



The UPS Store

Corporate Headquarters
6060 Cornerstone Court
W San Diego, CA 92121

August 20, 2014

To Our Valued Customers:

The UPS Store, Inc. ("The UPS Store"), among many other U.S. retailers, recently received a government bulletin regarding a broad-based malware intrusion targeting retailers in the United States. Upon receiving the bulletin, we retained an IT security firm and conducted a review of our systems and the systems of our franchised center locations. We discovered the malware present at 51 locations in 24 states (about 1%) of 4,470 franchised center locations throughout the United States. As part of our response to this incident, we have implemented various system enhancements and antivirus updates.

Based on our current assessment, we believe that information of The UPS Store customers who made credit and debit card purchases at the impacted franchised center locations between January 20, 2014 and August 11, 2014 may have been exposed. For some center locations, the period of exposure to this malware began after January 20, 2014. The malware was eliminated as of August 11, 2014 and you can shop securely at The UPS Store. The customer information that may have been exposed includes customers' names, postal addresses, email addresses and payment card information. Not all of this information may have been exposed for each customer.

Your trust is important to us. Based on the investigation, we feel it is critical to notify our customers of the potential data compromise. We are offering identity protection and credit monitoring services to those customers who made a purchase at one of the impacted locations during the applicable time period. To learn more about identity protection and credit monitoring services and for further information on the impacted store locations, as well as the timeframe for potential exposure to this malware at impacted locations, please visit <https://theupsstore.allclearid.com>.

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe your credit or debit card was impacted by this incident, you should immediately contact your payment card issuer or bank.

If you have any additional questions, please call us at 1-855-731-6016.

Please know we take our responsibility to protect customer information seriously and have committed extensive resources to addressing this incident. We understand this type of incident can be disruptive and apologize for any anxiety this may have caused.

Sincerely,

A handwritten signature in black ink, appearing to be "Tim Davis", written over a horizontal line.

Tim Davis
President, The UPS Store, Inc.

Additional Information

We encourage The UPS Store customers to take the following steps:

Order Your Free Credit Report. To order your free 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 provide free annual credit reports only through the website, toll-free number or request form.

We recommend that you remain vigilant by reviewing your credit reports. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your 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 in this information 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. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Reporting Incidents. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement or your state Attorney General. If you believe your 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 contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Identity Protection Services. The UPS Store has arranged with AllClear ID to offer affected customers identity protection and credit monitoring services at no cost to them. The following identity protection services start on the date of this notice and you can use them at any time during one calendar year following notification of this incident.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. This protection is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-731-6016 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring. For a child under 18 years old, AllClear ID ChildScan identifies fraud by searching various databases for evidence of misuse of the child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-731-6016 using the redemption code received when registering for the AllClear PRO service. Please note: Additional steps may be required by you in order to activate your phone alerts. The UPS Store has arranged with AllClear ID to offer affected customers identity protection services and credit monitoring at no cost to them. Customers who believe they may have been impacted are encouraged to visit <https://theupsstore.allclearid.com> for further information about these services.

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

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit bureaus without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. For more information on security freezes, you may contact the three nationwide credit bureaus or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three nationwide credit bureaus to find out more information.

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
ww.ncdoj.gov

The UPS Store®

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

August 20, 2014

[First_Name] [Last_Name]
[Address_Line_1]
[Address_Line_2]
[City], [State] [Zip]

Dear [First_Name] [Last_Name],

We are writing to notify you of an incident that involves certain of your personal information. The UPS Store, Inc. ("The UPS Store"), among many other U.S. retailers, recently received a government bulletin regarding a broad-based malware intrusion targeting retailers in the United States. The UPS Store discovered malware identified in the bulletin on systems at 51 locations in 24 states (about 1%) of 4,470 franchised center locations throughout the United States. Upon receiving the bulletin, The UPS Store retained an IT security firm and conducted a review of its systems and the systems of its franchised center locations. As part of its response to this incident, The UPS Store has implemented various system enhancements and antivirus updates.

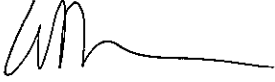
Based on the current assessment of The UPS Store and the IT security firm, we believe that certain personal information you provided in connection with establishing a MailBox Manager account at one of the impacted franchised center locations between January 20, 2014 and August 11, 2014 may have been exposed. For some center locations, the period of exposure to this malware began after January 20, 2014. The malware was eliminated as of August 11, 2014 and no longer presents a threat for customers shopping at The UPS Store locations in the United States. The customer information that may have been exposed in connection with the MailBox Manager accounts includes customers' names, postal addresses, Social Security numbers and driver's license numbers. In addition, we believe that your name, postal address, email address and payment card information may have been exposed to the extent you made credit or debit card purchases at the impacted franchised center locations during the same time period. Not all of this information may have been exposed for each customer. Based on the investigation, we think it is appropriate to notify you of the potential for data loss.

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe your credit or debit card was impacted by this incident, you should immediately contact your payment card issuer or bank. Because we value our The UPS Store customers, we are offering identity protection and credit monitoring services to you. To learn more about identity protection and credit monitoring services and for further information on the impacted store locations, as well as the timeframe for potential exposure to this malware at impacted locations, please visit <http://www.theupsstore.com> and <https://theupsstore.allclearid.com>. The attached Reference Guide provides additional information on registration and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

If you have any additional questions, please call us at 1-877-403-0238.

Please know we take our responsibility to protect customer information seriously and have committed extensive resources to addressing this incident. We apologize for any inconvenience caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to be 'TD', with a long horizontal line extending to the right.

Tim Davis
President, The UPS Store.

Reference Guide

We encourage The UPS Store customers to take the following steps:

Order Your Free Credit Report. To order your free 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 provide free annual credit reports only through the website, toll-free number or request form.

We recommend that you remain vigilant by reviewing your credit reports. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your 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 in this information 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. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Reporting Incidents. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement or your state Attorney General. If you believe your 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 contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Identity Protection Services. The UPS Store has arranged with AllClear ID to offer affected customers identity protection and credit monitoring services at no cost to them. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. This protection is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-403-0238 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring. For a child under 18 years old, AllClear ID ChildScan identifies fraud by searching various databases for evidence of misuse of the child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-403-0238 using the following redemption code: [Redemption_Code].

Please note: Additional steps may be required by you in order to activate your phone alerts.

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

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit bureaus without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. For more information on security freezes, you may contact the three nationwide credit bureaus or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three nationwide credit bureaus to find out more information.

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
ww.ncdoj.gov

The UPS Store®

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

August 20, 2014

[First_Name] [Last_Name]
[Address_Line_1]
[Address_Line_2]
[City], [State] [Zip]

Dear [First_Name] [Last_Name],

We are writing to notify you of an incident that involves certain of your personal information. The UPS Store, Inc. ("The UPS Store"), among many other U.S. retailers, recently received a government bulletin regarding a broad-based malware intrusion targeting retailers in the United States. The UPS Store discovered malware identified in the bulletin on systems at 51 locations in 24 states (about 1%) of 4,470 franchised center locations throughout the United States. Upon receiving the bulletin, The UPS Store retained an IT security firm and conducted a review of its systems and the systems of its franchised center locations. As part of its response to this incident, The UPS Store has implemented various system enhancements and antivirus updates.

Based on the current assessment of The UPS Store and the IT security firm, we believe that the login credentials you provided as a franchise owner in connection with accessing The UPS Store accounts at one of the impacted franchised center locations between January 20, 2014 and August 11, 2014 may have been exposed. For some center locations, the period of exposure to this malware began after January 20, 2014. The malware was eliminated as of August 11, 2014 and no longer presents a threat for impacted franchise owners. Based on the investigation, we think it is appropriate to notify you of the potential for data loss.

We encourage you to promptly change your user name and password to access all The UPS Store accounts. In addition, you should remain vigilant by reviewing your account statements and monitoring your free credit reports. We are offering identity protection and credit monitoring services to you. To learn more about identity protection and credit monitoring services and for further information on the impacted store locations, as well as the timeframe for potential exposure to this malware at impacted locations, please visit <http://www.theupsstore.com> and <https://theupsstore.allclearid.com>. The attached Reference Guide provides additional information on registration and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

If you have any additional questions, please call us at 1-877-403-0238.

Please know we take our responsibility to protect personal information seriously and have committed extensive resources to addressing this incident. We apologize for any inconvenience caused by this incident.

Sincerely,



Tim Davis
President, The UPS Store.

Reference Guide

We encourage The UPS Store franchise owners receiving this August 20, 2014 letter to take the following steps:

Order Your Free Credit Report. To order your free 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 provide free annual credit reports only through the website, toll-free number or request form.

We recommend that you remain vigilant by reviewing your credit reports. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your 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 in this information 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. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Reporting Incidents. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement or your state Attorney General. If you believe your 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 contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Identity Protection Services. The UPS Store has arranged with AllClear ID to offer affected franchise owners identity protection and credit monitoring services at no cost to them. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. This protection is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-403-0238 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring. For a child under 18 years old, AllClear ID ChildScan identifies fraud by searching various databases for evidence of misuse of the child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-403-0238 using the following redemption code: [Redemption_Code].

Please note: Additional steps may be required by you in order to activate your phone alerts.

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

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit bureaus without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. For more information on security freezes, you may contact the three nationwide credit bureaus or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three nationwide credit bureaus to find out more information.

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

Impacted Franchised Center Locations in California

UPS Store Address	City	Zip Code	Malware Intrusion Date	Secure Transactions Date
1608 W. Campbell Ave.	Campbell	95008	7/1/2014	8/11/2014
25A Crescent Drive	Pleasant Hill	94523	4/29/2014	8/11/2014
3419 E. Chapman Ave.	Orange	92869	4/29/2014	8/11/2014
3230 Arena Blvd., Ste. 245	Sacramento	95834	4/29/2014	8/11/2014