November 14, 2019

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

To Whom It May Concern:

On behalf of Macy's, Inc., I am writing to inform you about a recent incident in which certain information relating to Washington residents was accessed by an unauthorized third party.

On October 15, 2019, we were alerted to a suspicious connection between macys.com and another website. Our security teams immediately began an investigation. Based on our investigation, we believe that on October 7, 2019 an unauthorized third party added unauthorized computer code to two (2) webpages on macys.com. The unauthorized code was highly specific and only allowed the third party to capture information submitted by customers on the following two (2) macys.com webpages: (1) the checkout webpage - if payment card data was entered on the webpage and the "place order" button was hit; and (2) the wallet webpage - accessed through the My Account feature – if payment card data was entered. Our teams successfully removed the unauthorized code on October 15, 2019.

The information the cybercriminals potentially accessed were the following data elements if entered by the customer on either the macys.com checkout webpage or on the My Account wallet webpage: First Name; Last Name; Address; City; State; Zip; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; Payment Card Month/Year of Expiration. Customers checking out or interacting with the My Account wallet page on a mobile device or on the macys.com mobile application were not involved in this incident.

After identifying the suspicious connection, our security teams, as well as an IT security forensics firm, investigated. In addition to removing the unauthorized code, we increased monitoring for macy's.com, added outbound traffic blocking from the site and implemented additional controls. We also notified the FBI and US Secret Service of the event on October 17.

We will be mailing letters regarding this incident to 3,810 Washington residents beginning on November 14, 2019. We are providing these individuals with an offer for complimentary Experian IdentityWorks dark web scanning and identity repair services. These individuals can enroll in Experian services by calling a dedicated line or enrolling on the Experian website, using the contact information included in the letter (a sample of which is provided in the addendum).

Please do not hesitate to contact me at 513-579-7803 if you have any questions. I also can be reached at 7 West 7th Street, Cincinnati, OH 45202 and at michael.mccullough@macys.com.

Sincerely,

Michael McCullough
CPO & Data Risk, Macy's Inc.

ATTM: (1)

ATTACHMENT 1: *Sample Customer Notice of Data Breach Letter*

NOTICE OF DATA BREACH

November 14, 2019

Dear <Sample Customer>:

On behalf of Macy's, we are writing to inform you about a recent incident involving unauthorized access to personal information about you on macys.com. We regret that this incident occurred and appreciate your time to read this letter.

WHAT HAPPENED?

On October 15, 2019, we were alerted to a suspicious connection between macys.com and another website. Our security teams immediately began an investigation. Based on our investigation, we believe that on October 7, 2019 an unauthorized third party added unauthorized computer code to two (2) pages on macys.com. The unauthorized code was highly specific and only allowed the third party to capture information submitted by customers on the following two (2) macys.com pages: (1) the checkout page - if credit card data was entered and "place order" button was hit; and (2) the wallet page - accessed through My Account. Our teams successfully removed the unauthorized code on October 15, 2019.

The following provides additional information relating to this unfortunate event, including consumer protection options available to you. Payment card rules generally provide that cardholders are not responsible for fraudulent purchases on their payment cards so long as they report those transactions to their card issuers in a timely manner. Please be aware that Macy's will never ask you by phone, email, or text for your macys.com password or security question answers.

WHAT INFORMATION WAS INVOLVED?

Information the cybercriminals potentially accessed include: First Name; Last Name; Address; City; State; Zip; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; Payment Card Month/Year of Expiration *if* the values for these items were typed into the webpage while on either the macys.com checkout page or in the My Account wallet page. Customers checking out or interacting with the My Account wallet page on a mobile device or on the macys.com mobile application were not involved in this incident.

WHAT ARE WE DOING?

We immediately began an investigation as soon as we suspected a problem. We quickly contacted federal law enforcement and brought in a leading class forensics firm to assist in our investigation. We have reported the relevant payment card numbers to the card brands (i.e. Visa, Mastercard, American Express, and Discover). In addition, we have taken steps that we believe are designed to prevent this type of unauthorized code from being added to macys.com.

There is no reason to believe that this incident could be used by cybercriminals to open new accounts in your name. Nonetheless, you should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your account statements and immediately reporting any suspicious activity to your card issuer. You may also contact your card issuer and inform them that your card information may have been compromised. Your card issuer can suggest appropriate steps to protect your account. Payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

CUSTOMER PROTECTION

We at macys.com value our client relationship, appreciate your business and would like to provide as much assistance as we can. Therefore, as an added precaution, we have arranged to have Experian IdentityWorks℠ to provide you with its identity protection services for 12 months at no cost to you. These services are available to you as of the date of this letter. You can use the services at any time during the next 12 months. The activation code for these services is unique for your use only and should not be shared.

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 creditors 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).

Please note that Identity Restoration is available to you for 12 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 12-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, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/identity
- 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 at 855-557-2999 by November 30, 2020. Be prepared to provide engagement number DB16331 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 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:

- Internet Surveillance: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- 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[i]: Provides coverage for certain costs and unauthorized electronic fund transfers.

CONTACTING THE FEDERAL TRADE COMMISSION, LAW ENFORCEMENT & THE CREDIT BUREAUS

In addition, you may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, 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.consumer.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. 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 the 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 by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.equifax.com	www.experian.com	Chester, PA 19022
		www.transunion.com

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_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 protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three 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. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

Equifax – (800) 349-9960 Experian – (888) 397-3742 TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our support agents for this event at 800-222-3314 if you have any questions or concerns.

Sincerely,

Macys.com Customer Service

[i] 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.