



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

March 27, 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 CRC Companies LLC and its related companies, including CBG Building Company LLC, CEG Solutions LLC, ("CRC"), located at 4401 Fairfax Drive, Suite 800, Arlington, VA 22203, are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately ninety-nine (99) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CRC 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 January 6, 2023, CRC began receiving reports of fraudulent bank activity on employee bank accounts associated with direct deposit. Upon receiving of these reports, CRC launched an investigation into the activity and to confirm if the activity is connected to CRC. On behalf of CRC, we engaged cybersecurity specialists to determine if certain employee information may have been subject to unauthorized access thorough an accounting vendor. No evidence of suspicious activity was found in the CRC environment, however, certain information was being shared with a third party vendor. On or around March 7, 2023, the investigation concluded that sensitive employee information may have been accessible as a result of this engagement. CRC is providing notice to individuals in an abundance of caution.

Notice to Maryland Residents

On or about March 27, 2023, CRC provided written notice of this incident to approximately ninety-nine (99) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, CRC moved quickly to investigate and respond to the incident, assess the security of CRC systems, and identify potentially affected individuals. CRC is also working to implement additional safeguards for employees. CRC is providing access to credit monitoring services for 24 months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CRC 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. CRC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against fraud, 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. CRC is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/jrl
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

J2074-L05-0000005 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L05 CRCFORMAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



March 27, 2023

NOTICE OF [Extra2]

Dear Sample A. Sample:

We are making you aware of an incident that may impact the privacy of some of your information. We are providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? As we previously notified you, we began receiving reports on January 6, 2023 of fraudulent checks being presented against employee direct deposit bank accounts. Following reports of these fraudulent checks, we immediately launched an investigation and engaged a third-party cybersecurity specialist. On March 7, 2023, the specialist determined that an outside accounting vendor moved confidential employee data out of our secure environment and onto unsecure platforms. **This data included employee names, addresses, bank account numbers, and Social Security numbers.** The specialist believes this vendor's actions were likely the source of the bank account data leak that led to the fraudulent checks. No evidence has been found that any leaks occurred within our environment. We have shut down the vendor's access to our system and are continuing to investigate this matter in an attempt to identify any parties involved.

What Information Was Involved? The information moved out of our secure environment and into unsecure platforms included employee names, addresses, bank account numbers, and Social Security numbers.

What We Are Doing. We treat our responsibility to safeguard the information entrusted to us as an utmost priority. As such, we responded promptly to this incident and have been working diligently to provide you with an accurate and complete notice of the incident.

As an added precaution, we are providing you with 24 months of complimentary access to credit monitoring and identity restoration services through April of 2025, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

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 free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. In addition, we encourage you to contact your bank to close the account that you use to direct deposit your paycheck and open a new account. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Information*. There you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.

0000005



For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call Kenya Manning at 703-294-4553 or contact her at kenya.manning@crccompanies.com.

Sincerely,

Human Resources Department

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 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 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 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 June 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- 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 1-877-890-9332 by June 30, 2023. Be prepared to provide engagement number B088437 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your 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, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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.

