BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David B. Sherman
direct dial: 215.564.8380
dsherman@bakerlaw.com

October 13, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, Amphenol Canada Corporation ("ACC"), to provide notice of a security incident involving a resident of New Hampshire.[1]

ACC recently concluded its investigation of an incident that involved unauthorized access to, or exfiltration of, certain files on its computer systems. Upon identifying the incident, ACC immediately took its systems offline, reported the incident to law enforcement, and commenced an investigation. Through its investigation, ACC determined that an unauthorized actor accessed or obtained files from certain ACC computer systems between August 16, 2021, and August 20, 2021.

ACC then reviewed the files to identify individuals whose personal information was included therein. On September 29, 2021, ACC determined that the files may have included the name and passport number of one New Hampshire resident. ACC notified the affected individual via email on September 8, 2021. On October 13, 2021, ACC sent the individual a formal notification letter through U.S. mail. ACC encouraged individuals to remain vigilant by reviewing their credit reports and financial account statements. ACC is also offering complimentary Financial/Dark Web/Social Media account monitoring via Identity Force and established a dedicated, phone number for individuals to call to obtain more information regarding the incident.

[1] This notice is not, and does not constitute, a waiver of ACC's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

To help prevent a similar incident from occurring in the future, ACC enhanced its network security systems, reset all users' login credentials, and implemented multifactor authentication for all VPN users.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

David B. Sherman
Partner

Enclosure

Amphenol Canada Corp.
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

October 13, 2021

Dear <<First Name>> <<Last Name>>,

We recently completed our investigation of a security incident that involved some of your personal information, which was initially addressed in our correspondence to you dated September 8, 2021. This message includes additional information about what happened, measures we have taken, and some steps you may consider taking in response.

On August 20, 2021, we identified a security incident on our computer network. In response, we immediately took our systems offline, reported the incident to law enforcement, and commenced an investigation. We completed our investigation, restored our network, and confirmed that an unauthorized actor accessed or obtained files from certain ACC computer systems between August 16, 2021, and August 20, 2021.

We also completed our review of the files that the unauthorized actor accessed or obtained to identify individuals whose information was included in those files. We determined that one or more files included your name and passport number.

We recommend that you remain vigilant for signs of unauthorized activity by reviewing your financial account statements and credit reports. If you see charges or activity, you did not authorize, we suggest that you immediately contact your financial institution. As an added precaution, we arranged for you to receive complimentary Financial/Dark Web/Social Media account monitoring via Identity Force. Through this service, you will receive regular alerts notifying you of significant changes or abnormal activity within your financial, investment, and social media accounts. This product is free to you and enrolling in this program will not hurt your credit score.

For more information on identity theft prevention, additional steps you can take in response, and instructions on how to activate your Identity Force services if you have not already done so, please see the additional information provided with this letter.

We regret any inconvenience or concern this may cause you. To help prevent a similar incident from occurring in the future, we enhanced our network security systems, reset all users' login credentials, and implemented multifactor authentication for all VPN users.

If you have any questions about this incident, please contact your general manager, or Kathleen Perry via email at kathleenp@amphenolcanada.com or via telephone at 416-654-5710 Monday through Friday, between 8:30 a.m. and 4:30 p.m., Eastern Time.

Sincerely,

Andy Toffelmire
Aerospace GM

Susan Prakash
HSIO GM

Scott Kleinle
ACPA GM

IDENTITY MONITORING INSTRUCTIONS

To sign up for your free year of IdentityForce monitoring, please email amphenol@identityforce.com and provide:

- your full name;
- email address; and
- the following code, depending on your location: **USAMPCAN0921**

Within 48 hours, you will receive a reply providing further detail and enrolment instructions.

In the event that you experience fraud or identity theft issues, such as unauthorized charges on your credit card or a new account being opened using your personal information, you may contact Identity Force's Resolution Centre where a dedicated Fraud Specialist will work with you to assess your risk, make recommendations, call creditors or agencies, and stay with you throughout the entire resolution process. More information is available at www.identityforce.com

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.