1624 S Mojave Rd., Suite 110
Las Vegas, Nevada, 89104.
(702) 313 3333

March 10,2025

Anthohy G Brown
Maryland State Attorney General
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Subject: **Security Breach Notification**

I am writing to notify you of a data breach that has occurred involving personal information of individuals residing in Maryland. As required by The Personal Information Protection Act (PIPA) of Maryland, we are informing your office of this breach and providing the details outlined below.

1. Description of the Breach:

On December 7th, 2024, at 3:50 pm CST, distributors from The Reshaping and Nutritional Company LLC DBA Ardyss Life (the company), reported that they were unable to log into their Back Office (Website Company System Design to be used by Distributors to make orders and invoices). Once our IT Department verified the claims it was concluded that our server was down of service.

On December 8th, 2024, at 1:26pm CST, the server hosting third party provider (EPIC) notified to company that bandwidth consumption of server was excessive and recommended a bandwidth increase to improve the functionality and access of our distributors to the Back Office. Epic at 3:02 pm CST temporarily doubled the bandwidth from 10 Mbps to 20 Mbps to avoid disconnections.

Later on the day, at 5:07pm CST, EPIC returned the bandwidth to 10 Mbps because they noticed that there was an IP 91.227.77.32 located on Bulgaria (Country) that was consuming all the bandwidth using TCP port 56777, and it was fixed by blocking the connection to that destination using the server firewall.

1624 S Mojave Rd., Suite 110
Las Vegas, Nevada, 89104.
(702) 313 3333

On December 9th, 2024, the IT Department and Employees of our company tried to operate the system in our server, and it was not accessible, and reach EPIC to resolve the issue at 9:55 am CST. EPIC at 9:57 am CST, started a checkup on the server. After EPIC finalized the screening of the server found a trojan virus through the analysis of the antivirus tool of the manufacturer named Symantec and after running the analysis once again, the tool found no more threats and proposed to put our servers under the protection of new management firewall (11:55am CST).

Later that day, at 8:41 pm CST, EPIC reported to company that our server had been under attacked and detected a connection from the IP 77.72.85.166 using an application for file extraction via SFTP. After that, at 8:51 pm CST, EPIC received authorization from the company to place the servers under the protection of their Cisco firewall. Epic successfully completed the configuration of their firewall at 10:26 pm CST.

On December 10 th, 2024, at 7:11 a.m. CST, the company notifies EPIC that wa unable to access databases and operate system. After the report, EPIC begins checking the server. Aproximadly 20 minutes later EPIC confirmed that control had been loss over the information and the databases. Also let us known there was the following message: EMAIL US AT 0mid16b@protonmail.com, READ THE NOTE WE LEFT ON YOUR SERVER, THIS SERVER HAS BEEN HACKED BY 0MID16B, YOU HAVE 72 HOURS TO REPLY US BEFORE WE PUBLISH ALL DATA.

At 9:39 pm CST of December 10 th, 2024, EPIC provided the company the access credentials to new servers to migrate our data and applications.

On December 12, 2024 EPIC provided access to new servers and migrated our data and applications to the new server. Later that day, the company resumed operations with new infrastructure (new servers, IP addresses, passwords etc.) and an audit service was contracted for evaluation with AXTEL and service provider Security Metrics is making a forensic investigation.

2. Types of Information Involved:

The breach involved the following types of personal information:

1624 S Mojave Rd., Suite 110
Las Vegas, Nevada, 89104.
(702) 313 3333

- Name
- Address
- Social Security Number (SSN)
- Individual Taxpayer Identification Number (ITIN)

3. Number of Affected Individuals:

We have determined that 14,478 residents of Maryland State were impacted by this breach. The total amount of affected is 307,000.

4. Company Information.

- **Name:** The Reshaping and Nutritional Company LLC DBA Ardyss Life.
- **Address:** 1624 S Mojave Rd., Suite 110, Las Vegas, Nevada, 89104.
- **Type of Organization:** Retail
- **Contact Name:** Roberto Valencia
- **Phone Number:** (702) 204 9762
- **Email Address:** roberto.valencia@ardysslife.com

5. Actions Taken to Address the Breach:

Upon discovering the breach, we immediately took the following actions:

- Secure the affected systems.
- Conduct a forensic investigation (which remains open).
- Change of the equipment (servers).
- Install Firewalls to our servers.
- Delete Information from our clients.
- Updated the Written Information Security Plan (WISP).
- Revised Policy and Procedures.
- We have also notified affected individuals.
- Work with the Enforcement Agencies.

6. Notice to Affected Individuals.

1624 S Mojave Rd., Suite 110
Las Vegas, Nevada, 89104.
(702) 313 3333

- On January 12, 2025 the company posted in their website the Notice and the document as shown in **Exhibit 1**, this document can be consultable at https://welcome.ardysslife.com/recursos/NOTICE_OF_DATA_BREACH.pdf
- On January 12, 2025 the company posted in their back office (Website Company System Design to be used by Distributors to make orders and invoices) the notice of breach also.
- On February 18, 2024 we notified the affected individuals by email of the events and provided instructions for how they can protect themselves from identity theft and guidence as shown in **Exhibit 1**.
- On march 6, 2025 the company send a message to the telephone numbers with a link to read the document shown in **Exhibit 1**.

7. Notice to Law Enforcement Agencies.

- On 12/26/24 a report of data breach was submitted to the FBI (Federal Bureau of Investigation). The agent supervising the case is Kyle McKnight with email KMMCKNIGHT@fbi.gov
- The company is still submitting the notices of data breach that must file depending on state regulations.

8. Contact Information for Further Inquiries:

If you require further information or have any questions regarding this incident, please feel free to contact Roberto Valencia at (702) 204 9762 or roberto.valencia@ardysslife.com

We take the protection of personal information very seriously and are working diligently to prevent such incidents from occurring in the future.

Thank you for your attention to this matter.

Sincerely,

Roberto Valencia
The Reshaping and Nutritional Company LLC

1624 S Mojave Rd., Suite 110
Las Vegas, Nevada, 89104.
(702) 313 3333

EXHIBIT 1

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.