



Return Mail Processing PO Box 589 Claysburg, PA 16625-0589



N1996-L01-0000001 P001 T00001 ********SCH 5-DIGIT 12345 SAMPLE A SAMPLE - L01 US APT ABC 123 ANY STREET ANYTOWN, ST 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

Maxxis International – USA ("Maxxis," "we," or "our") is writing to inform you about a recent cybersecurity incident that may affect your personal information. Although we are unaware of any actual misuse of your information, we want to provide you with information about the incident, steps we are taking in response, and offer you some resources that you may find helpful to guard against identity theft, should you feel it is appropriate to do so.

What Happened? On October 19, 2024, we detected unusual activity within our computer systems and promptly launched an investigation with the help of independent cybersecurity experts. We determined that an unauthorized third party gained access to our network between October 17 and October 19, 2024. This access occurred after an employee inadvertently clicked on a malicious link, allowing the unauthorized party to access certain systems. Upon discovery, we promptly secured our environment and took action to block further access. We also reported the incident to law enforcement and have cooperated with their ongoing investigation.

What Information Was Involved? Based on our investigation, the unauthorized party may have accessed certain files that included personal information about you, including your [Extra1].

What Are We Doing? We take the security of your personal information seriously. In response to this incident, we engaged cybersecurity professionals to assist with a thorough investigation and have taken extensive steps to strengthen our network defenses. These measures include enhancing system monitoring, expanding multifactor authentication requirements, limiting remote access, and improving controls over internet access. We also added new security tools to detect and respond to threats in real time and hired dedicated cybersecurity resources to lead training efforts and system improvements. We are continuing to evaluate and update our security practices to help prevent something like this from happening again.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.



While identity restoration assistance is <u>immediately available to you</u>, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** July 31, 2025 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1153 by July 31, 2025. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- \$1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-918-1153 toll-free Monday through Friday from 8 am - 8 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

Kellie Carter Human Resources Director Maxxis International - USA

Kellie Carter

ENGAGE# N1996-L01

^{*} Offline members will be eligible to call for additional reports quarterly after enrolling.

^{**} The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR IDENTITY

Placing a Fraud Alert on Your Credit File

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any <u>one</u> of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/ credit-report-services/credit-fraudalerts/ (800) 525-6285

Experian

P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/ center.html (888) 397-3742

TransUnion LLC

P.O. Box 6790 Fullerton, PA 92834-6790 https://www.transunion.com/fraud-alerts (800) 680-7289

Consider Placing a Security Freeze on Your Credit File.

You may also request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/creditfreeze 1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from <u>each</u> of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

0000001



If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you remain vigilant and contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina) or 919-716-6000

ENGAGE#