King & Spalding

King & Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737
www.kslaw.com

Scott Ferber
Partner
Direct Dial: +1 202 626 8974
Direct Fax: +1 202 626 3737
sferber@kslaw.com

January 20, 2020

BY EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
securitybreach@atg.wa.gov

Re: Data Security Incident

Dear Attorney General Ferguson,

On behalf of The UPS Store, Inc. (TUPSS), I write to inform you of the recent discovery of a data security incident and to explain the steps the company is taking to address the incident, including notifying potentially impacted individuals and providing them ways with which to protect their personal information.

Between approximately September 29, 2019 and January 13, 2020, a small percentage of local store locations were the victim of a phishing incident in which an unauthorized person potentially had access to a limited number of local store email accounts. Immediately upon discovering this incident, TUPSS initiated an investigation to assess the incident's scope, including engaging a third-party cybersecurity firm, and has taken steps to further strengthen and enhance the security of systems in the TUPSS network, including updating administrative and technical safeguards. Based on its investigation to date, TUPSS has found personal information in the potentially affected accounts associated with what appear to be approximately 876 residents. The personal information was in documents that were emailed to store locations for printing or similar services provided by those locations. We are currently unaware of fraud or misuse concerning the personal information in those accounts.

Although our investigation into the matter is ongoing, TUPSS is proactively alerting this Office and the potentially impacted state residents out of an abundance of caution. We are providing the identified residents with complimentary credit monitoring and identify theft restoration services from Experian for 24 months. We also have established a call center to answer consumer questions. We are working expeditiously to complete the investigation within the next 90 days and will promptly notify any other potentially impacted state residents that are identified.

An unaddressed copy of the individual notification letter, which will be mailed on January 21, 2020, is attached as Exhibit A. We also are notifying consumer credit reporting agencies Equifax, Experian, and TransUnion. In addition, we have contacted law enforcement and intend to cooperate with any investigation.

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

Very truly yours,

Scott Ferber

Attachment

The UPS Store

6060 Cornerstone Court West
San Diego, CA 92121

January 21, 2020

F2730-L01-0000001 P001 T00002 **********MIXED AADC 159
SAMPLE A SAMPLE - ALL STATES
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Re: **Important Security Notification**
Please read this letter.

Dear Sample A Sample:

We are contacting you regarding a security incident that may have involved some of your personal information. We take the privacy and security of your personal information very seriously and for this reason want you to understand what we are doing to address this issue and what steps you can take to protect yourself. This letter explains what happened and offers assistance in protecting against potential identity theft. Although we have no information at this time that would indicate that your personal information has been used in an unauthorized manner, we are offering you complimentary credit monitoring and identity theft restoration services described in this letter.

What Happened

Between approximately September 29, 2019 and January 13, 2020, a small percentage of The UPS Store, Inc. local store locations were the victim of a phishing incident in which an unauthorized person potentially had access to a limited number of local store email accounts. Immediately upon discovering this incident, The UPS Store, Inc. initiated an investigation to assess the incident's scope, including engaging a third-party cybersecurity firm, and has taken steps to further strengthen and enhance the security of systems in The UPS Store, Inc. network, including updating administrative and technical safeguards. As part of the investigation, The UPS Store, Inc. reviewed the potentially affected accounts and found personal information in those accounts. The personal information was contained in documents that were emailed to the local store location for printing or similar services provided by those locations. You, or someone you know, may have emailed the document(s) containing personal information to the local store for this service. We are unaware of any misuse of your personal information in connection with this incident at this time.

What Information Was Involved

Based on the investigation, some of your personal information was in documents that were emailed to the accounts. Depending on the document(s) sent, this information may have included your name and one or more of the following

What We Are Doing

As part of our ongoing investigation, we have taken steps to further strengthen and enhance the security of systems in the network, including updating administrative and technical safeguards. We have also engaged a third-party cybersecurity firm to assist with our review and have notified law enforcement authorities and intend to cooperate with any investigation.

What You Can Do

We are currently unaware of fraud or misuse concerning the personal information in those accounts. As an added precaution, to help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠, which provides you with 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 April 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **ABCDEFGHI**

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 **855-776-8286** by **April 30, 2020.** Be prepared to provide engagement number **DB16539** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-month Experian Identity Works 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.
- **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 **855-776-8286**. 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 two years 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.

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. If you have any questions regarding this incident, please call **855-776-8286** toll-free Monday through Friday from 8 am – 10 pm Central or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,
The UPS Store

* 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

Reference Guide

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian and TransUnion) provide free annual credit reports only through the website, toll-free number or request form.

You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
888-766-0008	888-397-3742	800-680-7289

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in Free Credit Monitoring and Identity Restoration Services with Experian IdentityWorks

We encourage you to contact Experian with any questions at 855-776-8286 Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central Saturday and Sunday (excluding major U.S. holidays), and to enroll in free IdentityWorks services by going to https://www.experianidworks.com/3bcredit and using the Enrollment Code provided above. Please note that the deadline to enroll is **April 30, 2020**.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the FTC. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Placing a Security Freeze

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

https://www.equifax.com/personal/credit-report-services/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert

To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

MARYLAND RESIDENTS

You may obtain information about avoiding identity theft at:

Office of the State of Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

NORTH CAROLINA RESIDENTS

You may obtain information about avoiding identity theft at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
919-716-6400
www.ncdoj.gov

NEW MEXICO RESIDENTS

The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

RHODE ISLAND RESIDENTS

We first learned about a possible data security incident on December 23, 2019. Based on the investigation, personal information for eight Rhode Island residents was in documents sent to the potentially affected accounts. You may obtain information about avoiding identity theft at:

Office of the State of Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
401-274-4400
www.riag.ri.gov