23512

Olympus Corporation of the Americas
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

OLYMPUS

«Full_Name» «ID»
«Address_1»
«Address_2»
«Address_3»
«City», «State» «Zip», «Address_Country»

November 12, 2021

Dear «Full_Name»:

We are writing to notify you that our recent data security incident may have had an impact on some of your personal information. This letter is being sent to provide you with additional information and to advise you of services Olympus Corporation of the Americas ("OCA") is offering at no charge to you to help protect your continued privacy.

It is important to note that we have no evidence that your personal information has been used inappropriately, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to protect your continued privacy.

Unfortunately, these types of incidents are becoming common. They are frustrating and disruptive to organizations like ours and our employees. Despite our regular monitoring, vigilance, and prevention measures, this incident occurred, and we are working hard to ensure this does not happen again.

What Happened?

On October 10, 2021, OCA discovered suspicious activity on its network system that we have since confirmed to be a data security incident. Our investigation revealed that an unauthorized third-party gained access to OCA systems, and certain files that contained confidential company and employee information were corrupted and rendered unavailable in an attempt to disrupt our systems. There is no evidence that any unauthorized person viewed or accessed the employee data. Nor is there any evidence that the employee data was taken from our system, is in the possession of any unauthorized person, or has been disclosed publicly or on the Internet. We will continue to monitor for any such disclosure and will promptly notify you if any of your personal information is disclosed or published in that way.

What Information Was Involved?

The corrupted files likely included personal information, such as your name, address, social security number / social insurance number, and details of your participation in OCA's retirement programs. While there is no evidence that the data has been accessed by an unauthorized person or used in an unauthorized way, we did want to make you aware of the situation out of an abundance of caution given the nature of this information.

What We Are Doing

Immediately upon learning of this incident, we launched an investigation and recovery effort with the assistance of cyber experts and law enforcement. Determining whether information was compromised in any way was one of the top priorities of this effort so that we could notify potentially affected

individuals. Rest assured, we are also making increased efforts to improve our information security to prevent incidents like this from occurring in the future.

To help protect your identity, we have arranged to offer a complimentary two-year subscription to Experian IdentityWorks SM credit monitoring and identity theft protection. To activate your membership and start monitoring your credit and the use of your personal information:

- Ensure that you **enroll by «CM_Date»** (Your code will not work after this date).
- **Visit** the Experian IdentityWorks SM website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code: «CM_Code»**

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 877-288-8057. Be prepared to provide engagement number **«ENG_No»** as proof of eligibility for the identity restoration services by Experian.

What You Can Do

To help protect your personal information, we strongly recommend you take the following steps:

- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS) or Canada Revenue Agency (CRA). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number / social insurance number to establish credit and to block that credit from being established if you were not the one who initiated it.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this incident, please call 1-888-597-6901 from 8:00 AM to 5:00 PM Eastern Time. We have also included a **Frequently Asked Questions** section of this letter to address likely questions.

Please know that OCA takes this matter very seriously, and we apologize for any concern and inconvenience this may cause you.

Sincerely,

Stacey Morey
Vice President, Human Resources
Olympus Corporation of the Americas

@2

FREQUENTLY ASKED QUESTIONS

Q: What Happened?
A: As you likely know, on October 10, 2021, Olympus Corporation of the Americas ("OCA") discovered suspicious activity on its network system that we have since confirmed to be a data security incident. Our ongoing investigation has revealed that confidential company and employee information was likely compromised. We are working with appropriate technical forensic experts and law enforcement authorities on this situation and will continue to take all necessary measures to serve our employees and customers in a secure way.

Q: Is the Olympus network environment safe?
A: The recovery effort continues, but we are confident that our network systems are secure, and the threat has been contained. In addition, we have taken further steps to enhance our security measures going forward.

Q: How many employees are impacted? Are former employees impacted?
A: Given the nature of the incident, Olympus does not have sufficient information to determine the type of data involved or how many employees or former employees may be affected. Out of an abundance of caution, this notice was sent to all current and former employees dating back seven years of Olympus Corporation of the Americas.

Q: Are Olympus customers affected by this incident?
A: As part of our containment measures, we have taken significant steps to safeguard our customers, their assets and information. While Olympus' environment was affected, we have no reason to believe that our customers' environments have been or will be affected. If investigations uncover that a customer or business partner's environment was affected or data was involved in a way that calls for us to provide notification, we will do so.

Q: Why are you contacting me now?
A: As noted previously, immediately upon learning of this incident, we launched an investigation and recovery effort with the assistance of cyber experts and notified law enforcement. Once we determined that certain confidential company and employee information may have been compromised, we moved to provide notice regarding the incident.

Q: Is my laptop and information I store on my laptop also compromised?
A: Any information on your laptop, which may include certain personal information stored within files or web browsers, may have been compromised in this incident. We recommend you follow the steps outlined in the letter to protect your personal information.

Q: Do you know who is responsible for this incident?
A: While we cannot comment further on the details of the incident, we can say that we are working with technical forensic experts and law enforcement authorities in the ongoing investigation.

Q. Do I need to change my passwords?
A. We encourage you to follow the steps outlined in this letter to protect your personal information, but you may elect to take any additional action you feel is appropriate, including changing passwords to certain websites.

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Place 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 a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.