Return Mail Processing
PO Box 999
Suwanee, GA 30024

8 1 1981 ******************************MIXED WKG
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

August 7, 2026

NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to inform you of a data security incident involving certain personal data relating to you. This letter explains what happened, the categories of personal data involved, the steps we have taken or are taking in response, the measures you may wish to take to protect yourself, and how you can contact us for further information. We want to assure you that we are taking this matter very seriously and sincerely regret any concern it may cause you.

What Happened?

On April 29, 2026, Cushman & Wakefield became aware of unauthorized access to its data by a third party, who we determined was able to exfiltrate certain files. Upon becoming aware of the incident, Cushman & Wakefield promptly undertook a diligent review to determine what personal data may have been affected. This comprehensive review involved the analysis of a substantial volume of data and files to accurately determine the individuals whose personal data was affected and the nature of the information involved. That review identified that certain personal data relating to you was accessed and exfiltrated by the unauthorized third party.

What Information Was Involved?

Based on our investigation to date, we believe that there may have been unauthorized access to your name and [Extra2]. We have seen no indication that any of your personal information was actually viewed by an unauthorized third party. Further, we have seen no indication that any of your personal information has been misused. However, out of an abundance of caution, we are notifying you of this incident and providing you resources (described below and in the attached "Additional Resources" document).

What We Are Doing

Upon learning of this incident, we took immediate action to investigate the incident and secure our network with the assistance of third-party cybersecurity experts. We performed a broad-based reset of system passwords and access credentials, and we have implemented heightened monitoring across our environment.

We continue to monitor for any indication of misuse of the affected personal data and will take further remedial action where necessary. We have notified law enforcement to ensure the incident is properly addressed. We are also notifying you so that you can take the steps recommended below.

What You Can Do

We recommend that you remain alert for any suspicious activity involving your personal data. Depending on the personal data affected, you may wish to take precautions such as carefully reviewing unexpected communications or requests, avoiding the disclosure of personal or identification information unless you are satisfied that the request is legitimate, changing passwords or security credentials if these used elements of the personal data involved, contacting the relevant organization or authority if you identify anything suspicious, and, where official identification data was affected, following any applicable guidance from the issuing authority regarding monitoring, replacement, or additional protective steps. We also recommend that you remain vigilant and take steps to protect against identity theft or fraud, including monitoring your accounts and credit reports for signs of suspicious activity. Information about how to obtain a free credit report, security freezes, and other guidance is provided in the attached "Additional Resources" document, which we encourage you to review.

Although we have no indication that your personal information has been misused to commit fraud or identity theft, to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 24 months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 30, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/1Bcreditmembership
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by November 30, 2026 at 833-918-6825 Monday - Friday, 8 am - 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 file for indicators of fraud.
- **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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information

If you have questions regarding this service or need additional information, please call 833-918-6825 toll-free Monday through Friday from 8 am to 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number].

We regret that this incident occurred and take the protection of personal data seriously. We are committed to addressing this matter and to taking appropriate steps to protect the personal data entrusted to us.

Sincerely,

Cushman & Wakefield
225 West Wacker, Suite 3000
Chicago, IL 60606

Enclosures

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL RESOURCES

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.Equifax.com	http://www.Experian.com	Chester, PA 19022-2000
		www.transunion.com

Free Credit Report. Under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the FTC website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Maine, Maryland, Massachusetts, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

You also have other rights under the FCRA. For information about your rights under the FCRA, please visit:

- http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf; or
- www.ftc.gov.

You may also obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

Fraud Alerts. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. You can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. After receiving your request, the credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze in the future. You should keep the PIN or password in a safe place.

State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC (using the contact methods listed above) and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

- ***For Connecticut residents**:* You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5420, www.ct.gov/ag.
- ***For District of Columbia residents:*** You may contact the District of Columbia Attorney General's Office, 400 6th Street NW, Washington, DC 20001, 1-202-727-3400, http://oag.dc.gov.
- ***For Maryland residents**:* You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://oag.maryland.gov/, 1-888-743-0023.
- ***For Massachusetts residents:*** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. Under Massachusetts law, you have the right to obtain any police report filed in connection with this incident.
- ***For New York residents**:* You may contact the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, 1-800-771-7755. You may also contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.
- ***For North Carolina residents**:* You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
- ***For Oregon residents:*** Oregon residents are advised to report any suspected identity theft to law enforcement, the FTC, and the Oregon State Office of the Attorney General; https://www.doj.state.or.us/, 1-877-877-9392, 1162 Court Street NE, Salem, OR 97301-4096.
- ***For Rhode Island residents***: You may contact the Rhode Island Office of the Attorney General; www.riag.ri.gov, 1-401-274-4400, 150 South Main Street, Providence, Rhode Island 02903. In Rhode Island you may file or obtain a police report.