<<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>>

SCAN TO ENROLL

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

<<b2b_text_1 (Notice of Data Breach (CA only)) >>

Dear <<First_name>>,

We are writing to inform you that the Public Relations Society of America ("PRSA" or "we") experienced a recent data security incident that potentially involved your personal information ("Information"). This letter provides you with information about this Incident, our response, and information on where to direct your questions.

What Happened?

In September 2025, we became aware of a security incident that affected our computer systems (the "Incident"). Out of an abundance of caution, we immediately began an investigation and took steps to contain and remediate any activity in our systems that could be related to this Incident, including immediately isolating the potentially impacted systems, changing relevant passwords, notifying federal law enforcement, and engaging data security and privacy professionals to assist with our response. Our investigation determined that an unauthorized actor gained access to our server environment and copied a limited amount of data. Our investigation discovered that your Information was potentially included in the impacted data, but we are unaware of any financial fraud or identity theft associated with this Incident.

What Information Was Involved?

Our investigation recently determined that the following types of Information may have been impacted as a result of this Incident: <<b2b_text_2 (name Data Elements)>>. Our investigation did not identify evidence that your Information was misused for financial fraud or identity theft, but we are taking the steps below out of an abundance of caution.

What We Are Doing.

We take this Incident and the security of your Information in our care seriously. Upon identifying this Incident, we promptly began an investigation and worked with leading data security professionals to aid in our investigation and response, conducted a data review to determine the scope of Information potentially impacted by the Incident, and reported the matter to federal law enforcement and appropriate regulatory authorities.

What Can You Do?

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

There are simple steps experts encourage for protecting your Information, including changing your passwords regularly, monitoring your personal accounts closely, reporting suspicious activity, and never sharing your personal information with unknown or untrusted sources. Additionally, it is always recommended that you remain vigilant, regularly monitor free credit reports, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have any additional questions, you may call us at (844) 443-1769 from Monday through Friday from 9:00 am to 6:30 pm Eastern Time (excluding U.S. holidays).

Sincerely,

Public Relations Society of America

Public Relations Society of America

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com/personal/credit-report-services, 1-800-685-1111

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

TransUnion, PO Box 2000, Chester, PA 19016, https://www.transunion.com/data-breach-help, 1-833-799-5355

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) 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.

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) 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 them 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 five years; and (5) any applicable incident report or complaint with a law enforcement agency or Department 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.

FTC 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 FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid 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).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For 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, 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

For Connecticut Residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, www.ct.gov/ag, 1-860-808-5318.

For District of Columbia Residents: You can obtain information about steps to take to avoid identity theft from the FTC (contact information above) and the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, https://oag.dc.gov/, 1-202-737-3400.

For Massachusetts Residents: You may obtain one (1) 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). You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.