LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

January 12, 2021

VIA EMAIL
Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust
1050 East Interstate Avenue, Suite 200
Bismarck, ND 58503-5574
ndag@nd.gov

Re: Notice of Data Security Incident

Dear Attorney General Stenehjem:

We represent Sedgwick Claims Management Services, Inc. ("Sedgwick"). This letter is being sent pursuant N.D. Cent. Code §§ 51-30-01 et seq. because the information of 13 North Dakota residents may have been affected by a recent data security incident.

On July 31, 2020, Sedgwick detected that data on a limited number of servers within a network environment it acquired from the purchase of Cunningham Lindsey had been affected by a data security incident. It immediately launched an investigation and engaged a forensics firm to assist with its response. The incident did not have a material effect on its normal operations. Notably, it did not affect Sedgwick's core claims administration systems. Within 48 hours, over the course of a weekend, the affected servers had been restored.

At the conclusion of the forensic investigation, Sedgwick identified that certain data on its systems may have been acquired without authorization during the incident. It immediately launched a comprehensive review of that data with outside e-discovery experts, which concluded in December 2020. The personal information potentially involved included individuals' names, Social Security or other government ID number, financial account information, medical related information, health insurance or medical ID number, and/or other related employment records.

Sedgwick completed notifying the North Dakota residents on December 22, 2020. Sedgwick offered all potentially affected individuals credit monitoring and identity theft protection services through Experian. A template copy of the notice is attached. To the extent Sedgwick identifies any additional residents of North Dakota who may have been affected by this incident, those individuals will be promptly notified.

In addition to restoring its systems, Sedgwick has taken measures to further increase the security of the affected network environment. These measures included a thorough threat hunt using Carbon

Black Defense endpoint detection and response agents, during which the environment was monitored by a team of cybersecurity professionals. All malicious files identified by the forensics and threat hunting teams were blocked organization-wide using Carbon Black. Additionally, a global credential reset was conducted within the environment, during which users were required to confirm their identities with the Sedgwick help desk prior to obtaining new passwords.

Although Sedgwick has many processes in place to mitigate, detect and rapidly respond to attempts to access systems without authorization, it has implemented measures to enhance its information security program and reduce the risk of a recurrence of this or similar cybersecurity events. These enhancements included:

- Enhancing its endpoint detection and response program by applying Carbon Black Protection in High Enforcement mode on all Windows based servers, thereby preventing execution of unauthorized applications.
- Enhancing its program of continuously updating and regularly reviewing firewall and IDS/IPS rule sets.
- Deploying Darktrace Enterprise Immune System to these environments with real-time monitoring and alerts to Sedgwick's dedicated IT security team.

Please contact me should you have any questions.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Attachment: Consumer Notification Letter

Date

Name
Address
City/State/Zip

Notice of Data Security Incident

Dear Name,«GreetingLine»

We are writing to share with you some important information regarding an incident that may have involved some of your personal information.

What Happened.

On July 31, 2020, we detected unusual activity within two of our data centers and immediately launched an investigation. The investigation determined that records were acquired without authorization. The records were contained on Cunningham Lindsey data servers that were accessed without authorization between July 31 and August 2, 2020. Due to the complex nature of the data involved, an extensive review was required to ascertain the types of data that may have been affected. This review was conducted as swiftly as possible but took months to complete. It was determined that your information may have been involved in the incident. As a result, we are contacting you to offer credit and identity monitoring services at no cost to you.

What Information Was Involved.

The information involved may have included your name, address, telephone number, email address, date of birth, Social Security or other governmental ID number, financial account information, medical related information, health insurance or medical ID number and/or other related employment records.

What We Are Doing.

As soon as we discovered this incident, we took the measures referenced above. We engaged in a thorough review of this incident and have undertaken efforts to minimize the likelihood of such an incident happening again.

We are also to offering you the protection of one year of complimentary credit monitoring.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks^{SM}. This product provides you with superior identity detection and resolution of identity theft.

Please see the attached Experian document with the activation code.

Sedgwick works to protect the privacy of all individuals by continually refining our privacy and security programs and incident response procedures, regularly training of our employees, and conducting annual privacy assessments.

What You Can Do.

We recommend that you activate your complimentary Experian IdentityWorks[SM] services. Activation instructions are included with this letter. We also recommend that you review the guidance in this letter about how to protect your personal information.

Other Important Information.

By taking the following simple steps and availing yourself of the Experian services described above, you can further protect your personal information.

Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also 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, call 1-877-322-8228, or complete an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled with Experian, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with Experian, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned a Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

Notify Law Enforcement of Suspicious Activity: You should know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement.

Fraud Alerts: You may want to consider placing a fraud alert with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. 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. The contact information to place fraud alerts at all three bureaus is as follows:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 6790
www.equifax.com	www.experian.com	Fullerton, CA 92834-6790
		www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods to place a fraud alert. 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.

Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. There is no cost for this service. Simply contact the three national credit reporting bureaus listed above in writing to place the 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. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

For More Information.

You can obtain additional information about the steps you can take to avoid identity theft from the following:

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

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For Rhode Island Residents:
Rhode Island Attorney General
Consumer Protection Unit

For New York Residents:
New York Attorney General
Bureau of Internet and Technology

150 South Main Street Providence, RI 02903 www.riag.ri.gov Telephone: 401-274-4400	28 Liberty Street New York, New York 10005 www.ag.ny.gov Telephone 1-800-771-7755 **For all other US Residents:** Identity Theft Clearinghouse Federal Trade Commission 600 Pennsylvania Avenue, NW Washington, DC 20580 www.consumer.gov/idtheft 1-877-IDTHEFT (438-4338) TDD: 1-202-326-2502

We sincerely apologize for any inconvenience this event may cause you.

Sincerely,

Brenda Corey
Chief Privacy Officer