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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Schrader-Pacific ("Schrader") writes to notify you of a data security incident that may have impacted you. This letter is to inform you about the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On or about October 24, 2022, Schrader became aware that it was the victim of a data incident. Immediately, Schrader's management, IT, and leading third-party cybersecurity experts were engaged to investigate the incident, secure personal information, and protect Schrader's network from compromise. Law enforcement was notified, and we commenced an investigation to determine the nature and scope of the incident.

To date, our investigation has revealed that sometime between October 6 and 24, 2022 threat actors gained access to Schrader's IT environment. The threat actors were able to acquire a limited set of data from Schrader's network before being detected. Despite the fact that the threat actors acquired a limited set of data, we are informing all Schrader employees out of an abundance of caution. We want you to know that Schrader has further fortified its network defenses to prevent future attacks of this nature.

Possible Information That Was Involved? It is possible that your full name or first initial and last name combined with your Social Security number, date of birth, passport number or financial account information may have been seen or accessed. This information is called your personal information. It tells others about you and is a part of your identity.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Law enforcement was notified, and we commenced an investigation to determine the nature and scope of the incident. While investigation remains ongoing, we are taking steps now to implement additional safeguards and review policies and procedures relating to data privacy and security.

Schrader has implemented additional security measures designed to further protect the privacy of our employees, residents and vendors. Among other steps taken, we have engaged a leading strategic service provider to monitor our cybersecurity systems, reviewed our system's architecture, and implemented stronger policies to prevent future attacks.

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 two years. 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 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.

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. We also encourage you to review the "Steps You Can Take to Help Protect Your Information" pages enclosed herein.

For More Information. We understand that you may have some questions about this incident that are not addressed in this letter. Should you have additional questions, please contact (855) 504-4517, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major US holidays. Please have your membership number ready.

We apologize for any inconvenience that may have arisen as a result of this incident. In the meantime, we ask for your understanding and patience.

Sincerely,

Kersi Dordi
General Manager

Steps You Can Take to Help Protect Your Information

Check Your Accounts

We urge you to stay alert for incidents of identity theft and fraud, review your account statements, and check your credit reports for shady activity. Under U.S. law, you are eligible for one free credit report each year from each of the three major credit reporting bureaus. To order your free credit report, visit annualcreditreport.com or call toll-free 877-322-8228. You may also reach out to the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a security freeze on your credit report. The security freeze will stop a consumer reporting agency from giving out personal or financial information in your credit report without your consent. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Note: using a security freeze to take control over who gets access to your credit report may delay or prevent any new loan, credit, mortgage, or any other credit extension request or application you make from being approved timely. Under federal law, you cannot be charged to place or lift a security freeze on your credit report. If you wish to place a security freeze on your credit report, please reach out to these major consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/freeze/center

TransUnion
P.O. Box 160
Woodlyn, PA 19094
888-909-8872
transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
800-685-1111
equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide these items:

1. Your full name with middle initial and suffix (Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. The addresses where you have lived over the last five years, if you have moved
5. Proof of current address, such as a current utility bill or telephone bill
6. A clear photocopy of a government-issued identification card (state driver's license or ID card, military ID, etc.)
7. If you are a victim of identity theft, show a copy of either the police or investigative report or complaint to a law enforcement agency about identity theft

Instead of a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Businesses are required to take steps to verify a consumer's identity before extending new credit once they see a fraud alert on a credit file. If you are a victim of identity theft, you are eligible for an extended fraud alert. This is a fraud alert lasting seven years. If you wish to place a fraud alert, please reach out to any one of these agencies:

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/fraud

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
888-766-0008
equifax.com/personal/credit-report-services

More Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by reaching out to:

- The consumer reporting agencies.
- The Federal Trade Commission at: 600 Pennsylvania Ave. NW, Washington, DC 20580, identitytheft.gov, 877-ID-THEFT (877-438-4338); TTY: 866-653-4261.
  - The FTC also urges those who learn their information has been misused to file a complaint with them. Reach out to the FTC for steps to file such a complaint.
- Your state Attorney General.

You have the right to file a police report if identity theft or fraud ever happen to you. Note: to file a report with law enforcement for identity theft, you will need to give some proof you have been a victim. Also, you must report cases of known or presumed identity theft to law enforcement and your state Attorney General.

Also, under the Fair Credit Reporting Act:

- The consumer reporting agencies must correct or delete wrong, lacking, or unverifiable information.
- The consumer reporting agencies may not report outdated bad information.
- Access to your file is limited.
- You must give your consent for credit reports to be given to employers.
- You may limit "prescreened" credit and insurance offers you get based on information in your credit report.
- You may seek damages from a violator.

You may have more rights under the Act not reviewed here. Identity theft victims and active duty military personnel have more specific rights under to the Act. You can review your rights under the Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

KROLL

TAKE ADVANTAGE OF YOUR 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.

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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.