NORTON ROSE FULBRIGHT

June 30, 2020

Office of the Attorney General

Attn: Security Breach Notification

33 Capitol Street

Concord, NH 03301

Norton Rose Fulbright Canada LLP
1 Place Ville Marie
Suite 2500
Montréal, Quebec
H3B 1R1 Canada

Julie Himo
Partner
Direct line 514 971 2497
julie.himo@nortonrosefulbright.com

Tel +1 514 847 6017
nortonrosefulbright.com

Re: ***Legal Notice of Information Security Incident***

Dear Sirs or Madams:

We write on behalf of our client, Accedian Networks US Inc. (“**Accedian**”), to notify you of a security incident that resulted in the unauthorized access of the personal information of one New Hampshire resident.

On May 15, 2020, Accedian discovered it was the victim of a ransomware attack. The external threat actor was able to gain access to Accedian’s systems, infecting certain systems with ransomware and exfiltrating data off of certain servers in the system.

Once Accedian became aware it had been subject to a ransomware attack, the system was contained by shutting down all servers and machines. Accedian also immediately put in place an incident response plan and retained forensic experts to contain the incident and determine its scope. Additional containment and responsive measures taken include:

- Password reset and multi-factor authentication for all GSuite users;
- Separating routing from Firewall;
- Building a new Firewall to support Web Filtering;
- Building a green network with additional VLANs;
- Revalidating all internal routes (> 5000 IPs);
- Rebuilding an Active Directory (Windows 2016);
- Changing VPN Protocol and security (2 factor authentication + certificate); and
- Deploying Enterprise wide Antivirus/Malware/End-point security.

During the investigation the forensic experts advised that there was insufficient evidence from the logs to identify all files accessed by the attacker, and what data was transferred to the attacker’s infrastructure during the incident.

NORTON ROSE FULBRIGHT

On June 3, 2020, however, Accedian received information from the attacker on the files accessed and what data had been transferred during the incident. Upon receipt of this information, Accedian immediately undertook an assessment to determine the scope of individuals affected in the United States. From this review, Accedian determined that the personal information of one New Hampshire resident was accessed by the attacker, including name, address, resume, salary or fee schedule, social security number, tax forms banking details for direct deposit purposes and photo identification.

To help protect the identity of impacted individuals, we are offering a complimentary 2 year membership of identity theft and credit monitoring solutions from CyberScout. This product provides superior identity detection and resolution of identity theft.

The affected individual will be notified of the incident on July 2, 2020. A copy of the notification letter is enclosed.

If you have any questions or need further information regarding this incident, please contact me at (514) 971 2497 or julie.himo@nortonrosefulbright.com.

Very truly yours,

Julie Himo

CC

Enclosure

[DATE]

Dear «firstName» «lastName» :

Re: Privacy Incident

We are writing to inform you of a security incident at Accedian Networks US Inc. which may impact you. We also wish to advise you of the steps we are taking to continue to protect the personal information of our employees, consultants and independent contractors as your privacy is of the utmost importance to us.

What Happened

On May 15, 2020, Accedian Networks Inc. discovered that it was the victim of a network security breach. From their investigation, an unauthorized third party gained access to an area of their network that contains certain information of employees, consultants, and independent contractors of Accedian Networks US Inc. (the "**Database**"). Based on Accedian Networks Inc.'s investigation, the following personal information contained in the Database may have been compromised: name, address, resume, salary or fee schedule, social security number, tax forms, banking details for direct deposit purposes and photo identification.

What We Are Doing

Once they discovered this incident, Accedian Networks Inc. immediately began conducting a detailed investigation and hired a leading cybersecurity firm to implement a comprehensive incident response plan, including investigation of the incident to determine the extent of the compromise, as well as contain the incident. Accedian Networks Inc. has also reported the incident to the Cybercrime Division of their local police authority and the Canadian Anti-Fraud Centre.

As we take the security of our employees, consultants and independent contractors' personal information seriously, we wanted to notify you of this incident, as well as to advise you of the steps that are being taken to protect all individuals involved.

Please review the "Information About Identity Theft Protection Guide" reference, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

Additionally, Accedian is providing you complimentary identity theft and credit monitoring solutions from CyberScout free of charge for 2 years. Through this you will be able to receive regular alerts to notify you if there are significant changes on your credit report.

These services provide you with alerts when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau.

To enroll in Credit Monitoring services at no charge, please log on to https://www.myidmanager.com within the next 90 days and follow the instructions provided.
When prompted please provide the following unique code to receive services: «Unique_code»

Please note that the service requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

In the unlikely event that your information is abused, CyberScout's resolution service includes a personal fraud specialist who will help to resolve any identity fraud issues including working with relevant agencies, businesses, and institutions.

Should you have any questions on the data incident, or on the CyberScout services, you can contact the CyberScout Resolution Center through one of the toll-free numbers listed below.

- UK: 0808 189 0400 — Monday through Friday, 8:00 am – 5:00 pm GMT
- USA: 1-800-405-6108 — 24/7 access
- Canada: 1-866-272-1223 — Monday through Friday, 8:00 am – 5:00 pm EST

If your country is not listed above, you can request a call back from CyberScout at your preferred date/time. Please email your name, phone number, unique code, as well as a preferred time of contact (including time zone) and language to support@cyberscout.ca.

For More Information

Should you have any further questions or concerns regarding this matter and / or the protections available to you, you may contact our dedicated call center at the number or email outlined above.

Sincerely,

Carlo Fidanza, Chief People Officer of Accedian Networks Inc.
Martin Lebeau, Director of Accedian Networks US Inc.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
800-525-6285 Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	888-397-3742 Consumer Fraud Assistance P.O. Box 9556 Allen, TX 75013 www.experian.com	800-680-7289 Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016 www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

Free Credit Report. We remind you 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. 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, Georgia 30348-5281.

Medical Privacy. We recommend that you regularly review the explanation of benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

For California residents: We also suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also

may delay you when you seek to obtain credit. Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a fraud alert on your file free of charge.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. You have the ability to place a security 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 be able to use an online process, an automated telephone line, or 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 security freeze 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 five 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, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a security freeze on your credit report free of charge.

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 avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center. 600 Pennsylvania Avenue, NW, Washington, D.C. 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 Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274- 4400.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file 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. You also have a right to file a police report and obtain a copy of it.

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

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.