[Date]

[Name]
[Address]
[City], [State] [Zip Code]

Re: Notice of Data Breach

Dear [Name]:

Axis Insurance Services ("Axis") recently discovered an event that may affect the security of certain information related to your company. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. While we have no evidence that your company's information was actually accessed, viewed, acquired, or misused, we are notifying you of this incident out of an abundance of caution.

What Happened? On December 12, 2016, several Axis employees received a spam phishing email to their Axis email accounts. One Axis employee clicked on the link in the phishing email and entered her email credentials. That same day, this Axis employee's email account was used to send a similar phishing email to all of the individuals in the employee's contact list. Axis learned of this incident on December 12, 2016 and immediately initiated an investigation, with the assistance of third-party forensic investigators, into the nature and scope of the event. As part of this investigation, we recently determined that this employee's email account contained some of your company's information.

What Information Was Affected? The affected email account contained a copy of a business check, which contained your name, bank account number, and bank routing number.

What We Are Doing. We take this incident and the security of your company's information very seriously. In addition to hiring a third-party forensic expert to assist in our investigation, we took steps to prevent further misuse of this employee's credentials and confirm the security of both her workstation and our network. We also instructed all Axis employees to change their email passwords. We continue to monitor our systems to ensure the privacy and security of your company's information. In addition to providing notice of this event to you, we are also providing you with information you can use to better protect against identity theft and fraud. You can find more information and steps you can take in the enclosed *Privacy Safeguards Information*.

What You Can Do. We encourage you to review the enclosed *Privacy Safeguards Information* for additional information on how to better protect against identity theft.

For More Information. We sincerely regret any inconvenience or concern this incident may cause you. We understand that you may have questions that are not addressed in this notice. Please feel free to contact [name] at [contact information] with any additional questions or concerns.

Sincerely,

Signatory Name
Signatory Title

Enclosure

PRIVACY SAFEGUARDS INFORMATION

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your company's account statements and your company's account statements for suspicious activity. While companies do not have credit files, the following information relates to protecting an individual's credit:

Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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); and 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. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. This notice was not delayed as a result of a law enforcement notification.