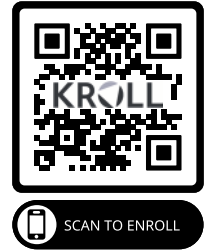


<<Return to Kroll>>  
<<Return Address>>  
<<City, State ZIP>>



<<FIRST\_NAME>> <<MIDDLE\_NAME>> <<LAST\_NAME>> <<SUFFIX>>  
<<ADDRESS\_1>>  
<<ADDRESS\_2>>  
<<CITY>>, <<STATE\_PROVINCE>> <<POSTAL\_CODE>>  
<<COUNTRY>>



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

**Re: Notice of Data Incident**

Dear <<FIRST\_NAME>> <<MIDDLE\_NAME>> <<LAST\_NAME>> <<SUFFIX>>,

We are writing to let you know about a security incident involving certain of your personal information. This notice explains what happened, what information may have been affected, what measures we are taking in response, and steps you can take to protect yourself.

**Who We Are**

Global Consulting Services & Software Development, provides IT consulting, software development, and business intelligence tools to companies around the world including to companies in the financial, bio-tech, and automotive industries. We process and maintain third-party information received via our customers in the normal course of providing our services. We recently discovered that certain personal data had been embedded in third-party information shared with us as a data recipient.

**What Happened**

On January 11, 2026, we were alerted to suspicious activity potentially impacting our network. In response, we launched an investigation and engaged third-party experts to assist. We also took measures to contain and remediate the incident, including quarantining assets, disabling affected accounts, blocking access to our network, and resetting passwords for affected accounts.

Based on our in-depth investigation to date, supported by our external experts, it appears that an unknown third-party gained unauthorized access to a limited set of electronically stored personal information between January 3, 2026 through January 7, 2026. As a result of our detailed analysis of the impacted information, we recently determined, on May 12, 2026, that certain of your personal information was included in the electronic data accessed during the incident. However, our investigation has revealed no evidence to suggest that your data has been fraudulently used.

**What Information Was Involved**

During our investigation we determined that social security numbers had been used to populate an impacted data field that was intended for other non-personal information. As a result, the personal information impacted included your name and social security number.

**What We Are Doing**

As noted above, as soon as we were alerted to the suspicious activity, we launched an internal investigation and engaged the assistance of leading experts. At the same time, we took measures to contain the incident, including quarantining assets, disabling affected accounts, blocking access to our network, and resetting passwords for affected accounts.

We take this matter very seriously, and in addition to the steps already described, GCS is offering you 24 months of free fraud detection and identity theft protection through Kroll. If you wish to take advantage of these services, activation instructions are below.

## What You Can Do

Though we have no evidence that any of your personal information has been fraudulently used, we encourage you to remain vigilant by reviewing your account statements and credit reports closely. At the end of this letter, we have provided you with additional information regarding steps you may want to take to further protect yourself should you determine your circumstances warrant such action. It describes information about (1) reporting suspicious activity or suspected identity theft, (2) credit reports, (3) fraud alerts, (4) credit/security freezes, (5) your rights under the Fair Credit Reporting Act, and (6) information about taxes. We encourage you to review that additional information.

**Free Credit Monitoring and Identity Theft Protection:** Even though we have no evidence that your personal information has been fraudulently used, as a precautionary measure, we are offering to provide you with 24 months of free identity monitoring, fraud consultation, and identity theft restoration services through Kroll. 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. Your free Kroll identity monitoring services include Triple Bureau Credit Monitoring, Fraud Consultation, and Identity Theft Restoration services.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6 (Date)>> to activate your identity monitoring services.

Membership Number: <<Member ID (S\_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com) or review the additional information provided at the end of this letter.

## For More Information

We take the security and privacy of your information very seriously, and deeply regret any inconvenience this may cause. If you have any questions, please call us at (844) 576-3067, toll-free 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.

Sincerely,



Hany M. ELTamami  
Chief Executive Officer



## MORE INFORMATION ABOUT YOUR KROLL IDENTITY MONITORING SERVICES

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

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

### **Additional Steps You Can Take to Protect Your Personal Information**

**Report Suspicious Activity or Suspected Identity Theft.** If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-IDTHEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at [www.ftc.gov](http://www.ftc.gov). You can also contact your state Attorney General (information for some specific AGs is listed below):

- District of Columbia residents may wish to review information provided by the District of Columbia Attorney General on steps to take to avoid identity theft at <https://oag.dc.gov/>, emailing at [consumer.protection@dc.gov](mailto:consumer.protection@dc.gov), calling (202) 442-9828, or by writing to Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001.
- Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us>, by sending an email to [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us), or by calling 410-576-6491.
- New York residents may wish to review information on security breach response and identity theft prevention and protection information provided by the New York Attorney General at <https://ag.ny.gov/internet/privacy-and-identity-theft> or by calling 1-800-771-7755 and by the New York Department of State, Division of Consumer Protection at <https://dos.ny.gov>, or by calling 800-697-1220.
- North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/>, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, NC 27699.
- Rhode Island resident may wish to review information provided by the Rhode Island Attorney General at <http://www.riag.ri.gov> or by calling 401-274-4400, or by writing to 150 South Main Street, Providence, RI 02903.

**Contacting the Internal Revenue Service:** If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate. For the IRS, you can use Form 14039 <https://www.irs.gov/pub/irs-pdf/f14039.pdf>. You can also call them at 800-908-4490 (Identity Theft Hotline). Information on how to contact your state department of revenue to make similar reporting may be found by going to <http://www.taxadmin.org/state-tax-agencies>.

**IRS Identity Protection PIN:** The IRS offers an Identity Protection PIN, which is a six digit number that prevents someone else from filing a tax return using your Social Security number. The Identity Protection PIN is known only to you and the IRS. For more information and to obtain an Identity Protection PIN, please visit the IRS website at <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

**Credit Reports/Fraud Alerts/Credit and Security Freezes:** Under federal law, you are entitled to one free copy of your credit report every 12 months. You can request a free credit report once a year at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling (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. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. 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 apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. There may be a fee for this service based on state law (in MA, there shall be no charge). To put a security freeze on your credit file contact the consumer reporting agencies listed below.

You may contact the three U.S. credit reporting agencies as follows:

Agency	Credit Report Contact	Fraud Alert Contact	Credit/Security Freeze Contact
TransUnion LLC	TransUnion LLC Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016; (800) 888-4213; <a href="https://www.transunion.com">https://www.transunion.com</a>	TransUnion Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19016; (800) 680-7289; <a href="https://www.transunion.com/fraud-victim-resource/placefraud-alert">https://www.transunion.com/fraud-victim-resource/placefraud-alert</a>	P.O. Box 160, Woodlyn, PA 19094; (888) 909-8872; <a href="https://www.transunion.com/credit-freeze/">https://www.transunion.com/credit-freeze/</a>
Experian	P.O. Box 2002, Allen, TX 75013; (888) 397-3742; <a href="https://www.experian.com/consumer-products/freecredit-report.html">https://www.experian.com/consumer-products/freecredit-report.html</a>	Experian, P.O. Box 9554, Allen, TX 75013; (888) 397-3742; <a href="https://www.experian.com/fraud/center.html">https://www.experian.com/fraud/center.html</a>	P.O. Box 9554, Allen, TX 75013; (888) 397-3742; <a href="https://www.experian.com/freeze/center.html">https://www.experian.com/freeze/center.html</a>
Equifax Information Services LLC	Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374; (866) 349-5191; <a href="https://www.equifax.com/personal/credit-reportservices/">https://www.equifax.com/personal/credit-reportservices/</a>	Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348-5069; (800) 525-6285; <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	Equifax Information Services LLC, P.O. Box 105788, Atlanta, GA 30348-5788; (888) 298-0045 or (800) 349-9960; <a href="https://www.equifax.com/personal/credit-reportservices/">https://www.equifax.com/personal/credit-reportservices/</a>

**Federal Fair Credit Reporting Act rights:** You have rights under the federal Fair Credit Reporting Act that include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. More information about your rights is at [www.ftc.gov](http://www.ftc.gov).