August 18, 2021

VIA UPS OVERNIGHT DELIVERY
Office of the New Hampshire Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

Pursuant to New Hampshire law, I am writing on behalf of SAC Wireless to notify you of a confirmed data breach.

Background of Data Incident

On June 16, 2021, SAC Wireless became aware that certain aspects of our internal technology infrastructure may have been accessed by an unauthorized third-party as part of a ransomware attack. Upon learning of the incident, we promptly deployed multiple security tools and infrastructure enhancements to contain the incident. We then contacted the FBI and engaged external counsel and cyber security experts to better understand the scope of the incident and determine what, if any, personal information was compromised. The forensic investigation was materially completed on August 13, 2021.

While it is unknown how the threat actor, Conti, initially gained access, the investigation did reveal that two .exe files were placed on a SAC server and were subsequently executed by Conti. Conti uploaded files from SAC's network to a cloud server and, on June 16, deployed ransomware to encrypt the files on SAC systems. Conti demanded a ransom payment in exchange for a decryption key to the files. SAC Wireless declined to pay the ransom amount.

We believe that the files affected by this incident could have possibly contained some or all of the following categories of personal information relating to current and former SAC Wireless employees: name, date of birth, contact information (such as home address, email, and phone), government ID numbers (such as driver's license, passport, or military ID), social security number, citizenship status, work information (such as title, salary, and evaluations), medical history, health insurance policy information, license plate numbers, digital signatures, certificates of marriage or birth, tax return information, and dependent/beneficiary names. While this list of personal information has been identified as part of the data set potentially compromised in this incident, it does not mean that each category of personal information listed was compromised for every individual. To the extent that an employee's dependents or beneficiaries were included on an SAC Wireless health plan, their personal information may also have been compromised. Conti has threatened to release the uploaded files on the dark web, but as of the date of this letter, no such release has occurred.

Outreach to New Hampshire Residents

The investigation has identified 3 New Hampshire residents whose unencrypted personal information was compromised by the breach. A notice will be sent to those affected individuals on or about August 19 via mail. A redacted copy of the consumer notice is enclosed below. We also notified the potentially impacted employees via email on June 21, at the very beginning of our investigation, out of an abundance of caution and before any determinations were made as to whether any personal information was accessed or acquired.

SAC Wireless will be offering affected individuals free identity theft and credit monitoring services for 24 months. These services will be provided by Experian.

Steps Taken to Remediate the Breach and to Prevent Future Incidents

SAC Wireless has taken several steps to contain the immediate threat and to reduce the risk of a similar event from occurring in the future, including but not limited to:

- changing firewall rules;
- disconnecting VPN connections;
- activating conditional access geo-location policies to limit non-U.S. access;
- deploying additional network and endpoint monitoring tools;
- providing additional employee training;
- expanding multi-factor authentication; and
- deploying additional threat-hunting and endpoint detection and response tools;

We continue to assess and monitor new threats and security vulnerabilities on an ongoing basis, and we are adding additional security enhancements over the coming months.

About SAC Wireless

SAC works with telecom carriers, major tower owners, and original equipment manufacturers (OEMs) across the United States to offer a complete portfolio of self-performing services to support major network builds, 5G LTE upgrades, and indoor/outdoor small cell and distributed antenna systems (DAS) deployments. Our core business consists of fully integrated network solutions, specializing in site development, architectural and engineering design management, construction services and management, equipment installation, commissioning and integration, operations, and maintenance.

For additional information about this incident, please contact me by telephone at (858) 344-6678; via email at Shawna.Brown@sacw.com; or by mail to 300 Airport Road, Suite A-1, Elgin, IL 60123.

Sincerely,

Shawna Brown, Associate General Counsel
SAC Wireless

Enclosures:

Employee Data Breach Notice

[Enclosure: Employee Data Breach Notice]

<<Date>>

<<first_name>> <<last_name>>
<<address_1>>
<<address_2>>
<<city>>, <<state>> <<ZIP code>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

We are writing to inform you of a data security incident that affected SAC Wireless. As a result of this incident, the security of some of your personal information may have been compromised.

WHAT HAPPENED

On June 16, 2021, SAC Wireless became aware that certain aspects of our internal technology infrastructure may have been accessed by an unauthorized third-party as part of a ransomware attack. Upon learning of the incident, we promptly deployed multiple security tools and infrastructure enhancements to contain the incident. We then contacted the FBI and engaged external counsel and cyber security experts to better understand the scope of the incident and determine what, if any, personal information was compromised. The forensic investigation was materially completed on August 13, 2021. The threat actor, Conti, gained access to the SAC systems, uploaded files to its cloud storage, and then, on June 16, deployed ransomware to encrypt the files on SAC systems.

WHAT INFORMATION WAS INVOLVED

Our internal review of potentially impacted personal information is ongoing, but we believe that the files affected by this incident could have possibly contained some or all of the following categories of personal information relating to current and former SAC Wireless employees: name, date of birth, contact information (such as home address, email, and phone), government ID numbers (such as driver's license, passport, or military ID), social security number, citizenship status, work information (such as title, salary, and evaluations), medical history, health insurance policy information, license plate numbers, digital signatures, certificates of marriage or birth, tax return information, and dependent/beneficiary names. To the extent that one of your dependents or beneficiaries was included on an SAC Wireless health plan, their personal information may also have been compromised. While this list of personal information has been identified as part of the

data set potentially compromised in this incident, it does not mean that each category of personal information listed was compromised for every individual.

WHAT WE ARE DOING

We have been working and will continue to work with our cyber and forensic experts to remedy this incident and to identify potential enhancements to our information security systems. In response to this ransomware attack, we have already changed firewall rules, disconnected VPN connections, activated conditional access geo-location policies to limit non-U.S. access, provided additional employee training, deployed additional network and endpoint monitoring tools, expanded multi-factor authentication, and deployed additional threat-hunting and endpoint detection and response tools. We will deploy additional new measures in the coming months, and we continue to assess and monitor new threats and security vulnerabilities on an ongoing basis.

As part of protecting your online identity and safety, we have engaged Experian to offer you a free 24-month membership to their identity protection services. Please refer to Appendix A for details on the services provided and how you can enroll for free.

WHAT YOU CAN DO

In addition to enrolling for free in Experian's identity protection services (see Appendix A for details), we recommend you take the following precautions:

Security Freeze – You can place a security freeze on your credit report, which may help prevent credit, loans, and services from being approved in your name without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift, or remove a security freeze. To place a security freeze on your credit report, you need to make a request to *each* consumer reporting agency (see contact info below). Depending on the agency, you may be asked to provide some or all of the following information when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. You may also need to 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, display your name and current mailing address, and the date of issue. You may obtain a free security freeze by contacting one or more of the following national credit reporting agencies:

Equifax	Experian	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com

Fraud Alert – You can place a fraud alert on your credit report, which may help prevent someone from opening accounts in your name or changing your existing accounts. You can place a fraud alert by contacting any one of the three national credit reporting agencies: Experian (www.experian.com/fraud/center.html); TransUnion (www.transunion.com/fraud-alerts); or Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf). You may also place a fraud alert by calling the three credit bureaus at the phone numbers listed above. Fraud alerts initially last for one year. Victims of identity theft can get an extended fraud alert for seven years. A fraud alert adds a layer of protection, but it might cause delays or prevent you from getting instant credit (such as an instant credit card offered by a retail store).

Order a free copy of your credit report. You are entitled to receive a free credit report annually, even if you don't suspect any unauthorized activity on your account or credit reports. To order your free credit report, visit www.annualcreditreport.com/, or call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Requests Service, P.O. Box 105281, Atlanta, GA 30348-5281. The FTC recommends that you check your credit reports and credit card statements periodically.

Remain vigilant in reviewing your bank account, credit card, or other financial transaction statements. You should monitor these statements as well as your free credit reports to protect yourself against fraud and identity theft. If you notice anything unusual, contact your financial institution. You may also wish to consider contacting your financial institution now, to discuss options for monitoring your bank account.

Monitor your mail for any disruption in delivery. If you notice any irregularities (such as missing financial statements, credit card statements or other documents), report such irregularities to the US Postal Service.

Contact the U.S. Federal Trade Commission or your state's Attorney General to obtain additional information about how to avoid identity theft. Contact information is below.

Report suspected identity theft to law enforcement, your state's Attorney General, and the U.S. Federal Trade Commission. If you suspect that someone has stolen or misused your personal information or that you are a victim of identity theft, you should immediately report the incident to the U.S. Federal Trade Commission and your local law enforcement (including your state's Attorney General):

- **U.S. Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, or 1-877-IDTHEFT (438-4338), or www.ftc.gov/idtheft.

- **California Office of Privacy Protection,** www.oag.ca.gov/privacy, for additional information on protection against identity theft.
- **Maryland Office of the Attorney General** Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, or 1-888-743-0023, or www.oag.state.md.us.
- **New York Office of Attorney General** Consumer Frauds & Protection, The Capitol, Albany, NY 12224, or 1-800-771-7755, or https://ag.ny.gov/consumer-frauds/identity-theft.
- **North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, or 1-877-566-7226, or www.ncdoj.com.
- **Rhode Island Office of the Attorney General** Consumer Protection, 150 South Main Street, Providence RI 02903, or 1-401-274-4400, or www.riag.ri.gov.
- **Washington, D.C. Office of the Attorney General** for the District of Columbia, 441 4th Street NW, Washington, DC 20001, or 1-202-727-3400, or https://oag.dc.gov/.

File and obtain a police report if you are the victim of identity theft. If you suspect that you are a victim of identity theft, you have the right to file a report with your local police or the police where the identity theft took place, and to obtain a copy of that police report.

Exercise your rights under the Fair Credit Reporting Act, such as the rights the right to know what is in your credit file, to dispute incomplete or inaccurate information, to be told if information in your credit file has been used against you, to limit "prescreened" offers of credit and insurance you get based on information in your credit report, and to ask for your credit score. Pursuant to the Fair Credit Reporting Act, you may seek damages from any violator.

FOR MORE INFORMATION

We understand that this incident may create concern and confusion and that you may have questions. For additional information or assistance, please contact Larry Pomykalski, Director of Fleet and Business Continuity, at Larry.Pomykalski@sacw.com, or call the SAC Wireless hotline at [details inserted by Experian prior to employee notices being sent].

We deeply regret any inconvenience this incident has caused.

Sincerely,

Michael Petrak, Vice President of Human Resources
SAC Wireless

APPENDIX A

INFORMATION ABOUT COMPLIMENTARY EXPERIAN SERVICES

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} 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 immediately available to you, 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 November 1, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [User-specific activation code]

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 [Experian TFN] by **November 1, 2021**. Be prepared to provide engagement number [DB#####] 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.[1]
- **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 ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

---

1 Offline members will be eligible to call for additional reports quarterly after enrolling.

2 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.