Seyfarth Shaw LLP
233 South Wacker Drive
Suite 8000
Chicago, Illinois 60606-6448
T (312) 460-5000
F (312) 460-7000

www.seyfarth.com

New Hampshire Office of the Attorney General
Office of Consumer Protection
VIA E-MAIL: DOJ-CPB@doj.nh.gov

January 15, 2024

Re: Notice of Data Incident

Dear Sir or Madam:

We represent Maxxis International - USA ("Maxxis") whose principal business office is located at 545 Old Peachtree Road, Suwanee, Georgia, 30024. We are writing to notify you on behalf of our clients of a data security incident involving 1 New Hampshire resident. This notice may be supplemented upon any further investigation. By providing this notice, Maxxis does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the relevant state statute, or personal jurisdiction.

Background: Maxxis first became aware of the incident on May 29, 2023 when it discovered that multiple servers were encrypted and made inaccessible as a result of a cyber-attack. The event was detected almost immediately, triggering a rapid response from our clients' IT security team to shut down connectivity and isolate impacted systems. Maxxis quickly initiated its incident response protocols and engaged third-party cybersecurity experts to conduct a comprehensive investigation to determine the nature and extent of the incident, including a confirmation that there were no persistent and/or ongoing threats to Maxxis' environment and that the threat actor was only active on Maxxis network for a specific windows of time on May 29, 2023. The forensic analysis was completed on July 31, 2023.

In parallel with the analysis performed by the cybersecurity experts, Maxxis also began identifying and collecting documents that may have been impacted by the security incident between mid-July and mid-August. These documents were then subsequently processed into a review platform in order to identify Personally Identifiable Information ("PII") and/or Protected Health Information ("PHI") within those documents. Utilizing a large team of contract reviewers, the first-level review of documents comprised of both electronic and hard copy documents spanning a variety of file formats, data types, and organizational structures was completed in mid-October. Maxxis also performed multiple rounds of quality control checks and supplemental analysis between mid-October and early December to resolve outstanding issues regarding specific data elements contained within the document population and discrepancies with specific residents' addresses. On December 19, 2023, Maxxis determined that one New Hampshire resident was impacted. To date, Maxxis is not aware of any reports of identity fraud or misuse of the potentially affected information.

To prevent future incidents and enhance Maxxis' cybersecurity posture, Maxxis implemented the following measures:

- Invested in advanced threat detection systems to identify abnormal behavior and potential breaches;
- Implemented a zero-trust security model to ensure only authorized users have access to critical systems and data;
- Established a cross-functional security team responsible for continuous monitoring, incident response, and threat intelligence;
- Collaborated with third-party security experts to conduct regular audits and vulnerability assessments; and
- Regularly update and train employees on cybersecurity best practices and the evolving threat landscape.

To further strengthen its security practices, Maxxis has engaged professional cybersecurity firms SentinelOne DFIR Team and Edge Solutions/CISO Global, and has begun implementing their recommendations to further secure its environment.

Notice to New Hampshire Residents: We have determined that the number of New Hampshire residents potentially affected by this security incident is 1. Written notice is being provided in substantially the same form the letter attached hereto as **Exhibit A**. Maxxis will begin mailing notice to impacted individuals subsequent to the transmittal of this letter, no later than January 12, 2024.

Other Steps Taken and To Be Taken: Maxxis is taking action to provide assistance to potentially affected individuals, even though it currently has no evidence of any misuse of or fraudulent activity relating to anyone's personal information as a result of this incident. Our clients are providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for through Equifax at no cost to the individuals.

Additionally, Maxxis is providing impacted individuals with guidance on how to better protect against identity theft and fraud. These measures include advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Our clients are also providing individuals with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information: Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at .

Very truly yours,

SEYFARTH SHAW LLP

Jay C. Carle

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<First Name>> <<Middle Name>> <<Last Name>>:

Maxxis International – USA ("Maxxis," "we," or "our") is writing to inform you about a recent cybersecurity incident that may affect the security of 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? Maxxis first became aware of the incident on May 29, 2023 when we discovered that multiple servers were encrypted and made inaccessible as a result of a cyber-attack. The event was detected almost immediately, triggering a rapid response from our IT security team to shut down connectivity and isolate impacted systems. We quickly initiated our incident response protocols and engaged third-party cybersecurity experts to conduct a comprehensive investigation to determine the nature and extent of the incident. The forensic analysis was completed on July 31, 2023 and we recently completed a thorough review of the impacted data.

What Information Was Involved? While we are presently not aware of any misuse of personal information, based on our investigation we have determined that the cyber-attacker may have had access to files that contained your <<Breached Elements>>.

What Are We Doing? We take the protection of personal information very seriously and have taken and will continue to take steps prevent a similar occurrence. In addition to taking active steps to bolster our security protocols, we have engaged professional cybersecurity firms Sentinel One and CISO Global, and we have begun implementing their recommendations to further secure our environment.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary two-year membership in Equifax Credit Watch™ Gold. Equifax Credit Watch™ Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax Credit Watch™ Gold including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.

This letter also provides 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 always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am to 9 pm Eastern Time.

Sincerely,

Kellie Carter
Human Resources Director
Maxxis International - USA

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

<<First Name>> <<Middle Name>> <<Last Name>>
Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. 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 one 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-fraud-alerts/
(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

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may 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.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each 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.

5. 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.

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 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.