LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
One PPG Place, 28th Floor
Pittsburgh, Pennsylvania 19522
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

February 14, 2022

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents CIC Wealth ("CIC"), a financial advisory firm headquartered in Rockville, Maryland in connection with a recent data security incident that may have affected the information of certain Maryland residents. This letter is being sent in pursuant to Md. Code Ann. Com m. Law 14-3504. The incident in question is described in further detail below.

1. NATURE OF THE SECURITY INCIDENT

On November 8, 2021, a CIC Wealth employee reported suspicious activity in its email environment. CIC Wealth immediately undertook efforts to secure its environment and commenced an internal investigation into the incident. CIC Wealth engaged leading, independent cybersecurity experts to assist in a forensic investigation, as well as a detailed and thorough review of information involved in the incident. As a result of its investigation, CIC Wealth learned that an unauthorized actor had access to one employee's email account from November 5 to November 7, 2021, that contained personal information belonging to some of CIC Wealth's clients. CIC immediately worked to collect the contact information for the individuals whose personal information was potentially impacted, including ten Maryland residents, which was completed on February 1, 2022.

The information potentially accessed without authorization may have included the first and last name, Social Security Number, driver's license number or state ID number, medical diagnosis or treatment information, health insurance information, and health insurance number of the individuals. To date, CIC has no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. NUMBER OF MARYLAND RESIDENTS AFFECTED

CIC notified ten (10) Maryland residents of this data security incident via first class U.S. mail on February 14, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. STEPS TAKEN RELATING TO THE INCIDENT

CIC implemented additional security features to reduce the risk of a similar incident occurring in the future. CIC also reported this incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to attempt to hold the perpetrators of this incident accountable, if possible.

While CIC has no indication that the information has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information. As a further precaution, CIC is also offering the Maryland consumers one (1) year of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of personal information and provides consumers whose information may have been accessed without authorization with identity protection support.

4. CONTACT INFORMATION

CIC is committed to protecting the security of the personal information in their possession. Please feel free to contact me at Lauren.Godfrey@LewisBrisbois.com or by phone at 412-567-5113 if you have any further questions.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

LDG
Enclosure: Sample Consumer Notification Letter

CIC Wealth, LLC
Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 14, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a recent data security incident discovered by CIC Wealth, LLC ("CIC Wealth") that may have impacted your personal information. CIC Wealth takes the privacy and security of all personal information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that CIC Wealth is making available to assist you.

What Happened? On November 8, 2021, CIC Wealth discovered abnormal activity in its email environment. Upon learning of this activity, CIC Wealth immediately undertook efforts to secure its environment and commenced an internal investigation into the incident. CIC Wealth engaged leading, independent cybersecurity experts to assist in the investigation including a detailed and thorough review of information involved in the incident. As a result of its investigation, CIC Wealth learned that an unauthorized actor had access to one employee's email account from November 5 to November 7, 2021, that contained personal information belonging to some of CIC Wealth's clients. We immediately worked to collect the contact information for the impacted individuals, and to notify you of this incident.

CIC Wealth has no evidence that any potentially affected information has been misused. Nonetheless, CIC Wealth is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal information.

What Information Was Involved? The following types of personal information may have been involved: your name and <<variable data.>>

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also began working with cybersecurity experts to identify areas in which we can further improve the security of our network to reduce the likelihood of a similar event occurring in the future. Additionally, CIC Wealth reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help protect your identity following this incident, CIC Wealth has secured the services of IDX to provide credit monitoring and identity theft restoration services at no cost to you for <<variable 2>>. IDX is a global leader in risk mitigation and response, and the IDX team has extensive experience helping people who have sustained an unintentional exposure of personal data. To enroll, call 1-800-939-4170 or visit the following website: https://app.idx.us/account-creation/protect . The enrollment code is <<XXXXXXXX>>. The enrollment period ends on May 14, 2022.

What You Can Do. CIC Wealth encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

CIC Wealth also encourages you to take full advantage of the services offered to you through IDX. IDX representatives are available to answer questions or address concerns you may have regarding protection of your information. IDX call center representatives are available Monday through Friday from 9:00 A.M to 9:00 P.M Eastern Time and can be reached by calling 1-800-939-4170.

For More Information. If you have questions or need assistance, please call 1-800-939-4170, Monday through Friday from 9:00 A.M to 9:00 P.M Eastern Time. Please accept our sincere apologies and know that CIC Wealth deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Frank Cappadora, Jr.
Managing Partner & Chief Compliance Officer
CIC Wealth, LLC

Additional Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Change Usernames or Passwords: Out of an abundance of caution, we recommend that you promptly change usernames, passwords, and/or security questions and answers in order to protect your online accounts that use the same login information impacted by this incident.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	Washington D.C. Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	441 4th Street, NW
Washington, DC 20580	Baltimore, MD 21202	Washington, DC 20001
consumer.ftc.gov, and	oag.state.md.us	oag.dc.gov
www.ftc.gov/idtheft	1-888-743-0023	1-202-727-3400
1-877-438-4338		

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf