ATI News

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.

---

https://news.atipt.com/2018-04-27