[ADDRESS]

Dear [NAME],

Aquionix takes the privacy and security of our employees seriously. Accordingly, we are writing to inform you of a security incident that may have affected personal information you provided to us.

What Happened?

We recently discovered that the email account of one of our employees was compromised. Although we do not know the duration of the compromise, or with certainty what information may have been accessed, we have reason to believe that an unauthorized individual gained access to an employee's email account and may have received copies of emails sent from the account from approximately 2/13/2009 through 4/18/2019. As soon as we became aware of this, we immediately secured the email account and engaged a forensic IT firm to investigate the incident, and notified law enforcement. At this time, Aquionix and its investigators believe that the relevant security vulnerability has been remediated.

What Information Was Involved?

The information potentially affected by this security incident varied depending on context, for example, the content of the email and information provided by the individual, whether the individual sent or received emails during the applicable time period, or underwent a background check or employment/contractor onboarding during the applicable period. Information may include the content of background check applications or reports, tax forms, health insurance, forms, or other documentation you provided in connection with your application for employment, or in connection with the creation of your employment or contractor relationship with Aquionix. Though additional information may have been compromised, we have reason to believe that the following information may have been accessed or acquired: your first and last name; email address; mailing address; phone number; social security number. We do not have any way to determine whether the recipient of the emails actually opened or viewed the information within any of the emails.

What We Are Doing?

We have prepared the attached resources to assist you in the event that you believe you have become a victim of fraud or identity theft. In addition, although we did not discover any malware in connection with the security incident, we continue to investigate the incident, to learn more and prevent a similar issue from occurring in the future. Though the matter has been remediated, we will continue to monitor the situation closely for any additional suspicious activity. Furthermore, we have applied important security updates to our systems and taken other proactive measures to help safeguard our services and protect your personal information.

What You Can Do?

Please closely monitor your online and financial accounts and be aware that criminals may attempt to send you targeted emails seeking to obtain other confidential information from you (i.e. phishing scams), or may otherwise try to use your personal information.

Report any illegal activities to law enforcement or an appropriate government authority (see below for helpful resources). If you notice any unauthorized or suspicious financial activity, such as new credit applications, loans, or account openings, report it to the appropriate financial institution in addition to government authorities. Remember, Aquionix will never ask for your sensitive personal information via email. If you receive an email from us requesting this information, do not open any attachments and do

not provide any personal information. If you have concerns or suspicions about an email from Aquionix, please contact us at 303-289-7520.

Although it is unclear if any passwords were breached, consider taking a moment to change any old, reused, or insecure passwords and remember to follow appropriate security practices when managing your online accounts. More information on creating strong passwords can be found on the Department of Homeland Security's website: https://www.us-cert.gov/ncas/tips/ST04-002.

Identity Theft Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **August 31, 2019.** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bplus
- Provide your **activation code**:**[########]**

Additional information regarding your IdentityWorks subscription is available in the attached resources. If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **August 31, 2019.** Be prepared to provide engagement number **[########]** as proof of eligibility for the identity restoration services by Experian.

For More Information.

If you have any questions regarding this notice or if you would like more information, please do not hesitate to contact us at 303-289-7520. Most importantly, we sincerely regret any concern this security incident may cause, and we value your trust and understanding.

Sincerely,

Roy Wilson
Business Manager
Aquionix, Inc.

IMPORTANT INFORMATION ABOUT IDENTITY THEFT PROTECTION

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report, or request information on how to place a fraud alert or security freeze on your credit file, by contacting any of the national credit bureaus below. Remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. The contact information for three major credit bureaus are as follows:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19022 1-800-888-4213 www.transunion.com

Additional Details Regarding your 12-month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Contact Information for the Federal Trade Commission
In addition to the credit bureaus above, you may contact or visit the website of the Federal Trade Commission to learn more about how to protect yourself against identity theft, or how to place a fraud alert or security freeze on your credit file. The contact information for the FTC is as follows:

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

How to Place a Fraud Alert on Your Credit File
To protect yourself from the possibility of identity theft or other fraud, you may place a fraud alert on your credit file. The fraud alert helps to prevent someone else obtaining credit in your name. If you have a fraud alert on your credit file, creditors will contact you and verify your identity before they open any new accounts or change your existing accounts, but it should not affect your credit score or your ability to obtain new credit (although it may cause a delay in any applications or approvals). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts, so you do not need to place alerts with more than one of the credit bureaus. To place a fraud alert, go to any of the following links and complete the requested steps:

https://www.experian.com/fraud/center.html
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

How to Place a Security Freeze on Your Credit File
If you wish to take more extensive measures to prevent new credit being opened in your name, you may consider placing a security freeze on your credit file. You should only place a security freeze if you want to prevent most parties from obtaining your credit report and prevent all credit, loans and related services from being approved in your name without your consent. Please consider that this may also impact or delay your ability to obtain certain government services, rental housing, employment, cell phone plans, insurance, utilities, and other services.

You will need to apply for a security freeze separately with each of the credit bureaus. The requirements to obtain a security freeze vary depending on your state of residence, and you may be required to pay a fee, provide your name and social security number, copies of important identification records (including a list of addresses, copies of government issued IDs, and/or utility bills), provide an incident report if you are a victim of identity theft, or take other measures as described on the credit bureaus' websites. You may need to follow these steps for each individual (such as a spouse or dependent) who will request a security freeze. You can find more information regarding a security freeze at the following links, or by calling each of the credit bureaus at the numbers listed in this notification letter:

https://www.freeze.equifax.com
https://www.experian.com/consumer/security_freeze.html
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Contact State Government Agencies
You may also contact your state's attorney general or state department of revenue, as there may be more information available at the state level.