MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 23, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Insuramax, located at 2200 Greene Way, Louisville, KY 40220, and are writing to notify you of an incident that may affect the security of the personal information of approximately one (1) New Hampshire resident. This notice may be supplemented if significant facts are learned subsequent to its submission. By providing this notice, Insuramax does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

Nature of the Data Event

On April 17, 2019, Insuramax became aware of suspicious activity relating to an employee email account. Insuramax immediately launched an investigation to determine what may have happened. Working together with a leading computer forensics investigation firm, their investigation determined that an unauthorized actor or actors accessed a total of three employee email accounts between February 12, 2019 and April 23, 2019. No other email accounts or Insuramax systems were impacted by this incident.

Because the investigation was unable to determine which email messages within the accounts may have been viewed by the unauthorized actor, Insuramax reviewed the entire contents of the three email accounts to identify what personal information was accessible to the unauthorized actor(s). The large volume and variety of documents in need of review required a combination of automated forensic tools and manual document review to check this data for the presence of PII. The identities of the individuals impacted by this incident were determined on June 14, 2019 after a thorough programmatic and manual review of the three email accounts. Insuramax is the owner

of certain data for its individual clients and is the collector of data for its business insured clients, most of which are employers. Insuramax began working to identify each impacted individual as either an independent individual client, or an employee of a business insured client, in order to prepare the proper notifications. Once the impacted individuals were matched to their employer where applicable, Insuramax began an extensive internal review to confirm the mailing addresses for the impacted individuals as well as its business insured clients whose employees were impacted, in order to provide notice of the event.

The types of PII relating to the New Hampshire resident stored within the impacted email accounts included the individual's name, Social Security number, and medical or health information provided in connection with preparation of life insurance policies or processing of worker's compensation and general liability claims.

Notice to New Hampshire Resident

On September 19, 2019, Insuramax provided notice of this incident to the impacted data owners and offered to fulfill individual and state regulatory disclosures the impacted data owners have as a result of this incident, upon direction from the impacted data owners to provide such notifications. Insuramax received authorization to provide the instant notice on behalf of one of the data owners on October 16, 2019. On October 23, 2019, Insuramax will begin providing notice to the individuals for whom they have address information, including the one (1) New Hampshire resident. Substitute notice is being provided to approximately two thousand five hundred twenty-nine (2,529) individuals for whom neither Insuramax nor the relevant data owner has address information. Notice is being provided to the impacted individuals in substantially the same form as the letter attached here as **Exhibit A**.

Other Steps Taken

Insuramax is offering affected individuals complimentary access to one year of free credit monitoring and identity restoration services through Kroll. Additionally, Insuramax is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, Insuramax will be providing notice to other state regulators.

Insuramax has taken several immediate steps to protect against similar incidents in the future. Upon learning of this incident, Insuramax quickly changed all employee email account passwords and took further steps to secure the email accounts. They are continuing to monitor their systems to ensure they are secure. Insuramax will be taking steps to enhance data security protections to protect against similar incidents in the future, including implementing additional technical safeguards and providing additional training and education to its employees.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:rjj
Enclosures

EXHIBIT A

INSURAMAX

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Privacy Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Insuramax is writing to notify you of an incident that may affect the security of some of your personal information. Insuramax is an independent insurance agent utilized by <<ClientDef1(Data Owner)>> to insure their company business needs. We take this incident seriously. While we are unaware of any actual or attempted misuse of your information, this letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On April 17, 2019, Insuramax became aware of suspicious activity relating to an employee email account. We immediately launched an investigation to determine what may have happened. Working together with a leading computer forensics firm, our investigation determined that an unauthorized individual or individuals accessed three employee email accounts between February 12, 2019 and April 23, 2019. Because we are unable to determine which email messages in the accounts may have been viewed by the unauthorized actor, we reviewed the entire contents of the three email accounts to identify what personal information was accessible to the unauthorized actor(s). On June 14, 2019, we identified the individuals potentially impacted by this incident after a thorough programmatic and manual review of the three email accounts. Once we confirmed the individuals who were potentially impacted, Insuramax worked to identify the best possible contact information for the impacted individuals and then began preparing an accurate written notice of this incident. No other email accounts or Insuramax systems were impacted by this incident.

What Information Was Affected? Although we cannot confirm whether your personal information was actually accessed, viewed, or acquired without permission, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The following types of your information were located in an email or attachment that may have been accessed or acquired by an unauthorized user: your <<ClientDef2(Impacted Data)>>.

What Are We Doing? Information privacy and security are among our highest priorities. Insuramax has strict security measures to protect the information in our possession. Upon learning of this incident, we quickly changed all employee email account passwords and took steps to secure the accounts. We are currently implementing additional technical safeguards as well as training and education for employees to prevent similar future incidents.

What Can You Do? Although we are not aware of any fraudulent misuse of your information, we arranged to have Kroll provide identity monitoring services for 1 year at no cost to you as an added precaution. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to activate and receive these services. Insuramax will cover the cost of this service; however, you will need to activate yourself in the identity monitoring services.

For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 1-877-594-0953, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time.

We sincerely regret any inconvenience this incident may cause you. Insuramax remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

Russ Wardlaw
President, Insuramax

Steps You Can Take to Protect Your Information

Activate Identity Monitoring

As an added precaution, we have arranged to have Kroll provide identity monitoring services for 12 months at no cost to you. 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 **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **December 30, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your financial and other account statements, and to monitor your credit reports for suspicious activity.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

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**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

If you request a security freeze with the above consumer reporting agencies, you may 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; and
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military information, etc.)

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice was not delayed by a law enforcement investigation. ***For Maryland residents,*** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***For North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1]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.