ATI Holdings, LLC

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00511
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 21, 2018

Re: Notice of Data Security Incident

Dear John Sample:

ATI Holdings, LLC and its subsidiaries ("ATI") recently discovered an event that may affect the security of your personal information. We want 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.

What Happened? On January 11, 2018, ATI discovered that certain employees' direct deposit information was changed in our payroll platform. We took immediate steps to mitigate the impact of the incident, and also promptly initiated an internal investigation, with the assistance of third-party forensic investigators, to determine the nature and scope of the incident, including whether any sensitive information was affected. ATI discovered that, due to a series of ongoing phishing attacks, some employee email accounts were subject to unauthorized access between: i) January 9, 2018 and January 12, 2018; and ii) February 26, 2018 and March 15, 2018. ATI discovered and remediated these phishing attacks during this same time period. Your information was included in one or more of the email accounts accessed between February 26, 2018 and March 15, 2018.

What Information Was Involved? As of June 1, 2018, ATI confirmed that one or more of the affected email accounts contained, and the unauthorized actor may have had access to, certain information related to you, including: name [redacted]. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of your personal information very seriously. In addition to working with a third-party forensic investigator to conduct an investigation, ATI has taken a multitude of steps to strengthen the security of its email systems moving forward, including ensuring all affected employees changed passwords, implementing multi-factor authentication, blocking certain links and attachments, and providing additional training to users and employees on how to identify phishing scams. ATI has also contacted and is working with appropriate law enforcement agencies and regulators regarding this incident. We are also providing you with information you can use to better protect against identity theft and fraud, as well as access to 12 months of credit monitoring and identity restoration services with AllClear ID, all at no cost to you. You can find more information regarding steps you can take, as well as information on how to enroll in the credit monitoring services, in the enclosed *Privacy Safeguards Information*.

What You Can Do. Please review the enclosed *Privacy Safeguards Information* for additional information on how to better protect against identity theft and fraud. You can also enroll to receive the complimentary credit monitoring and identity restoration services.

For More Information. Please know that nothing is more important to ATI than the security of the information we maintain. We understand that you may have questions that are not addressed in this notice. If you have additional questions, please call our toll-free dedicated assistance line at 1-855-828-5850. This toll-free line is available Monday through Saturday, from 8:00 am to 8:00 pm CT, excluding major national holidays.

Sincerely,

Sarah Buerger

Sarah Buerger
Head of Security

Enclosure

PRIVACY SAFEGUARDS INFORMATION

Enroll in Credit Monitoring. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-828-5850 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at [redacted] or by phone by calling 1-855-828-5850.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Monitor Your Accounts.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports and explanation of benefits forms for suspicious activity. 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.

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. 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 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. 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	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/credit-freeze/place-credit-freeze

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud 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 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, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 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 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 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 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.

NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

ATI Holdings, LLC and its subsidiaries ("ATI") recently discovered an incident that may affect the security of personal information of certain ATI patients. We have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. We are taking additional actions to strengthen the security of our email systems moving forward. ATI has also contacted and is working with appropriate law enforcement agencies and regulators regarding this incident.

FREQUENTLY ASKED QUESTIONS

What happened? On January 11, 2018, ATI discovered that certain employees' direct deposit information was changed in our payroll platform. We took immediate steps to mitigate the impact of the incident, and also promptly initiated an internal investigation, with the assistance of third-party forensic investigators, to determine the nature and scope of the incident, including whether any sensitive information was affected. As part of this investigation, ATI recently determined that certain ATI employee email accounts were accessed without authorization between January 9, 2018 and January 12, 2018, and that certain types of patient information were included within one or more of these email accounts.

What information may have been affected by this incident? Recently, ATI determined that one or more of the affected email accounts contained, and the unauthorized actor may have had access to, information related to certain ATI patients, including the following types of information: name, date of birth, driver's license or state identification number, Social Security number, credit card number, financial account number, patient identification number, Medicare or Medicaid identification number, medical record number, diagnosis, disability code, treatment information, medication/prescription information, doctor's or therapist's name, billing/claims information, and/or other health insurance information.. The type of information affected varies per impacted individual. Social Security number was only impacted for a small percentage of the affected population. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of patient information as a result of this incident.

How will I know if I am affected by this incident? ATI will mail notice letters to individuals whose protected information was contained within one or more of the affected emails accounts and may have been accessed by an unauthorized actor.

What is ATI doing? ATI is providing potentially impacted individuals access to free credit monitoring services. Information on these services is included in the notice letters that are being mailed to affected individuals, and can also be found at atiholdings.allclearid.com. We have ensured that all employees identified as impacted changed their passwords. We are taking additional actions to strengthen the security of our email systems moving forward, as well as providing additional training to users and employees on how to identify phishing scams. We continue to monitor our systems to better protect the privacy and security of your personal information.

Whom should I contact for more information? ATI has set up a call center to answer questions from those who might be impacted by this incident. Anyone with additional questions about the incident may contact the call center at 1-855-828-5850 (toll free), Monday through Saturday, 8:00 a.m. to 8:00 p.m. CT. If you do not receive a letter in the coming weeks, but want to know whether you are affected, please contact the call center at 1-855-828-5850.

What can I do to protect my information?

Monitor Your Accounts.

Credit Reports. ATI encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. 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.

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. 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 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or

insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 https://www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/

Additional Information.

Instances of known or suspected identity theft should be reported to law enforcement and the Federal Trade Commission. **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 encourages those who discover that their information has been misused to file a complaint with them.

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.

Updated April 27, 2018

Data Privacy Event Update

About the data privacy event

ATI Holdings, LLC and its subsidiaries ("ATI") recently discovered an incident that may affect the security of personal information of certain ATI patients. We have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. We are taking additional actions to strengthen the security of our email systems moving forward. ATI has also contacted and is working with appropriate law enforcement agencies and regulators regarding this incident.

Frequently asked questions

What happened? On January 11, 2018, ATI discovered that certain employees' direct deposit information was changed in our payroll platform. We took immediate steps to mitigate the impact of the incident, and also promptly initiated an internal investigation, with the assistance of third-party forensic investigators, to determine the nature and scope of the incident, including whether any sensitive information was affected. After a thorough digital forensic examination, investigators discovered that some patient information may have been accessible through certain of the impacted employees' email accounts between January 9, 2018 and January 12, 2018. During its investigation into and remediation of this incident, ATI uncovered evidence that additional employees were targeted and fell victim to continued phishing attacks between the dates of February 26, 2018 and March 15, 2018 (the "Continued Attacks"). ATI discovered the Continued Attacks beginning on February 26, 2018 and continuing through March 2018. After an exhaustive search of the email accounts affected by the Continued Attacks, ATI has determined that information belonging to patients was accessed between February 26, 2018 and March 15, 2018.

A forensic investigation reconfirmed that no ATI systems have been impacted except for certain employee email and payroll accounts. ATI has taken a multitude of steps to strengthen the security of its email systems moving forward, including ensuring all affected employees changed their passwords, implementing multi-factor authentication, blocking certain links and attachments, and providing additional training to users and employees on how to identify phishing scams. ATI has also contacted and is working with appropriate law enforcement agencies and regulators regarding this incident.

What information may have been affected by this incident? Information at risk includes: name, date of birth, driver's license or state identification number, Social Security number, credit card number, financial account number, patient identification number, Medicare or Medicaid identification number, medical record number, diagnosis, disability code, treatment information, medication/prescription information, doctor's or therapist's name, billing/claims information, and/or other health insurance information. The type of information potentially affected was not the same for each individual.

How will I know if I am affected by this incident? ATI's investigation is still ongoing; however, ATI will begin providing notice to newly identified affected individuals on a rolling basis, starting on April 27, 2018, and will be offering affected individuals credit monitoring and identity protection services.

What is ATI doing? ATI is providing potentially impacted individuals access to free credit monitoring and identity repair services for 12 months from the date of this notice. Information on these services is included in the notice letters that are being mailed to affected individuals, and can also be found at atiholdings.allclearid.com. Please note that AllClear ID is updating the website to reflect that the services will extend for 12 months from the date of this notice. We have ensured that all employees identified as impacted changed their passwords. We are taking additional actions to strengthen the security of our email systems moving forward, as well as providing additional training to users and employees on how to identify phishing scams. We continue to monitor our systems to better protect the privacy and security of your personal information.

Whom should I contact for more information? ATI has set up a call center to answer questions from those who might be impacted by this incident. Anyone with additional questions about the incident may contact the call center at 1-855-828-5850 (toll free), Monday through Saturday, 8:00 a.m. to 8:00 p.m. CT. If you do not receive a letter in the coming weeks, but want to know whether you are affected, please contact the call center at 1-855-828-5850.

What can I do to protect my information?

Monitor Your Accounts

Credit Reports. ATI encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. 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.

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. 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 19016**
1-800-525-6285	**1-888-397-3742**	**1-800-680-7289**
www.equifax.com	**www.experian.com**	**www.transunion.com**

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. 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**	**P.O. Box 2000**
Atlanta, GA 30348	**Allen, TX 75013**	**Chester, PA 19016**
1-800-685-1111	**1-888-397-3742**	**1-888-909-8872**
https://www.freeze.equifax.com	**www.experian.com/freeze/**	**freeze.transunion.com/**

Additional Information.
Instances of known or suspected identity theft should be reported to law enforcement and the Federal Trade Commission. **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 encourages those who discover that their information has been misused to file a complaint with them.

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.