

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

JASON M. GOODWIN
jgoodwin@c-wlaw.com

NICHOLAS MARTIN
nmartin@c-wlaw.com

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

January 9, 2024

Via Email (idtheft@oag.state.md.us)

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

RE: Data Security Incident Notification

To Whom It May Concern:

We serve as counsel for Capital Formation Group, Inc., ("CFG") located at 62 Walnut Street, Wellesley, Massachusetts, 02481. We write to provide notification of a recent data security incident. By providing this notice, CFG does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On October 24, 2023, CFG became aware of unusual activity related to an employee's email account. Upon discovery, CFG engaged a third-party forensic team to conduct a thorough investigation. This investigation identified unauthorized access between September 19, 2023, through October 26, 2023. Importantly, the investigation identified no evidence that a mailbox sync or download may have occurred. Further, the investigation identified limited activity performed by the unauthorized individual. While we understand the information associated with the identified activity to be minimal, CFG could not definitively rule out access to additional information and is therefore providing notification to those individuals whose information may have been present within the affected account(s) and thereby at risk. CFG reviewed the potentially impacted information to identify those whose information may have been at risk. This review was completed on or around November 20, 2023.

On January 3, 2024, CFG received its results from a National Change of Address (NCOA) search and confirmed this incident potentially affected one (1) Maryland resident. The information at risk included first and last name, financial account number, driver's license number, medical information, health insurance information and/or Social Security numbers.

In response to this incident, CFG conducted an investigation, notified law enforcement, changed account passwords and reset multi-factor authentication. Additionally, CFG began providing notice to the potentially affected individuals on January 9, 2023 via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, CFG is offering the potentially impacted individuals complimentary credit monitoring and identity protection services.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: 
Jason M. Goodwin, Esq.

Exhibit A



62 Walnut Street
Wellesley, MA 02481

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

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

January 9, 2024

<<NOTICE OF DATA BREACH>>

Dear <<First Name>> <<MI>> <<Last Name>> <<Suffix>>:

Capital Formation Group, Inc. (“CFG”) writes to notify you of an incident that may have involved some of your personal information as described below. We take the privacy of information in our care seriously. We are providing you with information about the incident, our response, and steps you can take to protect your information.

What Happened: We recently identified suspicious activity related to an employee email account. Upon discovery, we took immediate action to address and investigate the incident, including performing a password reset and engaging third-party specialists to assist in conducting a full investigation. The investigation ultimately determined that certain employee email accounts were accessed by an unauthorized person from September 19, 2023, through October 25, 2023. The investigation was unable to determine how the unauthorized person accessed the emails, but there is no evidence to suggest a CFG employee interacted with a phishing email. Additionally, while the investigation was unable to determine the full scope of information potentially accessed, the investigation confirmed that the method of access to the account involved would not permit the full mailbox to be downloaded. While the unauthorized activity was focused on unsuccessful attempts to redirect funds, additional activity could not be definitively ruled out. Therefore, CFG worked to identify individuals whose information may have been present within the affected account out of an abundance of caution.

What Information Was Involved: On November 20, 2023, we completed our review and determined the account included your first and last name, in combination with the following data elements: <<Variable Data 1>>.

What We Are Doing: Upon learning of this incident, we immediately took the steps outlined above to reset passwords and multifactor authentication sessions. While CFG has previously implemented protective measures to prevent such incidents, the unauthorized person was able to bypass these measures. Additionally, we are offering you <<CM Length>> months of complimentary credit monitoring and identity protection services through IDX, A ZeroFox Company, in an abundance of caution.

What You Can Do: You may enroll in the credit monitoring services we are making available to you. We have also provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information: The security of information is of the utmost importance to us. We stay committed to protecting

your trust in us and continue to be thankful for your support. This letter is written in an attempt to fulfill regulatory obligations. I encourage you to call me in order to discuss this in further detail at 978-318-0544 or 781-237-0123. Should you have questions regarding the monitoring services being made available to you, please contact our dedicated call center at 1-800-939-4170. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

Sincerely,

John Williams
Chief Executive Officer
Capital Formation Group

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is April 9, 2024.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

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

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

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

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

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

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>. You may also write to Capital Formation Group at 62 Walnut Street, Wellesley, MA 02481.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. You may also write to Capital Formation Group at 62 Walnut Street, Wellesley, MA 02481.

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