

December 3, 2024

WRITER'S DIRECT NUMBER: 317-236-2243
EMAIL: Sid.Bose@icemiller.com**VIA EMAIL:** idtheft@oag.state.md.us

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

Dear Sir or Madam:

Ice Miller LLP represents GEMCO Constructors, LLC ("GEMCO"). We are writing to notify you of a security incident involving the personal information of **seven (7)** Maryland residents.

On or about June 5, 2024, GEMCO was alerted to unauthorized activity on its networks through its monitoring systems. GEMCO promptly initiated a response to the alert and began investigating the anomalous activity. GEMCO also took protective actions to stop any unauthorized access to its systems, and also engaged a leading security and forensics company to help investigate the matter. GEMCO found that an unauthorized third-party was attempting to interfere with GEMCO's IT systems. Based on its investigations, GEMCO believes the incident may have begun on or around June 3, 2024. GEMCO was able to restore its systems by June 10, 2024.

GEMCO worked diligently to take measures necessary to determine the scope of the breach, prevent any disclosures, and restore the reasonable integrity of its systems. The incident primarily involved GEMCO's internal IT systems. As part of its investigative efforts, GEMCO undertook a comprehensive review of all files and documents that may have been involved in this incident. On or around **November 19, 2024**, GEMCO ascertained the full scope of personal information that may have been involved in this incident. Through its investigation, GEMCO learned the compromised data included Social Security numbers of **seven (7)** Maryland residents. GEMCO will be mailing letters notifying individuals about this incident on or around **December 3, 2024**.

GEMCO notified the Federal Bureau of Investigation (FBI) on or around June 10, 2024, via an Internet Crime Complaint Center (IC3) notification.

GEMCO does not believe the unauthorized party targeted personal information or intended to harm individuals. Instead, the evidence suggests the unauthorized party was motivated to target GEMCO and its company information, as is common with these types of incidents. Nonetheless, GEMCO is notifying individuals out of an abundance of caution because GEMCO's IT systems held certain personal information.

Since the incident, GEMCO has implemented additional security measures to ensure this type of incident does not reoccur. This includes implementing enhanced endpoint detection and

remediation tools, changing internal protocols, and updating its security policies. It is GEMCO's priority to continue to evaluate and deploy the level of robust security protocols, continuous monitoring, and staff training needed to prevent and defend against future threats.

Enclosed with this letter is a template notification letter sent to the Maryland residents. Please direct any questions or requests for additional information to me.

Sincerely,

ICE MILLER LLP

/s/ Sid Bose

Sid Bose
Partner

Enclosure: Template Notification


GEMCO
GEMCO Constructors, LLC
6525 Guion Road
Indianapolis, IN 46268

<<First Name>> <<Last Name>>
<<Address 1 >>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

December 3, 2024

<<Variable Data 2: Notice of Data Breach/blank>>

Dear <<First Name>> <<Last Name>>:

At GEMCO Constructors, LLC (“GEMCO,” “we,” or “us”) we take privacy seriously. For this reason, we are writing to let you know about an event that may affect the privacy of some of your personal information. Although we have no reason to believe that you are at any risk of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On June 5, 2024, GEMCO was alerted to anomalous activity on its networks. Promptly thereafter, we initiated a response to the alert, and began investigating the anomalous activity. We also took protective actions to stop any unauthorized access to our system. We thereafter engaged a leading security and forensics company to conduct an investigation into the matter. We also reported this incident to U.S. federal law enforcement.

What Personal Information Is Involved? GEMCO does not believe the unauthorized party targeted any of your personal information or intended to harm individuals. Instead, the evidence suggests the unauthorized party was motivated to target GEMCO and its company information, as is common with these types of incidents. Nonetheless, we are providing you with this notice out of an abundance of caution because GEMCO’s IT systems held some of your personal information.

The GEMCO company information may have also involved some of your personal information, including full name, and: <<Variable Data 1: PII_Involved>>.

What We Are Doing. We are taking this matter very seriously. Upon detecting unusual activity in our IT systems, we took immediate protective actions to contain the activity. We also retained an industry-leading cybersecurity company, scanned our environment, and implemented additional security measures. It is our priority to continue to evaluate and deploy the level of robust security protocols, continuous monitoring, and staff training needed to prevent and defend against future threats.

We believe that the unauthorized party was targeting GEMCO. Although we have no reason to believe your information has been or will be used or misused for fraudulent purposes, we are providing you with additional information about credit monitoring and other identity theft protection services, at no cost to you.

Services are available through IDX, an identity protection services provider. IDX identity protection services include: <<Membership Offering Length: 12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance

reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised from this incident.

What You Can Do. We take privacy seriously and sincerely regret any inconvenience this incident may have caused you. For more information on credit monitoring and other identity theft protection services, please see the enclosed attachment for a description of the services provided and instructions on how to enroll. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday to Friday 9:00 AM to 9:00 PM Eastern Time. The deadline to enroll is March 3, 2025.

We also encourage you to, as always, remain vigilant and monitor your account statements, financial transactions, and free credit reports for potential fraud and identity theft, and promptly report any concerns. We suggest you regularly review bills, notices, and statements, and promptly report any questionable or suspicious activity.

For More Information. If you have any questions regarding this incident or the services available to you, please call 1-833-903-3648 (excluding major U.S. Holidays) between Monday to Friday 9:00 AM to 9:00 PM Eastern Time.

Sincerely,

GEMCO Constructors, LLC

Recommended Steps 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.

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 1-833-903-3648 to gain additional information about this event and 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.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. 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. You can review your 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.