CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST KOSCHINEG
ekoschineg@c-wlaw.com

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

May 20, 2022

<u>Via Electronic Mail</u>
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
IDTheft@oag.state.md.us

RE: Security Incident Notification

To Whom It May Concern:

We serve as counsel for Skyline House Unit Owners Association ("Skyline") located at 3711 S. George Mason Dr., Falls Church, VA. 22041 and provide this notification to you of a recent incident. By providing this notice, Skyline does not waive any rights or defenses under Maryland law, including the data breach notification statute.

As part of the process for applying for an organizational tax credit through a third-party vendor, certain documentation regarding Skyline employees was provided for consideration. At the time this information was provided, it was believed that any sensitive information had been redacted from the files prior to submission. On February 3, 2022, Skyline made the decision to no longer move forward with the third-party vendor. Following this decision, it was discovered that sensitive information was inadvertently included within certain documents submitted with Skyline's application. Upon discovery, we requested the vendor delete any and all information provided as part of the application and on February 14, 2022, we received confirmation of the deletion. While Skyline has received confirmation of deletion of the sensitive information, Skyline is providing notification to affected employees in an abundance of caution. Skyline has discovered that the unredacted information included information related to three (3) residents of Maryland. The information at risk includes the individuals' name and Social Security number. It is important to note that the Social Security number was listed as an "Identification Number" with no indication that the number was an SSN

On May 20, 2022, Skyline will be mailing written notice of this incident to the Maryland residents pursuant to Maryland law in an abundance of caution. The notice letter includes an offer of complimentary credit monitoring and identity protection services offered through IDX for 12 months. A copy of the notice letter is attached hereto.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: E Koschineg
Ernest Koschineg, Esq.

SHUOA
Skyline House
Unit Owners Association
3711 S. George Mason Dr.
Falls Church, VA. 22041

To Enroll, Please Call: **1-800-939-4170**
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: **«CM_Code»**

May 12, 2022

«AddressBlock»

«GreetingLine»

We are writing to inform you of an incident experienced by Skyline House Unit Owners Association ("Sykline") that may have involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, this letter includes information about the incident and steps you can take to help protect your information.

What Happened: As part of the process for applying for an organizational tax credit through a third-party vendor, certain documentation regarding Skyline employees was provided for consideration. At the time this information was provided, it was believed that any sensitive information had been redacted from the files prior to submission. On February 3, 2022 Skyline made the decision to no longer move forward with the third-party vendor. Following this decision, it was discovered that sensitive information was inadvertently included within certain documents submitted with Skyline's application. Upon discovery, we requested the vendor delete any and all information provided as part of the application and on February 14, 2022, we received confirmation of the deletion.

What Information Was Involved: The documents provided as part of the application included certain files related to vision and dental benefit billings. While many of these files were redacted, we discovered that your name and Social Security number was included and not redacted within one or more of the submitted documents. It is important to note that your Social Security number was listed as an "Identification Number" with no indication that the number was an SSN. Further, as mentioned above, we received confirmation that the provided data has since been deleted.

What We Are Doing: We have taken the steps necessary to address the disclosure and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this disclosure, we immediately took the steps described above, including confirming deletion of the relevant data. While we have no reason to believe any information has been or will be misused, and we received confirmation that the information has been deleted, we are providing you with this notification and are offering you complimentary credit monitoring and identity protection services.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information: Should you have any questions or comments, please contact us at barry@shuoa.org. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

Barry T. Bauman

Barry T. Bauman
General Manager

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

Activate Identity Monitoring Services

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is October 1, 2022.
2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. Telephone. Contact IDX at **1-800-939-4170** to speak with knowledgeable representatives for enrollment should you not have access to online enrollment.
4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Available Services:

SINGLE BUREAU CREDIT MONITORING (adults*) - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCANTM - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Skyline House Unit Owners Association may be contacted at 3711 S. George Mason Dr., Falls Church, VA. 22041