



PROCOPIO
525 B Street
Suite 2200
San Diego, CA 92101
T. 619.238.1900
F. 619.235.0398

ELAINE F. HARWELL
P. 619.906.5780
elaine.harwell@procopio.com

DEL MAR HEIGHTS
LAS VEGAS
ORANGE COUNTY
SAN DIEGO
SCOTTSDALE
SILICON VALLEY
WASHINGTON, D.C.

February 8, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Maryland Attorney General
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Security Incident

Dear Attorney General Brown:

This office serves as counsel to Sun Taiyang Co. Ltd. Pursuant to Md. Code Ann., Com. Law §14-3504, I am writing on behalf of Sun Taiyang Co. Ltd. to inform you of a breach of security to its information systems that involved personal information of one or more residents of Maryland and to provide you with information about the incident that is known at this time.

On or about June 14, 2023, Sun Taiyang Co. Ltd. detected unauthorized access to its network as a result of a cybersecurity incident (ransomware attack) that resulted in the exposure of the data maintained on behalf of clients. Upon learning of the incident, Sun Taiyang Co. Ltd. immediately took steps to secure its network and mitigate against any additional harm. It promptly launched an investigation assisted by outside cybersecurity experts to determine whether any sensitive data had been compromised as a result of the incident. After extensive efforts to obtain, review, and analyze the impacted data, on December 26, 2023, Sun Taiyang Co. Ltd. determined that the impacted files contained identifiable personal information pertaining to [fifty-seven (57) residents of Maryland.

In response to this incident and through its continuing comprehensive review, Sun Taiyang Co. Ltd. has strengthened its network and implemented additional security improvements recommended by third-party cyber security experts. Sun Taiyang Co. Ltd. is also continually evaluating and modifying its practices and internal controls to enhance the security and privacy of the personal information it maintains.



The impacted files contained some or all of the following personal information: first name, last name, Social Security number, driver's license number, tax payer identification number, and credit/debit card number or financial account number with passwords or security codes.

Sun Taiyang Co. Ltd. has been working diligently in order to mail the attached notification letter to all affected residents on Friday, February 9, 2024 that will make them aware of the incident and provide them with resources they can use to protect themselves from the possibility of identity theft. To date, Sun Taiyang Co. Ltd. is not aware of any reports of identity fraud or improper use of the residents' personal information as a result of this incident. Nevertheless, out of an abundance of caution, Sun Taiyang Co. Ltd. is also providing all residents with proactive fraud assistance and access to identity theft protection services through IDX, a ZeroFox Company, who specializes in fraud assistance and remediation services. Through IDX, the residents will receive 24 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Sun Taiyang Co. Ltd. is committed to maintaining the confidentiality and privacy of personal information in its possession and will continue to take precautions to safeguard it. If you have any questions about this or anything else, please feel free to contact me at any time.

Very truly yours,

A handwritten signature in black ink, appearing to read "Elaine F. Harwell".

Elaine F. Harwell

EFH



Return Mail Processing
P.O. Box 989728
West Sacramento, CA 95798-9728

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:

[https://\[REDACTED\]](https://[REDACTED])

[REDACTED]

NOTICE OF DATA INCIDENT

Dear [REDACTED],

HL Choice Corporation, d/b/a SUN SCC, provides certain business support services to several companies, including Sun Taiyang Co., Ltd. We are writing to you on behalf of Sun Taiyang Co., Ltd. to inform you about a cybersecurity incident that involved your personal information. We want to provide you with information about the incident, outline the ongoing resources that are available to you, including complimentary identity theft protection and credit monitoring services, and assure you that significant measures to protect your information have been undertaken.

What Happened

On June 14, 2023, we detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the exposure of the data we maintain.

What We Are Doing

Upon learning of the incident, we immediately took steps to secure our network and mitigate against any additional harm. We promptly launched an investigation assisted by outside cybersecurity experts to determine whether any sensitive data had been compromised as a result of the incident. Our investigatory team learned in late July that the unauthorized individual(s) removed certain files from a limited portion of our network in and around April 2023. After several months of extensive efforts to obtain, review, and analyze the impacted data, on or about December 26, 2023, we determined that your records are among those that were accessed without authorization.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved

The impacted files contained some of your personal information including [REDACTED]
[REDACTED].

What You Can Do

To date, we are not aware of any reports of identity fraud or improper use of your personal information as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide resources you can use to protect yourself from the possibility of identity theft. We are providing you with access to Triple Bureau

Credit Monitoring services at no charge through IDX, a company specializing in fraud assistance and remediation services. These services include 2 years of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Finally, we are providing you with proactive fraud assistance through IDX to help with any questions that you might have or in the event that you become a victim of fraud.

This letter also provides information about other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, and obtaining a free credit report. Additionally, you should remain vigilant and regularly monitor your financial account statements and credit reports for fraudulent or irregular activity that you did not initiate or authorize.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please follow the detailed instructions on the following pages. You will need to reference the enrollment code at the top of this letter when enrolling online, so please do not discard this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity. Enrolling in the services will not hurt your credit score.

For More Information

If you have questions, need assistance or additional information, please contact our dedicated and confidential call center at 1-888-██████████ or visit <https://██████████>. The response line is available between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We are committed to maintaining the confidentiality and privacy of personal information in our possession and will continue to take precautions to safeguard it.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of these service offerings.

Sincerely,

SUN SCC

Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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 1-888-[REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 our 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need

to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about fraud alerts and security freezes from the credit bureaus listed above and the Federal Trade Commission.

8. You can obtain additional information about the steps you can take to avoid identity theft from the three Credit Bureaus listed above and the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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, Telephone: 1-800-952-5225.

Iowa Residents: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, <https://www.iowaattorneygeneral.gov/for-consumers>, Telephone: 1-888-777-4590.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Attorney General’s Office, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Washington D.C. Residents: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.