WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

May 25, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via E-MAIL

Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust Division
1050 E. Interstate Avenue, Suite 200
Bismarck, ND 58503
ndag@nd.gov

Re: Data Security Incident

Dear Attorney General Stenehjem:

We represent Mountain State Financial Group, LLC ("MSFG") with respect to a potential data security incident described in greater detail below. MSFG is a mortgage company based in Westminster, Colorado. MSFG takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future. At this time, MSFG does not have any evidence of the misuse of information.

1. **Nature of the incident.**

On April 26, 2021, an unknown third party broke into MSFG's office and stole some office equipment, including one hard drive. MSFG immediately began an investigation to determine what information was contained in the hard drive, and the individuals potentially impacted by the incident. The investigation concluded on May 11, 2021, and revealed that the drive contained borrowers' information necessary to obtain a loan (possibly including the name, address, date of birth, Social Security number, driver's license number, passport number, military ID number, W-2s, 1099s, paystubs, tax returns, pension, 401K, bank statements, student loan documentation, information on credit, insurance information, electronic signature, and other information necessary to apply for a mortgage). MSFG immediately filed a report with the police.

2. **Number of North Dakota residents affected.**

860 North Dakota residents may have been affected by this incident. Notification letters were mailed on May 25, 2021, by first class mail. A sample copy of the notification letter is included with this letter as **Exhibit A**.

3. Steps taken in response to this incident.

MSFG takes the security of all information in its control very seriously, and is taking steps to prevent a similar event from occurring in the future, as well as, to protect the privacy and security of potentially impacted individuals' information. Specifically, upon discovery of the incident, MSFG immediately changed all computer passwords, added internal security cameras, and had all internal and external locks changed to improve its office security. Moreover, MSFG promptly filed a report with the police following the incident. MSFG is also providing complimentary credit monitoring and identity theft protection services to the affected individuals for twelve months.

4. Contact information.

MSFG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

Exhibit A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

This letter is to notify you that Mountain State Financial Group, LLC ("MSFG") was the victim of a data security incident that might have resulted in unauthorized access to some of your personal information. MSFG takes the privacy and protection of your personal information very seriously. MSFG regrets any inconvenience this may cause. This letter contains information about what happened, steps MSFG has taken, and resources MSFG is making available to you to help protect your identity.

What Happened:

On April 26, 2021, an unknown third party broke into MSFG's office and stole some office equipment, including one hard drive. MSFG immediately began an investigation to determine what information was contained in the hard drive, and the individuals potentially impacted by the incident.

What Information Was Involved:

The investigation concluded on May 11, 2021, and revealed that the drive contained borrowers' information necessary to obtain a loan (possibly including the name, address, date of birth, Social Security number, driver's license number, passport number, military ID number, W-2s, 1099s, paystubs, tax returns, pension, 401K, bank statements, student loan documentation, information on credit, insurance information, electronic signature, and other information necessary to apply for a mortgage). MSFG immediately filed a report with the police. While MSFG does not believe that your personal information has been misused by any third parties, out of an abundance of caution MSFG wanted to inform you of this incident.

What We Are Doing:

Upon discovery of this incident, MSFG immediately changed all computer passwords, added internal security cameras, and had all internal and external locks changed to improve its office security. Moreover, MSFG promptly filed a report with the police following the incident. At this time, MSFG is not aware of your information being used in an unauthorized manner, but out of an abundance of caution, MSFG wanted to make you aware of this matter and offer resources to help you protect your information.

What You Can Do:

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **August 27, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

More Information:

MSFG sincerely regret any inconvenience that this incident may cause you and remains dedicated to protecting your personal information. Should you have any questions or concerns about this incident, please contact 1-???-???-???? between 7:00 a.m. and 4:30 p.m. Mountain Time, excluding some U.S. holidays.

Sincerely,

Robert Hoff, CFA, President
For Mountain State Financial Group, LLC

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281**.**

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included 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. 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.