

Nicholas J. DiCesare
Partner

June 8, 2022

VIA ELECTRONIC MAIL

Brian E. Frosh
Attorney General
Office of the Attorney General
200 St. Paul Place
Baltimore , MD 21202

Re: Wilkins Recreational Vehicles, Inc.: Notice of
Breach of Security

Dear Attorney General Frosh:

We are writing on behalf of our client, Wilkins Recreational Vehicles, Inc. (“Wilkins”), to notify you of a recent breach of security incident involving computerized data that may have affected ninety (90) Maryland residents.

On February 8, 2022, Wilkins became aware of unusual activity on its system, specifically some encryption of files appearing to be the initial stages of a ransomware attack. Wilkins immediately secured its system. A New York based cybersecurity expert, Avalon Cyber (“Avalon”), thereafter conducted a full forensic investigation. The investigation was able to determine that initial unauthorized access to the system occurred on February 2, 2022, and that it was associated with a ransomware attack (of the Conti variant). Wilkins did not interacted with the threat actor in any way, and was not otherwise contacted by the threat actor. Wilkins was able to recover any encrypted data from back-ups. The source of the access appears to be a phishing attack in which a Wilkins employee opened a malware-infected file. Wilkins was not able to locate the specific phishing e-mail, but did locate the infected file. The investigation was unable to determine with any degree of certainty what data may have been accessed by the threat actor, or what, if any, data may have been exfiltrated. Wilkins thereafter identified all individuals who may have had any protected personal information on its system, and notification is being mailed to such individuals on June 8, 2022. A copy of template for notification to individuals is provided herewith.

The potential information at issue includes drivers’ license numbers, Social Security Numbers, and possible credit card account numbers. However, there has been no indication of any Wilkins data being leaked on the dark web, and there has been no indication of any Wilkins data being used to commit identity theft. Nonetheless, Wilkins has offered credit monitoring and

Brian E. Frosh
June 8, 2022
Page 2

fraud prevention services for 1 year through Kroll, and has also established a call center through Kroll to address questions or concerns of any individuals potentially impacted by the incident.

In response to the breach, Wilkins engaged legal counsel to assist with its investigation and response, and worked with Avalon to perform forensic investigation. Avalon performed a full risk assessment of Wilkins' system. Wilkins also conducted a review of its policies and practices, as well as its technological defenses. Additionally, Wilkins conducted further training of its employees to be aware of and identify potentially malicious emails. Wilkins has also added active monitoring of its computer system as further protection against, and means of more quickly identifying, unusual activity.

If you have any questions regarding this submission or require additional information, kindly contact me. Thank you.

Very truly yours,

s/

Nicholas J. DiCesare

NJD



"Serving You For Three Generations Since 1936"

www.wilkinsrv.com

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to tell you about a data security incident at Wilkins RV that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

We recently completed an investigation involving a cyber-attack against Wilkins in which unauthorized criminal actors gained access to some of Wilkins' electronic systems. Upon learning of the attack, Wilkins immediately took steps to secure its systems and began an investigation with the assistance of cybersecurity experts. The investigation determined that Wilkins was the victim of a ransomware attack, in particular a type of ransomware known as Conti. The ransomware attack itself occurred on February 8, 2022. The forensic investigation has determined that criminals first accessed Wilkins' systems on February 2, 2022, most likely through a "phishing" attack in which a Wilkins employee opened a file infected with malware. Wilkins was able to secure its systems shortly after the attack on the 8th, and did not respond to or pay the ransom demanded by the criminals. The forensic investigation, however, was unable to determine if any data was actually taken or what specific data may have been accessible to the criminal actors during the attack.

What information was involved?

Out of an abundance of caution and to proactively address any potential issues, we have identified all individuals for whom Wilkins may have maintained any sort of private information. On May 12, 2022, we determined that Wilkins did have certain of your personal data on its systems that could have been accessible to the criminal actors, in particular your driver's license number and, if you obtained financing through Wilkins RV or exchanged credit card information through e-mail, your Social Security number and financial account numbers.

What we are doing.

Although Wilkins has always taken great care to ensure the protection of its data, we have used this attack as an opportunity to review our information security practices and protections. We have conducted further training of employees to identify potentially malicious emails. We also retained information security experts to review our technological protections and actively monitor our systems for unusual activity.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call (855) 503-3047, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

A handwritten signature in black ink, appearing to be "Brian Wilkins", with a stylized, looped flourish at the end.

Brian Wilkins
President

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.