimentary one-year membership in Kroll's identity monitoring services to help protect your identity. We encourage you to be vigilant in monitoring your account statements and credit reports regularly for potential identity theft. Details on how to activate the free identity monitoring services are below.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter. For more information about Kroll and their identity monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate the identity monitoring services offline and receive monitoring alerts via the US Postal Service, you may activate using Kroll's automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time. Please note that to activate monitoring services, you will be required to provide your name, your membership number listed above, date of birth, and Social Security number through Kroll's automated phone system.

For More Information

We apologize for any inconvenience or concern that this matter may cause you. We continue to work diligently to address the impact of this incident, and continually assess our cybersecurity policies and procedures, enhancing them as appropriate. If you have any questions, please have your membership number ready and contact [1-800-833-8333](tel:1-800-833-8333), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'Stafford Moser', followed by a horizontal line.

Stafford Moser
SVP, Co-Head of Lincoln Financial Securities, Head of GA Channel
Lincoln Financial Network

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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 Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, 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).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have 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 contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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 Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

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

For DC residents: You may contact the DC Office of the Attorney, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, 202-727-3400, <http://www.oag.dc.gov>

For RI residents: You may contact the RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.