haynesboone

VIA E-MAIL AND FEDERAL EXPRESS

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

November 30, 2020

Dear Sir or Madam:

We represent Insurance Audit Services, Inc., 214 West 35th Street, Davenport, IA 52806 ("IAS"). Pursuant to Iowa Code Ann. § 715C.2, we write to notify you of an incident that affects the security of information relating to 5,997 Iowa residents. At this point, we are not aware of any losses or harm arising from the incident. By providing this notice, IAS does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

IAS is a leading provider of premium audit services and solutions to the P&C insurance industry. On behalf of its commercial carrier clients, IAS audits the commercial insurance policies of thousands of businesses nationwide. In the course of those audits, IAS collects information from its carrier clients and their policyholders.

On October 28, 2020, attackers deployed a ransomware attack in IAS's network. Immediately after discovering the attack on the morning of October 28, IAS retained legal counsel and engaged a computer forensics firm to investigate and determine the scope of the attack. IAS also notified law enforcement and is cooperating with an investigation. On November 6, 2020, IAS's forensics team identified evidence consistent with exfiltration of data. On November 10, 2020, IAS completed its analysis of the data that we believe may have been compromised to identify those impacted by the incident.

In consultation with IAS's legal and forensics teams, IAS paid the ransom that the attackers demanded and received the keys needed to decrypt its network, details regarding any information the attackers copied from its network, and confirmation that they had deleted any such data.

It appears that data belonging to IAS employees and audited policyholders in Iowa was exfiltrated from IAS's network. With respect to IAS employees, the impacted data included copies of employees' IRS Forms 1095-C, which contain names, addresses, and Social Security numbers. With respect to audited policyholders, the impacted data may have included the policyholders' business names, business addresses, phone numbers, insurance policy numbers, federal employer identification numbers ("FEIN"), and IAS-generated usernames and one-time-use initial passwords to an IAS file transfer portal. In some cases, the impacted FEINs may have been Social Security numbers.

Haynes and Boone, LLP
Attorneys and Counselors
2323 Victory Avenue
Suite 700
Dallas, Texas 75219
T (214) 651-5000
F (214) 651-5940
www.haynesboone.com

haynesboone

Pursuant to Iowa Code Ann. § 715C.2, IAS is providing notice to 48 employees and 5,949 policyholders in Iowa. IAS notified its employees of the incident by e-mail on November 12, 2020 and is in the process of sending a follow-up letter to those employees. IAS is also in the process of disclosing this security incident by letter to all impacted policyholders in this state. Notices will be mailed on November 30, 2020. This notice has not been delayed as a result of a law enforcement investigation.

After a thorough analysis and investigation into the attack, IAS believes that the risk of harm to consumers is low. IAS paid the ransom the attackers demanded and received confirmation that any data exfiltrated from IAS's network had been deleted. Moreover, the policyholders whose FEINs were impacted by this incident are nearly all commercial entities. As such, much of the impacted FEINs were true FEINs, rather than Social Security numbers. As to those consumers, the risk is even further reduced, and the impacted data does not qualify as personal information. Iowa Code Ann. § 715C.1(11)(a) (defining "personal information" with no mention of business information in definition). IAS is choosing to disclose to those policyholders because of its inability to determine with certainty that the impacted FEINs are not Social Security numbers.[1]

Nonetheless, and out of an abundance of caution, IAS opted to provide notice of the incident. IAS has also retained Single Bureau Credit Monitoring to provide one year of free credit monitoring to affected employees and policyholders. Iowa residents can activate this service by enrolling using the code provided in their notice letter within 90 days from the date of the letter. In the event that an affected individual becomes a victim of fraud, IAS is also providing $1 Million in Expense Reimbursement Insurance along with remediation support from a CyberScout Fraud Investigator. Enclosed, you will find a sample of the notice letters containing further details.

IAS is reviewing its policies and procedures and implementing additional safeguards to ensure information in its control is appropriately protected. IAS is also conducting additional training for its employees on the proper handling of sensitive information.

---

[1] With respect to the IAS-generated usernames and passwords impacted by the incident, those credentials are generated by IAS, they are issued to businesses and not individuals, the portal to which they provide access does not retain any documents or information uploaded through it (and thus no data is available using the credentials), and after logging in the first time, users were required to change their password. No user-selected passwords were compromised. As such, these login credentials do not constitute personal information requiring disclosure.

haynesboone

For further information, please do not hesitate to contact me.

Sincerely,

Timothy Newman
Haynes and Boone, LLP
timothy.newman@haynesboone.com
Direct Dial 214-651-5029

INSURANCE AUDIT SERVICES, INC.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

We value the relationship we have with our employees, and we are writing to make you aware of an incident that may have impacted your personal information. At this point, we are unaware of any losses or harm arising from the incident.

1. What happened and what information was involved:

On October 28, 2020, attackers deployed a ransomware attack in our network. As you may know, ransomware is a form of malware that hackers use to encrypt a company's files and disrupt their business, and attackers demand a ransom in exchange for decryption keys that allow a company to recover its files. In some cases, hackers copy data from a company's network as additional leverage for demanding a ransom.

Immediately after discovering the attack the morning of October 28, we retained legal counsel and engaged a computer forensics firm to investigate and determine the scope of information potentially impacted. We also notified law enforcement and are cooperating with an investigation. In consultation with our legal and forensics teams, we paid the ransom that the attackers demanded and received the keys needed to decrypt our network, details regarding the information the attackers copied from our network, and confirmation that they had deleted that data. Our forensics team identified evidence consistent with the attacker's representations regarding what data was exfiltrated.

We have reviewed the data that we believe the attacker copied from our network. It included copies of our employees' IRS Forms 1095-C, which contain your name, address, and Social Security number. We are not aware of any other sensitive employee information being compromised.

2. What we are doing and what you can do:

Given the nature of this attack, we believe the risk of harm to you is low. The attackers sought a ransom, which we paid, and the attackers confirmed that they deleted the exfiltrated data. Nonetheless, and out of an abundance of caution, we wanted to notify you of the incident, so that you can take any necessary precautions. This notice has not been delayed as a result of a law enforcement investigation.

As an additional precaution, we are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for one year from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access to $1 Million in Expense Reimbursement Insurance along with remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

To enroll in Credit Monitoring services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Activation Code>>.

Please understand that we take this incident very seriously and apologize for any inconvenience it may have caused. We are reviewing our policies and procedures and implementing additional safeguards to ensure information in our control is appropriately protected.

3. For more information:

If you have questions that are not addressed in this letter, please call our dedicated assistance line at 855-914-4707, available Monday through Friday, from 8:00 a.m. to 8:00 p.m., Central Time.

Sincerely,

Chip Chaon
President & CEO

Reference Guide

Website and Enrollment: Go to https://www.myidmanager.com and follow the instructions for enrollment using your Enrollment Code provided in the letter.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

You should also 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 or to the Attorney General.

Fraud Alerts: 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. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Additional Information: You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you

may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

INSURANCE AUDIT SERVICES, INC.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

We are writing to inform you of a data security incident suffered by Insurance Audit Services, Inc. ("IAS" or the "Company") that may have impacted your personal information. At this point, we are not aware of any losses or harm arising from the incident.

1. What happened and what information was involved:

IAS is a leading provider of premium audit services and solutions to the P&C insurance industry. At some point, your commercial insurance carrier hired IAS to perform an audit of your policy. In the course of performing that audit, we collected certain policy-related information from you or your carrier.

On October 28, 2020, attackers deployed a ransomware attack in our network. This attack was an attack on IAS, not your commercial insurance carrier. As you may know, ransomware is a form of malware that hackers use to encrypt a company's files and disrupt their business, and attackers demand a ransom in exchange for decryption keys that allow a company to recover its files. In some cases, hackers copy data from a company's network as additional leverage for demanding a ransom.

Immediately after discovering the attack the morning of October 28, we retained legal counsel and engaged a computer forensics firm to investigate and determine the scope of information potentially impacted. We also notified law enforcement and are cooperating with an investigation. In consultation with our legal and forensics teams, we paid the ransom that the attackers demanded and received the keys needed to decrypt our network, details regarding the information the attackers copied from our network, and confirmation that they had deleted that data. Our forensics team identified evidence consistent with the attacker's representations regarding what data was exfiltrated.

We have reviewed the data that we believe the attacker copied from our network. Depending on the individual circumstances, it may have contained your name, business address, phone number, insurance policy number, federal employer identification number ("FEIN"), and the IAS-generated username and the one-time-use initial password that we issued to you in order to access the Company's file transfer portal. After logging on the first time, you were required to change that password. No user-selected passwords were compromised. In some cases, your FEIN may have been your social security number. We are not aware of any other sensitive information being compromised.

2. What we are doing and what you can do:

Given the nature of this attack, we believe the risk of harm to you is low. The attackers sought a ransom, which we paid, and the attackers confirmed that they deleted the exfiltrated data. If the FEIN we have in our records is an actual FEIN and not a social security number, the risk is even further reduced. The usernames and passwords impacted by this incident were generated by IAS, and they do not allow access to any data. Once documents are uploaded to IAS, they are no longer available using those credentials, even to the user, and those credentials expire shortly after our audit is complete. Nonetheless, and out of an abundance of caution, we wanted to notify you of the incident so that you can take any necessary precautions. This notice has not been delayed as a result of a law enforcement investigation.

As an additional precaution, we are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for one year from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access to $1 Million in Expense Reimbursement Insurance along with remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

To enroll in Credit Monitoring services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Activation Code>>.

Please understand that we take this incident very seriously and apologize for any inconvenience it may have caused. We are reviewing our policies and procedures and implementing additional safeguards to ensure information in our control is appropriately protected, and we are conducting additional training for our employees on the proper handling of sensitive information.

3. For more information:

If you have questions that are not addressed in this letter, please call our dedicated assistance line at 855-914-4707, available Monday through Friday, from 8:00 a.m. to 8:00 p.m., Central Time.

Sincerely,

Chip Chaon
President & CEO

Reference Guide

Website and Enrollment: Go to https://www.myidmanager.com and follow the instructions for enrollment using your Enrollment Code provided in the letter.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

You should also 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 or to the Attorney General.

Fraud Alerts: 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. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Additional Information: You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek

damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.