

New York Life Insurance Company
PO Box 130539
Dallas TX 75313-0539



February 14, 2024

Submitted via email to: Idtheft@oag.state.md.us

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

Re: Information Security Incident Affecting 1 Maryland Resident

To Whom it May Concern:

Pursuant to Md. Code Ann. Comm. Law 14-3504, we are sending this letter to notify you of an information security incident.

Cumberland Advisors, Inc. ("Cumberland") a sub-advisor to Evestnet, was the victim of a business email compromise as explained below. Evestnet is an asset management platform used by Eagle Strategies LLC (a subsidiary of New York Life Insurance Company) that provides investment advisory services to Eagle Strategies customers.

On September 5, 2023, Cumberland discovered suspicious activity related to an employee email account. Cumberland immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to two (2) employee email accounts between August 31 and September 5, 2023. Therefore, Cumberland undertook a comprehensive and time-intensive review of the contents of the email accounts to determine what information was contained therein and to whom it related. The unauthorized access was related to these email accounts; this situation did not provide unauthorized access to Cumberland's core portfolio management system used by Cumberland to manage client investment accounts. On November 20, 2023, Cumberland finalized this review and determined that information related to certain customers was contained within the impacted accounts, including name, address, account number, Social Security Number, and date of birth. Cumberland subsequently took steps to enhance its existing security protocols and is evaluating its policies and procedures related to data privacy and security.

Cumberland, on behalf of New York Life, is mailing notifications to the affected individuals on February 14, 2024 and offering 12 months of credit monitoring and identity protection services through Experian. New York Life continued to follow-up with Cumberland to ensure notifications were promptly mailed to affected individuals. Cumberland stated that the delay in mailing notifications was due to difficulties coordinating with other impacted firms.

Attached is a sample of the notification letter sent to the 1 resident of your state. Please feel free to call me at (212) 576-5244 if you have any questions or require additional information.

Sincerely,

/s/ Justin Keslowitz

Justin Keslowitz

[COMPANY LOGO]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Date>>

<<City>>, <<State>> <<Zip>>

<<Country>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

Cumberland Advisors, Inc. ("Cumberland") is writing to notify you of an incident that may have involved some of your information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it's necessary to do so.

What Happened? On September 5, 2023, Cumberland discovered suspicious activity related to an employee email account. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to two (2) employee email accounts between August 31 and September 5, 2023. Therefore, Cumberland undertook a comprehensive and time-intensive review of the contents of the email accounts to determine what information was contained therein and to whom it related. The unauthorized access was related to these email accounts; it is important to note that this situation would not have provided unauthorized access to our core portfolio management system used by Cumberland to manage client investment accounts. On November 20, 2023, we finalized this review and determined that information related to you was identified within the impacted accounts.

What Information Was Involved? The information contained in the impacted accounts included your: [insert data elements]. Cumberland is not aware of any actual misuse of this information as a result of the event.

What We Are Doing. Cumberland takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the issue, we immediately commenced an investigation to confirm the nature and scope, and to identify what information could have been affected. We also took steps to enhance our existing security protocols and are evaluating our policies and procedures related to data privacy and security.

As an added precaution, we are offering you access to twelve/twenty-four (12/24) months of complimentary credit monitoring and identity protection services through [vendor] at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. We further encourage you to enroll in the complementary services being provided through [vendor].

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions please call ###-###-#### Monday through Friday from #:00 a.m. to #:00 p.m. or Saturday and Sunday from #:00 a.m. to #:00 p.m. Eastern Time, excluding US holidays. You may also write to Cumberland at 2 North Tamiami Trail, Suite 303, Sarasota, Florida. 34236.

Sincerely,

Cumberland Advisors, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

[Enrollment Instructions]

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [X] Rhode Island residents that may be impacted by this event.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 14, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Cumberland Advisors, Inc. ("Cumberland") located at 2 North Tamiami Trail, Suite 303, Sarasota, FL 34236. We are writing to supplement our December 20, 2023 notification to your office regarding an incident that may affect the security of certain personal information relating to an additional twenty-seven (27) Maryland residents. Our previous notification to your office is attached as ***Exhibit AA***. This notice will be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Cumberland does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 5, 2023, Cumberland discovered suspicious activity related to an employee email account. Cumberland immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Cumberland's investigation determined that there was unauthorized access to two (2) employee email accounts between August 31 and September 5, 2023. Therefore, Cumberland undertook a comprehensive and time-intensive review of the contents of the email accounts to determine what information was contained therein and to whom it related. It is important to note that the unauthorized access was limited to two (2) email accounts and that there was no access to Cumberland's core portfolio management system. On November 20, 2023, Cumberland finalized this review and determined that information related to Maryland residents may have been impacted. The information that could have been subject to unauthorized access includes name, financial account information, and Social Security number.

As Cumberland does not own some of the data at issue, Cumberland provided notice of the incident to appropriate data owners after its review was completed, and offered to provide notices on their behalf to

individuals and regulators. Since providing its initial notice, Cumberland continued to work with data owners and is now providing notice on certain data owners' behalf.

Notice to Maryland Residents

On February 14, 2024, Cumberland provided written notice of this incident to an additional twenty-seven (27) Maryland residents. In total, Cumberland provided notice to forty-four (44) Maryland residents in relation to this event. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit BB**.

Other Steps Taken and To Be Taken

Upon discovering the event, Cumberland moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, Cumberland notified federal law enforcement and implemented additional safeguards. Cumberland is providing individuals whose personal information was potentially affected by this incident access to credit monitoring services for two (2) years through Experian.

Additionally, Cumberland is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Cumberland is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Cumberland is providing written notice of this incident to relevant state regulators and to the three major consumer credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,

A handwritten signature in black ink, appearing to read "Colin D. Scanlon". The signature is fluid and cursive, with the first name "Colin" being more prominent.

Colin D. Scanlon of
MULLEN COUGHLIN LLC

EXHIBIT AA

From: Ian Mandell
Sent: Wednesday, December 20, 2023 5:50 PM
To: idtheft@oag.state.md.us
Cc: Colin Scanlon; Jennifer McKelvie; Kelsey Hutchinson
Subject: Notice of Data Event - Cumberland Advisors - MD
Attachments: Notice of Data Event - Cumberland - MD.pdf

Dear Sir or Madam,

Please see the attached Notice of Data Event.

Ian Mandell

Attorney

Mullen Coughlin LLC

426 W. Lancaster Avenue, Suite 200

Devon, PA 19333

(267) 930-4208 - Office

(267) 401-5298 - Mobile

imandell@mullen.law

<https://www.mullen.law/>

This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 20, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Cumberland Advisors, Inc. ("Cumberland") located at 2 North Tamiami Trail, Suite 303, Sarasota, FL 34236, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seventeen (17) Maryland residents. This notice will be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Cumberland does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 5, 2023, Cumberland discovered suspicious activity related to an employee email account. Cumberland immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Cumberland's investigation determined that there was unauthorized access to two (2) employee email accounts between August 31 and September 5, 2023. Therefore, Cumberland undertook a comprehensive and time-intensive review of the contents of the email accounts to determine what information was contained therein and to whom it related. It is important to note that the unauthorized access was limited to two (2) email accounts and that there was no access to Cumberland's core portfolio management system. On November 20, 2023, Cumberland finalized this review and determined that information related to Maryland residents may have been impacted. The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Notice to Maryland Residents

On December 20, 2023, Cumberland provided written notice of this incident to seventeen (17) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. As Cumberland does not own some of the data at issue, Cumberland also provided notice to

appropriate data owners who may request that Cumberland provide additional notices on their behalf to individuals and regulators. Accordingly, Cumberland may supplement this notice as needed to report additional residents who are notified on behalf of one or more data owners.

Other Steps Taken and To Be Taken

Upon discovering the event, Cumberland moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, Cumberland notified federal law enforcement and implemented additional safeguards. Cumberland is providing individuals whose personal information was potentially affected by this incident access to credit monitoring services for one (1) year through Experian.

Additionally, Cumberland is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Cumberland is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Cumberland is providing written notice of this incident to relevant state regulators and to the three major consumer credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,

A handwritten signature in black ink, appearing to read "Colin D. Scanlon". The signature is fluid and cursive, with the first name "Colin" being more prominent.

Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS/jlm
Enclosure

EXHIBIT A



CUMBERLAND
— ADVISORS —

Return Mail Processing
PO Box 999
Suwanee, GA 30024

41804*****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



December 20, 2023

NOTICE OF [Extra3]

Dear Sample A. Sample:

Cumberland Advisors, Inc. (“Cumberland”) is writing to notify you of an incident that may have involved some of your information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it’s necessary to do so.

What Happened? On September 5, 2023, Cumberland discovered suspicious activity related to an employee email account. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to two (2) employee email accounts between August 31 and September 5, 2023. Therefore, Cumberland undertook a comprehensive and time-intensive review of the contents of the email accounts to determine what information was contained therein and to whom it related. The unauthorized access was related to these email accounts; it is important to note that this situation did not provide unauthorized access to our core portfolio management system used by Cumberland to manage client investment accounts. On November 20, 2023, we finalized this review and determined that information related to you was identified within the impacted accounts.

What Information Was Involved? The information contained in the impacted accounts included your: [Extra1]. Cumberland is not aware of any actual misuse of this information as a result of the event.

What We Are Doing. Cumberland takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the issue, we immediately commenced an investigation to confirm the nature and scope, and to identify what information could have been affected. We also took steps to enhance our existing security protocols and are evaluating our policies and procedures related to data privacy and security.

As an added precaution, we are offering you access to [Extra4] months of complimentary credit monitoring and identity protection services through Experian at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. We further encourage you to enroll in the complementary services being provided through Experian.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 833-514-1448 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding US holidays. You may also write to Cumberland at 2 North Tamiami Trail, Suite 303, Sarasota, Florida. 34236.

Sincerely,

Cumberland Advisors, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra4] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra4] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra4]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** March 29, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-514-1448** by March 29, 2024. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra4]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 0 Rhode Island residents that may be impacted by this event.

EXHIBIT BB



CUMBERLAND
— ADVISORS —

Return Mail Processing
PO Box 999
Suwanee, GA 30024

411056 *****SINGLP

SAMPLE A. SAMPLE - General

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



February 14, 2024

NOTICE OF [Extra3]

Dear Sample A. Sample:

Cumberland Advisors, Inc. (“Cumberland”) is writing to notify you of an incident that may have involved some of your information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it’s necessary to do so.

What Happened? On September 5, 2023, Cumberland discovered suspicious activity related to an employee email account. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to two (2) employee email accounts between August 31 and September 5, 2023. Therefore, Cumberland undertook a comprehensive and time-intensive review of the contents of the email accounts to determine what information was contained therein and to whom it related. The unauthorized access was related to these email accounts; it is important to note that this situation would not have provided unauthorized access to our core portfolio management system used by Cumberland to manage client investment accounts. On November 20, 2023, we finalized this review and determined that information related to you was identified within the impacted accounts.

What Information Was Involved? The information contained in the impacted accounts included your: [Extra1]. Cumberland is not aware of any actual misuse of this information as a result of the event.

What We Are Doing. Cumberland takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the issue, we immediately commenced an investigation to confirm the nature and scope, and to identify what information could have been affected. We also took steps to enhance our existing security protocols and are evaluating our policies and procedures related to data privacy and security.

As an added precaution, we are offering you access to twenty-four (24) months of complimentary credit monitoring and identity protection services through Experian at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. We further encourage you to enroll in the complementary services being provided through Experian.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions please call 833-918-1125 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding US holidays. Be prepared to provide your engagement number B116481. You may also write to Cumberland at 2 North Tamiami Trail, Suite 303, Sarasota, Florida 34236.

Sincerely,

Cumberland Advisors, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for twenty-four (24) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24)-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** May 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/plus>
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1125 by May 31, 2024. Be prepared to provide engagement number B116481 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There is approximately 1 Rhode Island resident that may be impacted by this event.