

GULSHAN MANAGEMENT SERVICES, INC.

<<Return to Kroll>>

<<Return Address>>

<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

We are writing to tell you about a data security incident that Gulshan Management Services, Inc. (“GMS”) has experienced that may have involved some personal information about you. GMS is a business services company, and we are providing this notice on behalf of our customers to explain the circumstances of the incident and provide information about the steps you can take.

What happened?

On the weekend of September 27, 2025, GMS discovered that an unauthorized third party had gained access to its information systems. Subsequent investigation determined this unauthorized access came from a successful phishing attack on September 17, 2025. The third party was able to access servers that hosted personal data and deploy malicious software that encrypted portions of GMS’s network. Working with third-party investigators and cybersecurity experts, GMS took immediate efforts to contain and remediate the incident, and to expel the third party from GMS’s systems. GMS was able to bring its systems back online using known-safe backups.

What information was involved?

The investigation confirmed that the unauthorized third party may have had access to the following types of personal information: names, contact information, social security numbers, and drivers’ license numbers.

What we are doing.

In response to this incident, GMS promptly implemented measures to secure its affected systems and prevent similar occurrences in the future. For instance, GMS reset all access credentials to affected networks and systems, completely rebuilt its compromised systems, installed additional threat-monitoring software, and introduced more stringent access requirements for privileged accounts. GMS has also notified law enforcement and regulatory authorities in relevant jurisdictions.

In addition, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The identity monitoring services being offered by Kroll include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What you can do.

We encourage you to activate the Kroll identity monitoring services. Specifically, visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services. You will need to use the following Membership Number: <<Member ID (S_N)>>. Remember, you have until <<b2b_text_6 (Date)>> to activate your identity monitoring services.

For more information about Kroll and the Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing these services is included with this letter.

In addition, you should remain vigilant and carefully review your financial accounts for any suspicious activity. Among other things, you should consider:

- Changing your passwords and ensuring that two-factor authentication is enabled on all financial accounts. Also, if you detect any unauthorized activity on an account, you should change the password and security questions associated with the account.
- Actively monitoring your credit information, initiating a fraud alert with all three credit bureaus, and placing a freeze on your credit reports.

Finally, please review the “Additional Resources” attachment we have provided with this letter. This describes steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, certain state resources that may be available to you, and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call (844) 574-1257, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. On behalf of GMS, we sincerely regret any concern or inconvenience this matter may cause you and appreciate your understanding.

Sincerely,

Gulshan Management Services, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [https://www.marylandattorneygeneral.gov/](http://www.marylandattorneygeneral.gov/), 1-888-743-0023.

For 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/](http://ag.ny.gov/), and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, <http://www.dos.ny.gov/consumerprotection>, 1-800-697-1220.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.