GlobalLogic Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

GlobalLogic
A Hitachi Group Company

[redacted]

November 6, 2025

NOTICE OF DATA SECURITY INCIDENT

Dear [redacted]

We are writing to inform you of a recent data security incident involving a third party vendor that we believe may affect your personal information. We take the security of your information very seriously. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information, including enrolling in the complimentary credit monitoring services we are offering you, should you choose to do so.

What Happened?
Oracle issued a security advisory on October 4, 2025, about a previously unknown zero-day exploit. GlobalLogic uses Oracle E-Business Suite, a collection of applications, to manage core business functions such as finance, HR, accounts payable and receivable. As soon as we learned of the vulnerability, GlobalLogic immediately investigated and determined that it had been exploited within our instance of Oracle. Once we made this determination, we activated our incident response procedures, engaged leading third-party cybersecurity experts to assist in a comprehensive investigation, and notified law enforcement. We also promptly applied software patches upon their release from Oracle to address the vulnerability. GlobalLogic's investigation identified access to Oracle and exfiltration on October 9, 2025. We then began drafting and sending out notifications. The investigation has identified the earliest date of threat actor activity as July 10, 2025, with the most recent activity occurring on August 20, 2025.

This incident did not target or impact GlobalLogic's systems outside our Oracle platform, and, based on industry reports, we are one of many Oracle customers believed to have been impacted.

What Information was Involved?
The personal information involved in this incident was from our Oracle platform, which includes HR information for current and former personnel. That information includes personal information collected as part of Human Resources, and could involve the following information of yours: name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, internal GlobalLogic employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number.

What We Are Doing.
In response to the incident, GlobalLogic promptly applied software patches upon their release from Oracle to its customers to address the vulnerability. As noted above, third party forensic experts were retained to investigate further. In addition, GlobalLogic reported this incident to law enforcement. This notice has not been delayed by law enforcement. This incident resulted from a zero-day vulnerability in our vendor's software and we have taken all of the vendor's recommended steps and also taken additional steps to enhance our security.

What You Can Do
We recommend that you review the "Additional Important Information" section enclosed, which contains important steps you can take to protect your personal information. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

Additionally, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How You Enroll In the Free Services
To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. For you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information
Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-833-655-0132 and supply the fraud specialist with your unique code listed above.

We appreciate your patience and understanding, and we deeply regret any inconvenience or concern the incident may cause you.

Sincerely,

GlobalLogic Inc.

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your 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 at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013-9544	Woodlyn, PA 19094
www.equifax.com/personal/credit-report-services/credit-freeze/	http://www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
1-866-478-0027	1-888-397-3742	1-800-916-8800

For residents of *Iowa* and *Oregon*: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These 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. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

Massachusetts and Rhode Island residents: You have the right to obtain or file a police report.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft. There were 17 Rhode Island residents notified in this incident.

District of Columbia Attorney General
400 6th Street NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

New York Attorney General
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

Rhode Island Attorney General
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov