

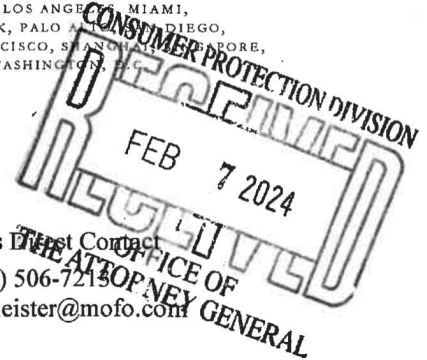
MORRISON FOERSTER

250 WEST 55TH STREET
NEW YORK
NEW YORK 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP
AUSTIN, BEIJING, BERLIN, BOSTON,
BRUSSELS, DENVER, HONG KONG,
LONDON, LOS ANGELES, MIAMI,
NEW YORK, PALO ALTO, SAN DIEGO,
SAN FRANCISCO, SINGAPORE, SUIZHORN,
TOKYO, WASHINGTON, D.C.



Writer's First Contact
+1 (212) 506-7215
mwugmeister@mofo.com

February 5, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

On behalf of The UPS Store, Inc. ("The UPS Store"), I am writing to inform you about an incident that involved six independently owned and operated The UPS Store franchise locations and covered personal information relating to three (3) Maryland residents.

On November 3, 2023, The UPS Store determined that an unauthorized third party accessed store-specific email accounts, operated by six individual The UPS Store franchisees, between November 1, 2023 and November 2, 2023.

As soon as The UPS Store became aware of this activity, The UPS Store began an investigation to determine the nature and scope of the incident and took measures to terminate the unauthorized access and designed to prevent future unauthorized access. As part of the investigation, The UPS Store used a dedicated review team to conduct a detailed review and analysis of the relevant email accounts. This review was completed on January 5, 2024.

Through the investigation, The UPS Store determined that the covered personal information relating to three (3) Maryland residents involved in this incident was information contained in emails with a The UPS Store franchise location, many of which were for document printing, scanning, or other services provided by The UPS Store franchise location.

The UPS Store will notify the three (3) Maryland residents of this incident on February 5, 2024. The UPS Store will provide these individuals with an offer for two years of complimentary credit and identity monitoring services, which include, among other things, credit monitoring, identity theft protection, and resolution services, and up to \$1 million in identity fraud loss reimbursement.

Attached is a sample of the letter that The UPS Store is providing to the relevant Maryland residents.

Please do not hesitate to contact me if you have any questions regarding this letter.

Sincerely,

Miriam H. Wugmeister

Attachment

The UPS Store, Inc.
6060 Cornerstone Ct W
San Diego, CA 92121

February 5, 2024

Notice of Data Breach

Dear <first name> <last name>,

We are writing to inform you about an incident relating to six The UPS Store franchise locations that involved personal information about you. We wanted to alert you to this incident and make you aware of how we are responding and the steps you can take to protect yourself, including by enrolling in the complimentary credit monitoring and identity theft monitoring and restoration services described in this letter.

WHAT HAPPENED. On November 3, 2023, we determined that an unauthorized third party accessed store-specific email accounts, operated by individual The UPS Store franchisees, between November 1, 2023 and November 2, 2023. As soon as we became aware of this activity, we began an investigation to determine the nature and scope of the incident and took measures to terminate the unauthorized access. As part of the investigation, we used a dedicated review team to conduct a detailed review and analysis of the relevant email accounts. This review was completed on January 5, 2024.

WHAT INFORMATION WAS INVOLVED. The personal information about you involved in this incident was information contained in emails with a The UPS Store franchise location, many of which were for document printing, scanning, or other services provided by The UPS Store franchise location. This information may have included your name and Social Security number, driver's license or other government-issued ID number, financial account or payment card number, health insurance policy number, date of birth, and/or health information.

WHAT WE ARE DOING. As noted above, we began investigating the incident as soon as we learned of it and took quick and proactive measures to restrict access to the email accounts involved and designed to prevent future unauthorized access. We conducted a detailed review and analysis of the relevant emails to determine whether personal information was accessed without authorization. We are providing you with this letter to alert you to the incident and provide you with an offer for complimentary credit monitoring.

WHAT YOU CAN DO. We are providing you with the following information about steps that you can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary two-year credit monitoring service. We have engaged Equifax to provide you with its credit and identity monitoring services, which include, among other things, credit monitoring, identity theft protection, and resolution services, and up to \$1 million in identity fraud loss reimbursement. You have until April 30, 2024 to activate the free credit monitoring service by using the following activation code: <Code>. This code is unique for your use and should not be shared. To enroll, visit www.equifax.com/activate.

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, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 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. In addition, under federal law, 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 by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
www.TransUnion.com

You also have other rights under the Fair Credit Reporting Act (FCRA). For information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. 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.

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 containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION. Protecting the personal information of customers is one of our highest priorities, and we sincerely apologize for any inconvenience or concern this incident may cause. You may contact us at (858) 597-8526 Monday through Friday from 7AM to 5PM Pacific Time (excluding major U.S. holidays) if you have any questions or concerns.

Sincerely,
The UPS Store

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
<https://oag.dc.gov/>

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

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

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

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

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor Suite 650
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE A RHODE ISLAND RESIDENT: You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov/>