MAYNARD
COOPER GALE

**Sarah Glover**
DIRECT 205.254.1877
EMAIL sglover@maynardcooper.com

January 29, 2021

RECEIVED
FEB 02 2021
CONSUMER PROTECTION

**Attorney General Gordon McDonald**
Office of Attorney General
33 Capitol Street
Concord, NH 03301

**Re: Security Incident**

Dear Attorney General McDonald,

I am writing to let you know that our client, Wind River Systems, Inc. ("Wind River" or "Company"), experienced a security incident that affected the personal information of some of its current and former employees.

The Company supplied notice to affected individuals in December (current employees) and January (former employees) to let them know what happened, and to inform them of available resources to further monitor and protect their personal information. We are providing notice to your office pursuant to N.H. Rev. Stat. § 359-C:19, *et seq*.

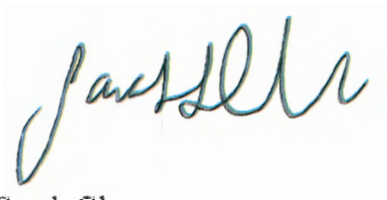
On September 29, 2020, Wind River discovered that it had fallen victim to a ransomware attack after detecting encrypted files on its network. The Company immediately reported the incident to law enforcement. The Company also engaged outside experts through its insurance carrier to conduct an investigation, which concluded this month.

The forensic investigation revealed that the threat actor, identified as Darkside, utilized a suite of sophisticated, modular malware and highly obfuscated PowerShell scripts to access the Company's network and execute malicious programs. These malware tools were used to exfiltrate data and deploy the ransomware. The root cause of the attack could not be identified with available forensic evidence.

A review of the exfiltrated files uncovered the personal information of ninety-seven New Hampshire residents. This information included the individual's name and social security number. One year of complimentary credit monitoring and identity theft protection services were extended to the affected individuals. A copy of the individual notice is enclosed.

Please do not hesitate to let me know if you have any questions or would like additional information.

Sincerely,



Sarah Glover

WNDRVR

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

**Re: Notice of Security Incident**

Dear <<Name 1>>,

I hope this letter finds you well. I am writing to let you know about a security incident at Wind River that unfortunately may have affected your personal information we had on file for you. We are not aware of any actual or attempted misuse of personal information as a result of this event. However, we want to make sure you are aware of the facts surrounding this event so that you can take the appropriate precautions you feel are needed to protect your personal information. We have enclosed information on several identity protection resources.

**What Happened?**

We have been working with law enforcement and outside experts to investigate a security incident that occurred toward the end of September. Our outside experts recently determined that some of your personal information would have been available within one or more files that were downloaded from our network on or about September 29, 2020. We have no indication that any information in these files has been misused. Recent searches by our experts did **not** uncover any of these files online.

**What Information Was Available?**

The type of personal information our experts observed varied, and included information maintained within our personnel records, such as date of birth; social security, social insurance, driver's license, or national identification number; passport or visa number; health information; and/or financial account information.

**What We Are Doing**

We are committed to protecting the information we maintain here at Wind River. We've already installed additional security monitoring tools, implemented new processes, and will continue to focus on improving the cyber-resiliency and security posture of our company.

**What You Can Do**

The enclosed Reference Guide includes information on general steps you can take to monitor and protect your personal information. If you would also like to receive complimentary identity monitoring services, please call the number below to make this request.

We are sorry for any inconvenience this may cause. If you have any questions, please reach out to our dedicated call center at 800-281-3059. The call center is open in North America, Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Standard Time. Internationally, you may reach the call center 24/7 at the one of the following numbers: United Kingdom (03332127246); Outside the United Kingdom (+4433 212 7246).

Sincerely,

Terese Lam
Chief People Officer

## IDENTITY PROTECTION REFERENCE GUIDE (U.S.)

**1. Review your Credit Reports**. We recommend that you remain vigilant by monitoring your credit reports. Under federal law, you 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 from one of the three credit bureaus every four months.

**2. Place Fraud Alerts.** A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. 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. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 740241 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30374-0241 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | 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.

**3. Place Security Freezes.** By placing a security freeze, someone who fraudulently acquires your personally 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 each of the three national credit reporting bureaus listed above in writing to place the freeze. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your Social Security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

**4. Monitor Your Accounts.** We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective financial institution.

**5. You can obtain additional information** about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the Federal Trade Commission ("FTC"). You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

***

**District of Columbia Residents:** You can obtain additional information about preventing identity theft from the FTC Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502, and the Office of the Attorney General for the District of Columbia at: 400 6th St NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

**Iowa Residents**: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

**Maryland Residents**: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, https://www.marylandattorneygeneral.gov/.

**Massachusetts Residents**: You have the right to obtain any police report filed regarding this incident. You also have the right to file and obtain a copy of a police report if you are the victim of identity theft.

**New York Residents:** You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

**North Carolina Residents:** You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

**Oregon Residents:** You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

**Rhode Island Residents**: You have the right to obtain any police report filed regarding this incident. You also have the right to file and obtain a copy of a police report if you are the victim of identity theft. You can obtain additional information about identity theft prevention and protection from the Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov/.

## IDENTITY PROTECTION REFERENCE GUIDE (INTERNATIONAL)

**Review your Credit Profile**. If your country has a publicly available credit bureau, we would recommend that you remain vigilant by monitoring use of your credit profile.

**Monitor Your Financial Accounts.** We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective financial institution.

**Watch For Signs of Identity Theft or Fraud.** Identity thieves may facilitate loans, purchases, or other transactions in your name – be aware of any correspondence you receive about a transaction you did not make, or a past due account or charge you do not recognize.

**Keep Your Devices Secure.** Securely maintain your smart phones, laptops, tablets, and other devices in your possession or safely store them away.

**International Online Resources**

Canada: https://www.canada.ca/en/services/finance/fraud.html

Costa Rica: https://www.bancobcr.com/wps/portal/bcr/bancobcr/soporte/seguridad/

Europe: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/tips-and-advice-to-prevent-identity-theft-happening-to-you

India: http://cyberpolicebangalore.nic.in/dos-and-donts/dnd-families.html

Japan: https://www.j-credit.or.jp/customer/

Singapore: https://www.gov.il/en/Departments/publications/reports/identity_theft_online

Taiwan: https://www.ait.org.tw/zhtw/visas-zh/combating-fraud-zh/victim-online-scam-zh/

United Kingdom: https://ico.org.uk/your-data-matters/identity-theft/