



13873 Park Center Road
5th Floor
Herndon VA 20171

November 4, 2021

000001



Re: Notice of Data Incident

Dear ,

We are writing to make you aware of a recent phishing incident that had some limited impact on EWA email accounts. This letter outlines what happened, what information of yours may have been affected, what measures we are taking, and steps you can take in response.


What Happened

Based on our investigation, we determined that a threat actor infiltrated EWA email on August 2, 2021. We were made aware of the situation when the threat actor attempted wire fraud. We have no reason to believe the purpose of the infiltration was to obtain personal information. Nevertheless, the threat actor's activities did result in the exfiltration of files with certain personal information (as described below).

What Information Was Involved

Based on our investigations your name and Social Security Number and/or drivers' license number appeared on files that were downloaded.

What We Are Doing

We investigated this matter thoroughly with the help of outside counsel and an experienced third-party forensics firm immediately upon discovery of the suspicious wire fraud activity. Because we take these matters seriously, although we do not have evidence that your information has been misused, we are offering you free fraud detection and identity theft protection through Equifax's Complete Premier services at no charge for two years. This product provides for credit monitoring, fraud alerts, identity restoration and up to \$1,000,000 coverage for identity theft insurance. To activate the service, visit www.equifax.com/activate and use your unique activation code, . Full details of Equifax's services and detailed instructions on how to enroll are at the end of this letter. Please remember that the deadline to enroll for this service is March 31, 2022.

What You Can Do

We encourage you to remain vigilant, including by reviewing your credit reports and financial account statements closely. We also recommend that you pay close attention to any suspicious activity that could be related to identity theft, including communications from the IRS. At the end of this letter we have described additional steps you can take to protect yourself, which include suggestions from the IRS in addressing fraud. We encourage you to review that additional information.

For More Information

If you have any questions about this matter please contact Brian McNally ((703) 904-5700).

Sincerely,



Carl N Guerreri
President, CEO and Chairman
13873 Park Center Road, 5th Floor
Herndon VA 20171



Additional Steps You Can Take to Protect Your Personal Information

Report Suspicious Activity or Suspected Identity Theft. If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at www.ftc.gov. You can also contact your state Attorney General.

If you suspect that you have been the victim of tax-related identity theft, the IRS has recommended actions you can take at their website <https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft>. This site provides instructions on what to do in the event a fraudulent return is filed in your name or in the name of one of your dependents, including responding to IRS notices you receive and how to handle potential fraudulent tax filings made in your name see (www.irs.gov/individuals/instructions-for-requesting-copy-of-fraudulent-returns).

Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, by sending an email to idtheft@oag.statemd.us, or by calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, NC 27699.

Credit Reports/Fraud Alerts/Credit and Security Freezes: Under federal law, you are entitled to one free copy of your credit report every 12 months. You can request a free credit report once a year at www.annualcreditreport.com, by calling (877) 322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. There may be a fee for this service based on state law. To put a security freeze on your credit file contact the consumer reporting agencies listed below.

You may also contact the three U.S. credit reporting agencies as follows:

Agency	Credit Report Contact	Fraud Alert Contact	Credit/Security Freeze Contact
TransUnion LLC	Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016; (800) 888-4213; https://www.transunion.com/#	TransUnion Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19016; (800) 680-7289; https://www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 160, Woodlyn, PA 19094; (888) 909-8872; https://www.transunion.com/credit-freeze/
Experian	P.O. Box 2002, Allen, TX 75013; (888) 397-3742; https://www.experian.com/consumer-products/free-credit-report.html	Experian, P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/fraud-center.html	P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/freeze-center.html
Equifax Information Services LLC	P.O. Box 740241, Atlanta, GA 30348-0241; (800) 685-1111; https://www.equifax.com/personal/credit-report-services/	Equifax, P.O. Box 105069, Atlanta, GA 30348-5069; (800) 525-6285; www.equifax.com/fraud-alerts	P.O. Box 105788, Atlanta, GA 30348-5788; (888) 298-0045 www.equifax.com/freeze

Equifax Credit Monitoring: The product is available to individuals over 18, and provides access to your 3-bureau credit report, daily access to your Equifax credit report, and more. Also included are WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites as well as automatic fraud alerts² which encourage potential lenders to take extra steps to verify your identity before extending credit. To enroll go to www.equifax.com/activate and include the unique activation code that was provided in this letter. You will need to follow the onscreen instructions to register, complete and account, and will be prompted to verify your identity. At the end you will see a checkout page where you simply need to click “sign me up” to finish the process. You can access your products using “view my product” features.

IRS Identity Protection PIN: The IRS offers an Identity Protection PIN, which is a six digit number that prevents someone else from filing a tax return using your Social Security number. The Identity Protection PIN is known only to you and the IRS. For more information and to obtain an Identity Protection PIN, please visit the IRS website at www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

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