July 2, 2018

Bob Ferguson
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.

Specifically, on June 11, 2018, our security suite alerted us to a spike in anomalous login activities on macys.com and bloomingdales.com. Our investigation showed that, beginning on or about April 26, 2018 through our remediation on June 12, the attacker used valid user credentials (user names and passwords) to login to some online profiles. Importantly, there is no evidence of compromise of Macy's systems containing login credentials, and we believe valid login credentials were stolen from another company and/or sourced from the dark web.

On June 11, 2018, Macy's Information Security teams identified the attack pattern definition by testing the attacker's scripts. The traffic pattern matching the script signature was blocked within six (6) hours of pattern validation as a temporary mitigation. Within 24 hours on June 12, we blocked access to the relevant customer profiles, purged all payment card data from the profiles and blocked the profiles until our customers changed their passwords.

Based on our investigation, we believe the attacker accessed certain information stored in customer profiles logged into by the attacker and attempted to access encoded payment data stored on those profiles. The information accessed by the attacker included: First and Last Name; Full Address; Phone Number; Email Address; and month and day of birth. The attacker also attempted to access encoded payment card numbers and expiration dates, the majority of which were for Macy's Proprietary Cards that can only be used at Macy's, Inc. entities. Note that CVV is not associated with a customer's profile. We can only confirm activity suggesting *attempts* to access encoded payment card data.

We will notify 3,564 Washington residents of this incident by first class mail on July 3, 2018. We are providing these individuals with an offer for complimentary AllClear Identity Theft Monitoring and AllClear Identity Repair services. An individual can enroll in AllClear ID services by calling a dedicated line or enrolling on the AllClear website, using the contact information included in the letter (a sample of which is attached).

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 St, Cincinnati, OH 45202 and michael.mccullough@macys.com.

Sincerely,

Michael McCullough
CPO & V.P. Enterprise Information Management

Attachments:

*(1) Sample Customer Notice of Data Breach Letter*

**ATTACHMENT 1: NOTICE OF DATA BREACH**

June 27, 2018

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

**WHAT HAPPENED?**

On June 11, 2018, our cyberthreat alert tools detected suspicious login activities related to certain macys.com customer online profiles using valid usernames and passwords. We immediately began an investigation. Based on our investigation, we believe that an unauthorized third party, from approximately April 26, 2018 through June 12, 2018, used valid customer user names and passwords to login to customer online profiles. We believe the third party obtained these customer usernames and passwords from a source other than Macy's.

On June 12, we blocked profiles with suspicious logins. A customer's profile will remain blocked until the customer updates the password associated with the profile. You should have received an email notifying you that your profile was blocked for security purposes. If you did not receive the email, please see the section below entitled "What if I did not get an email notice?"

The following provides additional information relating to this unfortunate event, including consumer protection options available to you. Please be aware that Macy's will never ask you for your profile password.

**WHAT INFORMATION WAS INVOLVED?**

After logging into a macys.com online profile, the unauthorized party was able to access the following information available in the profile: First and Last Name; Full Address; Phone Number; Email Address; Birthday (Month & Day only) and Debit or Credit Card Number with expiration dates.

Macys.com online profiles do not include Credit Verification Values (CVV) or Social Security numbers. As a result, this information was not accessed.

**WHAT ARE WE DOING?**

As discussed above, we immediately began an investigation as soon as we discovered the suspicious login activity. We have blocked profiles where we believe there was suspicious login activity. We have reported relevant debit and credit card numbers to Visa, Mastercard, American Express, and Discover. We have also added additional security rules around website login.

As discussed below, we are also making certain AllClear ID identity protection services available to you, at no cost to you.

**WHAT CAN YOU DO?**

You should remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. You may also contact your credit or debit card company and inform them that your card information may have been compromised. Your bank or credit card provider can suggest appropriate steps to protect your account. You should review your bank and card statements regularly, and immediately report any suspicious activity to your bank or credit card provider. Payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

Because we believe that the unauthorized third party used your valid username and password to login to your profile and the third party obtained your credentials from a source other than Macy's, we strongly encourage you to change your password for any online account for which you used the same username and password. In addition, it is always a good idea to ensure passwords to your online accounts are unique, changed regularly and that the same or similar passwords are not reused.

**WHAT IF I DID NOT GET AN EMAIL NOTICE?**

If you did not receive an email with the subject line "Important information about your Macy's online profile," please check your junk mail folder. If you cannot locate the email, please know that your macys.com profile is blocked, and you will not be able to login until you change your password. We encourage you to change your password to a unique password that you do not use at another website.

**CUSTOMER PROTECTION**

We at macys.com value our customer 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 AllClear ID (www.allclearid.com) provide you with identity protection services for 12 months at no cost to you. 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 Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-861-4018 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Identity Theft Monitoring: This service offers additional layers of protection including identity theft monitoring that delivers secure, actionable alerts to you by phone, as well as $1 million identity theft insurance coverage. To use this 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 1-855-861-4018 using the following redemption code {Redemption_Code}.

Please note: Additional steps may be required by you to activate your phone alerts and monitoring options.

**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 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) 525-6285
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) 916-8800
Fraud Victim Assistance Division
P.O. Box 2000
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.

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:

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

You will need to supply your name, address, date of birth, Social Security number and other personal information. The fee to place a credit freeze varies based on where you live. 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 1-855-861-4018 if you have any questions or concerns.

Sincerely,

Michael J. Gatio
President, Macy's Credit & Customer Services
Macy's, Inc.

**ADDITIONAL INFORMATION FOR SOME STATES**

*IF YOU ARE AN IOWA RESIDENT:* You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.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 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 Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

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

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