EXHIBIT A

Akumin, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

AKUMIN

December 23, 2024

Dear [redacted] :

We are reaching out to you because you received services from Akumin, a healthcare organization and provider of imaging and related health services, or you received services from Akumin at a partnered health care facility or hospital. As we disclosed on our website at the time of the incident, Akumin experienced a ransomware incident in October 2023. Since the incident, we conducted a detailed review of the impacted data, and are reaching out to you to let you know that the incident involved some of your information. This correspondence provides you with a summary of why we have your information, what happened, steps we have taken in response to this matter, and steps you may take should you wish to do so.

Why Does Akumin Have My Information? Akumin is a healthcare organization and provider of imaging, radiation oncology, and related health services. Akumin provides these services at Akumin's locations, and also provides services at partnered health care facilities. Akumin has your information because you received services from Akumin at one of Akumin's locations, a location of an Akumin owned subsidiary, a company acquired by Akumin, or on-site at a hospital or partner location where Akumin provides imaging or radiation oncology services.

What Happened? On October 11, 2023, we learned that malware had been used to lock access to some of our computer files without permission. We promptly began an investigation and notified certain law enforcement and other governmental authorities. We also took measures to contain and assess the incident, including taking our systems offline until we were able to securely restore them. Within days, we published information about this incident on our website. In December 2023, we also published formal notification on our website and began issuing rolling notification letters.

During our investigation of this matter, we identified that files on certain systems were copied without permission. The files were copied on October 11, 2023. To ensure we could properly notify individuals that their information was in the copied files, including the types of information about them contained within the files, we undertook an intensive review of those files. We recently completed the portion of our review that identified your information on December 11, 2024.

What Information Was Involved? Based on our review, we understand that the copied files included the following types of information related to you: name, home address, other contact information, date of birth, Social Security number, medical record number and billing or claims information. Please note, however, that your information being contained in the files does not mean that you are the victim of identity theft or fraud, and we have no indication of an individual experiencing verified identity theft as a result of this incident, and any steps you may wish to take in response to this matter are a personal decision. Nevertheless, if you have any concerns, we are providing you with free resources and guidance as detailed below.

What We Are Doing. Following our review, we continue to notify individuals whose information was in the copied files on a rolling basis, and expect all notice to be complete by the end of the year. Additionally, we are providing individuals with free resources and guidance in the enclosed "Steps Individuals Can Take To Protect Personal Information." While no safeguards can fully prevent all cybersecurity attacks, we also implemented additional technical measures and processes to further enhance the company's security.

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 and to detect errors. We also recommend you review the "Steps Individuals Can Take To Protect Personal Information" section of this letter. There, you can find more information, and a list of free resources to help protect your information should you feel it is appropriate to do so.

For More Information. If you have questions about this matter, we have a dedicated assistance line with agents ready to answer your questions. Please contact our toll-free dedicated assistance line at 1-833-799-4335, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern, excluding holidays. You may also write to us at Akumin, Attn: Compliance Department, 8300 W. Sunrise Blvd., Plantation, FL 33322.

We are committed to maintaining the security of your information and confidence in our services. We thank you for your patience and understanding.

Sincerely,

Akumin

* Una versión de esta notificación en español está disponible en nuestro sitio web en www.Akumin.com.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

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 a free credit report, visit **www.annualcreditreport.com** or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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; 1-202-442-9828; and **oag.dc.gov**.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and **https://www.marylandattorneygeneral.gov/**. You may also contact Akumin at Akumin, Attn: Compliance Department, 8300 W. Sunrise Blvd., Plantation, FL 33322.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 Avenue NW, Washington, DC 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; 1-401-274-4400; and **www.riag.ri.gov**. Under Rhode Island law, individuals have the right to obtain any police report filed regarding this matter. There are approximately 15,448 Rhode Island residents that may be affected by this matter.

[redacted]

Akumin, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

AKUMIN

December 23, 2024

Dear [redacted]:

We are reaching out to you about a matter that involves your information. As we disclosed on our website at the time of the incident, Akumin experienced a ransomware incident in October 2023. Since the incident, we conducted a detailed review of the impacted data, and are reaching out to you to let you know that the incident involved some of your information. This correspondence provides you with a summary of why we have your information, what happened, steps we have taken in response to this matter, and steps you may take should you wish to do so.

Why Does Akumin Have My Information? Akumin is a healthcare organization and provider of imaging, radiation oncology, and related health services. In this capacity, Akumin receives personal information from current and former employees, which can include their beneficiaries and dependents. Akumin also maintains personal information for certain vendors. Akumin may have your information because you or a guardian were employed by, or a vendor of, or were in a contractual relationship with Akumin to provide professional or technical services at Akumin, an Akumin owned subsidiary, or a company acquired by Akumin.

What Happened? On October 11, 2023, we learned that malware had been used to lock access to some of our computer files without permission. We promptly began an investigation and notified certain law enforcement and other governmental authorities. We also took measures to contain and assess the incident, including taking our systems offline until we were able to securely restore them. Within days, we published information about this incident on our website. In December 2023, we also published formal notification on our website and began issuing rolling notification letters.

During our investigation of this matter, we identified that files on certain systems were copied without permission. The files were copied on October 11, 2023. To ensure we could properly notify individuals that their information was in the copied files, including the types of information about them contained within the files, we undertook an intensive review of those files. We recently completed the portion of our review that identified your information on December 11, 2024.

What Information Was Involved? Based on our review, we understand that the copied files included the following types of information related to you: Social Security number, and payment card information. Please note, however, that your information being contained in the files does not mean that you are the victim of identity theft or fraud, and we have no indication of an individual experiencing verified identity theft as a result of this incident, and any steps you may wish to take in response to this matter are a personal decision. Nevertheless, if you have any concerns, we are providing you with free resources and guidance as detailed below.

What We Are Doing. Following our review, we continue to notify individuals whose information was in the copied files on a rolling basis, and expect all notice to be complete by the end of the year. Additionally, we are providing individuals with free resources and guidance in the enclosed "Steps Individuals Can Take To Protect Personal Information." While no safeguards can fully prevent all cybersecurity attacks, we also implemented additional technical measures and processes to further enhance the company's security.

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 and to detect errors. We also recommend you review the "Steps Individuals Can Take To Protect Personal Information" section of this letter. There, you can find more information, and a list of free resources to help protect your information should you feel it is appropriate to do so.

For More Information. If you have questions about this matter, we have a dedicated assistance line with agents ready to answer your questions. Please contact our toll-free dedicated assistance line at 1-833-799-4331, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern, excluding holidays. You may also write to us at Akumin, Attn: Compliance Department, 8300 W. Sunrise Blvd., Plantation, FL 33322.

We are committed to maintaining the security of information in our care, and thank you for your patience and understanding.

Sincerely,

Akumin

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

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 a free credit report, visit **www.annualcreditreport.com** or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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; 1-202-442-9828; and **oag.dc.gov**.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and **https://www.marylandattorneygeneral.gov/**. You may also contact Akumin at Akumin, Attn: Compliance Department, 8300 W. Sunrise Blvd., Plantation, FL 33322 or 1-800-559-7226.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 Avenue NW, Washington, DC 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; 1-401-274-4400; and **www.riag.ri.gov**. Under Rhode Island law, individuals have the right to obtain any police report filed regarding this matter. There are approximately 15,448 Rhode Island residents that may be affected by this matter.