Gregory Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1127 High Ridge Road, #301
Stamford, CT 06905

June 4, 2020

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Interstates ("Interstates") located at 1400 7th Avenue NE, PO Box 260, Sioux Center, Iowa 51250, and are writing to notify your office of an incident that may affect the security of some personal information relating to six hundred eighty three (683) Iowa residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Interstates does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 20, 2020, Interstates discovered that personal information of its employees may have been accessed by an unauthorized third party in connection with a data security incident experienced by Paperless Pay. Paperless Pay is a vendor Interstates previously utilized to provide employees with access to their paystubs and W2 forms. With the assistance of third-party forensic specialists, Paperless Pay determined that an unknown third party accessed a Paperless Pay server that stores information of Interstates' employees on February 18, 2020. While the investigation by third-party forensic specialists was able to confirm access to the Paperless Pay server, the investigation was unable to rule out access to Interstates' employee information on the server.

The information that could have been subject to unauthorized access includes names, addresses, and Social Security numbers.

Notice to Iowa Residents

On or about June 4, 2020, Interstates provided written notice of this incident to all affected individuals, which includes six hundred eighty three (683) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Interstates moved quickly to investigate and respond to the incident and notify potentially affected individuals. Interstates is no longer utilizing the services of Paperless Pay and is seeking assurances that Paperless Pay is destroying any information of Interstates' employees from their systems. Interstates is also providing access to credit monitoring services for one year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Interstates is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Interstates is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory Bautista of
MULLEN COUGHLIN LLC

GJB /kml

EXHIBIT A

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

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

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

Interstates writes to inform you of a recent incident experienced by a third-party vendor of Interstates that may affect the security of some of your personal information. As a current or former employee of Interstates, we take the security of your information very seriously and sincerely apologize for any concern this incident may cause. This letter contains information about the incident, our response, and steps you may take to better protect yourself against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What happened?

On April 20, 2020, Interstates discovered that your personal information may have been accessed by an unauthorized third party in connection with a data security incident experienced by Paperless Pay. Paperless Pay is a vendor Interstates previously utilized to provide employees with access to their paystubs and W2 forms. With the assistance of third-party forensic specialists, Paperless Pay determined that an unknown third party accessed a Paperless Pay server that stores information of our employees on February 18, 2020. While the investigation by third-party forensic specialists was able to confirm access to the Paperless Pay server, the investigation was unable to rule out access to any Interstates employee information stored on the server.

What information was involved?

We determined that your name, address, and Social Security number were stored on the accessed Paperless Pay server. While we are not aware of any attempted or actual misuse of anyone's information in connection with this incident, we are notifying you of this incident and offering you resources to help you protect your information.

What we are doing.

We take this matter and the security of your personal information very seriously. We want to assure you that we are no longer utilizing the services of Paperless Pay and are seeking assurances that Paperless Pay is destroying any Interstates employee information from their systems. As part of our ongoing commitment to the security of personal information in our care, we are also working to review our existing policies and procedures and to implement additional safeguards to enhance the security of employee information in our possession.

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 **September 2, 2020** to activate your identity monitoring services.*

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

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Steps You Can Take to Help Protect Personal Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-844-994-2103, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Again, we sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is a top priority for Interstates and we remain committed to safeguarding your personal information.

Sincerely,

Joel Van Egdom
Chief Financial Officer

Steps You Can Take to Help Protect Personal Information

Take Advantage of Your Identity Monitoring Services. You've 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.

Monitor Your Accounts. We encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity.

Free Credit Report. Under U.S. law you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report, 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 website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

For Colorado, Georgia, Maryland and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Fraud Alert. As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alerts	www.equifax.com/personal/credit-report-services

Federal Trade Commission and State Attorney General Offices. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

- **For Maryland residents.** You may contact the Maryland Office of the Attorney General, Consumer Protection Division at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, www.oag.state.md.us, (410) 528-8662.
- **For North Carolina residents.** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, (919) 716-6000.

Reporting of Identity Theft and Obtaining a Police Report.

- **For Iowa residents.** You are advised to report any suspected incidents of identity theft to local law enforcement or the Iowa Attorney General.
- **For Oregon residents.** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.