EXHIBIT AA

[redacted]

From: Nicole Bayer
Sent: Monday, February 13, 2023 4:08 PM
To: ocpdatabreach@mt.gov
Cc: Richard Aponte-Boyd; Katharin DiRosa
Subject: Intelligent Business Solutions – Notice of Data Event – Montana
Attachments: Intelligent Business Solutions - Notice of Data Event - MT.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Hello,

Please see the attached notice of data event.

Thank you,

Nicole

Nicole Bayer
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-4430 - Office
(215) 534-9176 - Mobile
nbayer@mullen.law

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 10, 2023

VIA E-MAIL

Montana Department of Justice
Office of Consumer Protection
P.O. Box 200151
Helena, MT 59620-0151
E-mail: ocpdatabreach@mt.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Intelligent Business Solutions ("IBS") located at 301C S. Liberty Street, Winston-Salem, North Carolina 27101, and write to notify your office of an incident that may affect the security of certain personal information relating to one (1) Montana resident. 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, IBS does not waive any rights or defenses regarding the applicability of Montana law, the applicability of the Montana data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around November 14, 2022, IBS became aware of suspicious activity within its computer network. IBS immediately launched an investigation, with the assistance of third-party computer forensic specialists, and determined that its network had been infected with malicious software that prevented access to certain files on certain systems. On November 25, 2022, IBS notified certain clients that some of its patients' information had been compromised by the security incident. Through our investigation, we determined that, between November 10, 2022, and November 15, 2022, an unauthorized actor may have had access to certain systems that stored personal information. A thorough and time-intensive review of the systems impacted was conducted, with the assistance of third-party experts to determine if any personal information may have been accessible within the system and to whom that information relates.

The information that could have been subject to unauthorized access includes name, Social Security number, medical treatment and procedure information

Notice to Montana Resident

On or about February 10, 2023, IBS began providing written notice of this incident to one (1) Montana 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, IBS moved quickly to investigate and respond to the incident, assess the security of IBS systems, and identify potentially affected individuals. Further, IBS notified federal law enforcement regarding the event. IBS is providing access to credit monitoring services for two (2) years through CyberScout to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, IBS 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. IBS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

IBS is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. IBS also notified the U.S. Department of Health and Human Services, as well as federal law enforcement.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,

Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/kld
Enclosure

EXHIBIT A

Intelligent Business Services
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

February 10, 2023

NOTICE OF Security Incident

Dear

Intelligent Business Solutions ("IBS") writes to notify you of an incident that may affect the privacy of some of your personal information. IBS provides services for Riverside Health System ("Riverside") related to Riverside cardio thoracic patients. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about November 14, 2022, IBS became aware suspicious activity within its network systems. IBS immediately launched an investigation, with the assistance of third-party computer forensic specialists, and determined that its network had been infected with malware which prevented access to certain files on certain system. Through our investigation, we determined that, between November 10, 2022, and November 15, 2022, an unauthorized actor may have had access to certain systems that stored personal information. A thorough and time-intensive review of the systems impacted was conducted, with the assistance of third-party experts to determine if any personal information may have been accessible within the system and to whom that information relates to. Once the determination of whose information was impacted, address information was compiled for the impacted individuals, for purpose of providing notice.

What Information Was Involved? Our investigation determined the following types of your information may have been impacted by this incident: Social Security number, date of birth, health insurance information, medical treatment and procedure information, and your name. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. Data privacy and security are among IBS' highest priorities, and there are extensive measures in place to protect information in IBS' care. Upon discovery, IBS promptly commenced an investigation with the assistance of third-party cyber security specialists to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. Although IBS had policies and procedures surrounding data security at the time of the incident, as part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies and procedures to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities, as required by law. IBS notified law enforcement and is cooperating with its investigation.

As an added precaution, we are also offering you access to twenty-four (24) months of complimentary credit monitoring services through CyberScout. Individuals who wish to receive these services must enroll by following the attached enrollment instructions, as we cannot enroll you on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached Steps You Can Take to Help Protect Personal Information. There you will also find more information on the complimentary credit monitoring services we are making available to you. While these services will be at no cost to you, you will need to enroll in the services yourself as we cannot do so on your behalf.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-570-2911 between the hours of 8:00 a.m. and 8:00 p.m. ET, Monday – Friday, excluding holidays. You may also write to IBS at 301 South Liberty Street, Suite C, Winston-Salem, North Carolina, 27101.

Sincerely,

Intelligent Business Solutions

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration:

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/intelligentbusiness** and follow the instructions provided. When prompted please provide the following unique code to receive services: In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two (2) Rhode Island residents impacted by this incident.

EXHIBIT B

Intelligent Business Solutions
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07163B 1-1

[redacted]

February 23, 2023

[redacted]

Intelligent Business Solutions ("IBS") writes to notify you of an incident that may affect the privacy of some of your protected health information. IBS, a vendor of The Cleveland Clinic Foundation ("Cleveland Clinic"), provides an online service to enable Cleveland Clinic to share patient information with patient registries, which are clinical databases that help healthcare organizations measure, benchmark, and improve quality of care. In this role, IBS became aware of a security incident involving protected health information. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you wish to do so.

What Happened? On or around November 14, 2022, IBS became aware of suspicious activity within its computer network. IBS immediately launched an investigation, with the assistance of third-party computer forensic specialists, and determined that its network had been infected with malicious software that prevented access to certain files on certain systems. On January 10, 2023, IBS notified Cleveland Clinic that some of its patients' information had been compromised by the security incident. Through our investigation, we determined that, between November 10, 2022, and November 15, 2022, an unauthorized actor may have had access to certain systems that stored personal information. A thorough and time-intensive review of the systems impacted was conducted, with the assistance of third-party experts to determine if any personal information may have been accessible within the system and to whom that information relates.

What Information Was Involved? Our investigation determined the following types of your information may have been impacted by this incident: [redacted]. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. Data privacy and security are among IBS's highest priorities, and there are extensive measures in place to protect information in IBS's care. Upon discovery, IBS promptly commenced an investigation with the assistance of third-party computer forensic specialists to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. Although IBS had policies and procedures surrounding data security at the time of the incident, as part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies and procedures to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities, as required by law. IBS notified law enforcement and is cooperating with its investigation.

As an added precaution, we are also offering you access to twenty-four (24) months of complimentary credit monitoring services through Cyberscout. Individuals who wish to receive these services must enroll by following the attached enrollment instructions, as we cannot enroll you on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached Steps You Can Take to Help Protect Personal Information. There you will also find more information on the complimentary credit monitoring services we are making available to you. While these services will be at no cost to you, you will need to enroll in the services yourself as we cannot do so on your behalf.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-570-2911 between the hours of 8:00 a.m. and 8:00 p.m. ET, Monday – Friday, excluding holidays. You may also write to IBS at 301 South Liberty Street, Suite C, Winston-Salem, North Carolina, 27101.

Sincerely,

Intelligent Business Solutions

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/intelligentbusiness** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus: Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. 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 Connecticut residents, you may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection | New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. There are two (2) Rhode Island residents impacted by this incident.