January 12, 2025

NOTICE OF DATA BREACH

Dear Customer,

We are writing to inform you of a security incident that may have affected your information in a data base stored in our servers in a third party location. While we have no evidence of misuse to this date, we are notifying you as a precaution and to help you take protective measures.

What Happened?
On December 9th, 2024 we were informed of unauthorized access to servers operated by our third-party provider Epic. An intruder installed malware, gaining access to our customer information data between December 8 and December 9, 2024.

What Information Was Involved?
The accessed data may include your first and last name, address, phone number, email and social security number or any other personal information we may have from you, excluding bank and credit /debit card information.

What Are We Doing?
We have taken immediate action with cybersecurity experts to remove the malware and secure the security of our servers. Our company has been cooperating with federal and state authorities to investigate the incident.

What Can You Do?
We recommend you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You should report any suspicious activity to your financial institution or the appropriate service provider. Also me recommend to learn more about identity theft at www.privacy.ca.gov.

Want to contact us?
Please be assured that we are committed to helping you protect your information and identity and ensuring that your information is safe and secure. We regret this incident and apologize for any concern it may have caused you.

If you have further questions in regard to this matter, please do not hesitate to contact us at service@arydsslife.com

Sincerely,
ArdyssLife

Steps to Take Following a Data Breach

If you have been notified of a data breach that may have compromised your personal information, it is crucial to take immediate action to protect yourself from potential fraud or identity theft. Below are specific recommendations, along with contact information for relevant institutions:

1. Contact Your Bank or Card Issuer

- **Recommended Actions:**
  - Inform your bank or card issuer about the possible exposure of your information.
  - Request a replacement card if necessary.
  - Inquire about fraud monitoring services or suspicious activity alerts.
- **Contact Information:**
  - Use the customer service number located on the back of your card or visit your nearest branch.

2. Review Your Account Statements and Report Any Suspicious Activity

- **Recommended Actions:**
  - Check your recent transactions for unauthorized activity.
  - Immediately report any suspicious charges to your bank or card issuer.
- **Contact Information:**
  - Contact your financial institution's customer service for assistance.

3. Monitor Your Credit Report

- **Recommended Actions:**
  - Obtain a free copy of your credit report from the major credit reporting agencies:
    - **Equifax:** www.equifax.com/personal/credit-report-services/
    - **Experian:** www.experian.com/consumer-products/free-credit-report.html
    - **TransUnion:** www.transunion.com/credit-reports
  - Consider placing a **fraud alert** on your credit file to ensure lenders verify your identity before issuing credit in your name.
- **Contact Information:**
  - **Equifax:** (800) 685-1111
  - **Experian:** (888) 397-3742
  - **TransUnion:** (800) 916-8800

4. Consider a Credit Freeze

- **Recommended Actions:**
  - A **credit freeze** prevents unauthorized access to your credit file, reducing the risk of fraudulent accounts being opened in your name.
  - Credit freezes can be requested for free through the credit bureaus mentioned above.

- **Contact Information:**
  - Visit the websites of Equifax, Experian, and TransUnion to initiate a credit freeze.

5. Be Cautious of Suspicious Emails and Calls

- **Recommended Actions:**
  - Do not provide personal information to unknown callers or unverified sources.
  - Avoid clicking on links in suspicious emails that may attempt to steal your data (phishing scams).
- **Additional Information:**
  - Always verify the authenticity of any request for personal information before responding.

6. Review Official Resources on Identity Theft

- **Recommended Actions:**
  - Visit the Federal Trade Commission (FTC) website for guidance on identity theft prevention and reporting: www.identitytheft.gov
  - Review resources provided by the California Office of Privacy Protection: www.privacy.ca.gov
- **Contact Information:**
  - **FTC:** (877) 438-4338 (Press 2 for Spanish)
  - **California Office of Privacy Protection:** (916) 445-1254

By following these steps and utilizing the resources provided, you can mitigate the risk of fraud and better safeguard your financial and personal information. If you have any questions or require further assistance, please contact the relevant institutions listed above.