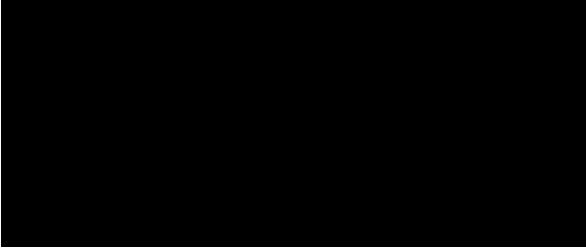


Ocusun, LLC

Legal Department
150 Alameda Del Prado
Novato, CA 94949
Legal@zennioptical.com

Ocusun, LLC
150 Alameda Del Prado
Novato, CA 94949

January 29, 2026



NOTICE OF DATA SECURITY INCIDENT



We are writing to provide you with information about a data security incident involving our Workforce Management System, Rippling, that involved some of your personal information. This letter is being sent to provide you with additional information and to advise you of services Ocusun, LLC (“Ocusun”) is offering at no charge to you. **It is important to note that we have no evidence at this time that your information has been used for any purpose that could cause you any harm as a result of this incident.** Nonetheless, we are sending this letter to tell you what happened, what information was involved, what we have done, and what you can do should you feel it is appropriate to do so.

What Happened?

On January 7, 2026, Ocusun was notified by Rippling that an unauthorized third party obtained access to your personal information on January 7, 2026. We launched an investigation with Rippling and believe that the unauthorized third party may have obtained your login credentials from another source and used them to log into Rippling. While logged into Rippling, the unauthorized third party was able to view information about you.

What Information Was Involved?

The unauthorized third party was able to view your personnel file, which included your first and last name, home address, date of birth, Social Security number, government issued identification numbers, banking and salary information. We have found no evidence that any of this information has been or is likely to be disclosed or misused for fraudulent purposes, or otherwise used in a way that could harm you as a result of this incident.

What We Are Doing.

Upon becoming aware of the unauthorized access, Rippling took steps to block the unauthorized third party from your account. Your account also has been frozen pending password and security changes. Further, we are reviewing Rippling’s policies and procedures to ensure all security measures are taken to

avoid such an incident from occurring again. In this endeavor, Ocusun's IT security team confirmed the unauthorized third party has not, and does not, have any access to any of Ocusun's network.

We are also making resources available to you by offering you two (2) years of Identity Theft coverage from LifeLock. For concerns regarding your coverage, please reach out to Angie Fontana at angie.fontana@zennioptical.com for further information.

What You Can Do.

To help protect your personal information, we strongly recommend that you take the following steps:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and Social Security Number to establish credit and restoration assistance if you are not the one who initiated it.
- Carefully review statements from your bank, credit card company, or other financial institutions, as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached Reference Guide describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please contact our Sr. Corporate Paralegal at julie.demarco@zennioptical.com and Angie Fontana at [Angie Fontana at Angie Fontana at angie.fontana@zennioptical.com](mailto:angie.fontana@zennioptical.com).

Very truly yours,

/s/

Legal Department
Ocusun, LLC

Enclosures

cc: Rebecca Frise

REFERENCE GUIDE

If you suspect you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps:

1. **Fraud Alerts.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus, which are identified below.

2. **Security Freeze.** You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may require that you provide proper identification prior to honoring your request. You can request a security freeze by contacting the credit bureaus, who shall provide a freeze to you free of charge pursuant to 15 U.S.C. § 1681c-1. To request a security freeze, you will need to provide the following identifying information: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) If you have moved in the past five (5) years, the addresses where you have lived over those prior five years; (5) Proof of current address such as a current utility bill or telephone bill; and (6) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. **Free Credit Report.** You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

If you see anything on your credit report that you do not understand, you should notify the credit bureau that sent you the report immediately. If you find any suspicious activity on your credit report, call your local police or sheriff's office, and file a police report for identity theft. You have a right to obtain a copy of the police report, which you may need to provide to creditors to clear up your records.

Equifax P.O. Box 105069 Atlanta, GA 30348 800-525-6285 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022-2000 800-680-7289 www.transunion.com
---	--	---

4. **Massachusetts Residents.** You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

5. **Additional Information.** Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement. A checklist of the steps listed above and links to forms and other helpful information can be found on the site at <https://IdentityTheft.gov/steps>.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.