15399

ATTUNITY
A Division of Qlik

Notice of Data Breach

Dear **[Current or Former Attunity Employee]**:

1. **What Happened?**

We are writing to notify you that, due to an inadvertent misconfiguration of cloud storage tools, back-ups of Attunity employee data were potentially accessible to the public prior to May 16, 2019. Once Attunity became aware of the Incident, Attunity swiftly remedied the situation by closing off public access to the data.

At the current stage of the investigation, while access may have been possible, there is no evidence of access of the data by any malicious third parties. Nonetheless, out of caution, we are writing to inform you of the incident. During the subsequent investigation, we have learned that the relevant data contains backups of ex-employee emails, desktop files and OneDrive files. Therefore, if you are an ex-employee and sent or stored personal data in any of these mediums, any personally identifiable information relating to you in these mediums may be impacted.

2. **What Information Was Involved?**

Based on our investigation, which is ongoing, data contained in work emails, laptops and OneDrive (e.g. Word, Excel) files may have been involved. The data may contain personal details such as your name, Social Security (or local equivalent) number, address(es), date of birth, email, financial information, health information, and information of other individuals contained on your work laptop.

3. **What Could Be the Consequences?**

At the current stage of the investigation, while access may have been possible, there is no evidence of access of the data by any malicious third parties. Nonetheless, out of caution, we are writing to inform you of the incident. If the data was to be accessed by unauthorized parties, it could expose you identity theft or fraud. If you are an ex-employee, as it was back-ups of ex-employee laptop data that was involved, and if you stored or sent personal passwords in your Attunity work email or laptop, there is a risk misuse of your online accounts (if you use the same username and/or password as the one(s) used by you while you worked at Attunity).

4. **What We Are Doing.**

We deeply regret that this incident may affect you. Attunity has taken various measures to address the incident, notably:

- We swiftly shut down public access to the data;
- We launched an investigation into the incident with the assistance of two IT forensic firms to determine the data content and likelihood of malicious access.
- We are providing you with 2 years of free credit monitoring and identity theft monitoring through Equifax ID Patrol® if you wish to use it. A description of this

product is provided in the attached material, which also contains instructions on how to enroll (including your personal activation code).

5. What You Can Do.

We encourage you to enroll in the free credit monitoring and identity theft monitoring services offered to you. While our investigation to date has not shown that any credit card or bank information was involved, to prevent unauthorized access to your online accounts, we also recommend that you immediately change your passwords for those accounts if you use the same username and/or password as the one(s) used by you while you worked at Attunity. Further, if you are an ex-employee, to the extent that you did ever use your Attunity work email or documents to store or email any personal passwords, we encourage you to change those passwords.

Please refer to the "Guide to Protecting Yourself from Identity Theft" enclosure for additional actions you can consider taking to reduce the chances of identity theft or fraud.

For More Information.

We sincerely regret any inconvenience this may cause you. If you have any additional questions or concerns, please contact me, Hadar Bloom, via email at HR_Attunity@qlik.com or via telephone at +972-9-899-3004.

Sincerely,

Hadar Bloom
VP Human Resources
Attunity, a Division of Qlik

EQUIFAX®

Enter your Activation Code: *<INSERT ACTIVATION CODE>*

Product Information

Equifax ID Patrol® provides you with the following key features:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- Automatic Fraud Alerts[2]. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).
- Credit Report Lock[3] Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning[4] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID
- Up to $1 MM in identity theft insurance[5]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/patrol

1. Welcome Page: Enter the Activation Code provided above in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept and click the "Continue" button.

4. **Verify ID**: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

[1]Credit monitoring from Experian® and Transunion® will take several days to begin.

[2]The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3]Locking your Equifax credit file with Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Global Consumer Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4]Internet scanning will scan for your Social Security number (if you choose to), up to 5 bank accounts, up to 6 credit/debit card numbers that you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet Scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guaranteed that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[5] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

ATTUNITY
A Division of Qlik

Guide to Protecting Yourself from Identity Theft

Please review the following information which will assist you incombating the possibility of identity theft or fraud.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. Remain vigilant and monitor your account statements. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Place an initial fraud alert.
- Order your credit reports.
- Create an FTC Identity Theft Affidavit by submitting a report about the theft at http://www.ftc.gov/complaint or by calling the FTC.
- File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report.
- Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from refurnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting agencies,

and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consumers Have The Right To Obtain A Security Freeze You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. See below for more details on placing a fraud alert on your credit file.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

How to Place A Security Freeze on Your Credit File. Placing, temporarily lifting, and removing a security freeze (also known as a "credit freeze") are free of charge. To place, temporarily lift, or remove a security freeze on/from your credit file, you must make a request with each of the three nationwide consumer reporting agency individually. For more information on security freezes, you may contact the three nationwide consumer reporting agencies as described below or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)

- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285 (Fraud Alert) 1-800-349-9960 (Credit Freeze)	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289 (Fraud Alert) 1-888-909-8872 (Credit Freeze)	www.transunion.com

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. You can obtain information from the Oregon Attorney General's Office about preventing identity theft. You can contact the Oregon Attorney General at:

Oregon Department of Justice
1162 Court St. NE
Salem, OR 97301
1-(877) 877-9392 (toll-free)
https://www.doj.state.or.us/

For Rhode Island Residents. You can obtain information from the Rhode Island Attorney General's Office about preventing identity theft. You can contact the Rhode Island Attorney General at:

Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov