July [●], 2018

[FIRST] [LAST]
[ADDRESS 1]
[ADDRESS 2]
[CITY] [STATE], [ZIP / POST CODE]
[COUNTRY]

Dear [PREFIX] [LAST],

Notice of Data Breach

At Coty, we take the protection of your privacy and the security of your personal data extremely seriously, which is why, as a precautionary measure, we are writing to let you know that there may have been unauthorized access to your personal details as a result of a recent data security incident.

What Happened?

In January and February of this year, hackers using 'phishing' techniques accessed a number of Coty employee email accounts. A phishing email is designed to trick recipients into clicking on a link or revealing their login details. As a result, the emails within those accounts may have been seen or downloaded. We became aware of the incident on January 12, 2018, and immediately took steps to stop the hackers, and initiated an investigation to understand what had happened and the extent of the breach. After thorough analysis, our security experts have confirmed that the incident has been contained and that the additional security measures we have implemented will help guard against similar incidents in the future.

What personal data were involved?

Our forensic experts have identified that following information may have been included in the compromised emails:

- [APPLICABLE PERSONAL DATA]

What we are doing

We have taken steps to reduce the chance of an incident like this occurring again: resetting global passwords, enhancing processes to identify and block fraudulent emails, modifying access policies, conducting forensics with external security partners, taking steps to identify and remove malware from its computers, and internally communicating with Coty employees and leadership to reemphasize the need for vigilance against such attacks. We have also reported this incident to law enforcement in the United States both at the federal and state levels.

What you can do

Our forensic experts have advised that the hackers were primarily targeting corporate financial information, however you should remain vigilant against incidents of fraud, identity theft and potential phishing emails and telephone calls. We would recommend that you also follow these good security practices:

- Regularly reviewing any credit card or bank account statements that you receive for unusual or unexpected charges;
- Be aware of potential phishing emails and telephone calls from businesses or institutions requesting your personal details:
    - Avoid opening attachments or clicking links in emails and messages (including texts and social media messages) from unknown senders;
    - Verify the identity of anyone contacting you by phone or email. For example, if someone contacts you claiming to represent Coty or another organization, you should ask for their name and then try to call them back through the main switchboard or publicly available phone number. This is particularly important whenever anyone that you do not already know contacts you seeking money or information;
- Change your passwords on other online services, if you re-use the same password;
- Enable multi-factor authentication and other available security measures provided by your other online services;
- Install anti-virus software and keep it updated; and
- Apply all recommended software patches from operating system and software providers.

To help reassure you, we have made certain credit monitoring and identity restoration services available to you, free of charge, through Experian. Further details of these services and how to make use of them are included in the Appendix to this letter and can also be accessed here [hyperlink].

For residents of the United States or persons with credit cards, bank accounts, and other commercial relationships in the United States, you may further protect yourself by monitoring free credit reports available from the major credit reporting agencies, for any indication of unexpected activity, and by instituting fraud alerts and security freezes on your credit report profiles. You may also ask for certain information or assistance from state or federal law enforcement. These measures are described further in the Appendix to this letter.

For More Information

If you have any questions about the incident, you may contact me at:

[NAME OF COTY'S DATA PROTECTION OFFICER / OTHER CONTACT]
[ADDRESS 1]
[ADDRESS 2]
[CITY] [STATE], [ZIP / POST CODE]
[EMAIL]

You may also reach a representative by calling the dedicated free phone number on +1 (877) 890-9332. Or, you may find more information at [URL FOR ONLINE VERSION OF NOTIFICATION].

Sincerely,

[IMAGE OF SIGNATURE]

[NAME, OR SIGNED ON BEHALF OF COTY AS AN ENTITY]
[TITLE]

Appendix: Additional Information

Credit monitoring and identity restoration services made available by Coty:

If you have concerns about the 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 (details below). 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 offer is available to you for one-year 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^{SM} for a complimentary one-year 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:

- URL to activate the membership is **www.experianidworks.com/credit**
- Toll-free number for enrollments/questions is **+1 (877) 890-9332**
- Enrollment end date: **September 30, 2018**
- Engagement #: **DB07592**

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 +1 (877) 890-9332 by September 30, 2018. Be prepared to provide engagement number DB07592 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:

- **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.
- **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:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.Experianidworks.com/restoration for this information.

Measures that you can take to protect yourself with regard to consumer credit reporting bureaus:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

Fraud Alert. When you place a "fraud alert" on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other three bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A "security freeze" or "credit freeze" goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

- prevent you from getting your free annual credit report;

- keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance;

- prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and

other personal information. Each credit reporting agency may charge a fee, usually $5 to $10, for the placement of a security freeze on your credit reports, and may similarly charge a fee for lifting a security freeze.

The contact information of the main credit reporting agencies is provided below:

Equifax

Fraud Alerts

Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
+1 (866) 349-5191
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Security Freezes

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
+1 (800) 685-1111 (automated service line)
+1 (888) 298-0045 (customer care agents)
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Credit Reports

Equifax Information Services LLC
P.O. Box 740241
Atlanta, GA 30374-0241
+1 (866) 349-5191
https://www.annualcreditreport.com/index.action

Experian

Fraud Alerts

Experian
P.O. Box 4500
Allen, TX 75013
+1 (888) 397-3742
https://www.experian.com/help/identity-theft-victim-assistance.html

Security Freezes

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013 (regular mail)

Experian
711 Experian Parkway
Allen, TX 75013 (overnight mail)

+1 (888) 397-3742
https://www.experian.com/freeze/center.html

Credit Reports

Experian
P.O. Box 4500
Allen, TX 75013
+1 (888) 397-3742
https://www.annualcreditreport.com/index.action

TransUnion

Fraud Alerts

TransUnion Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
+1 (888) 909-8872
https://fraud.transunion.com

Security Freezes

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
+1 (888) 909-8872
https://freeze.transunion.com/

Credit Reports

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
+1 (800) 888-4213
https://www.annualcreditreport.com/index.action

Information and assistance that you can obtain from federal and state law enforcement and consumer protection agencies:

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC by mail at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
+1 (877)-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

Protections of the Federal Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary or your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to* www.ftc.gov/credit *or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580*.

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, all consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. *See* www.ftc.gov/credit *for additional information.*

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. *See* www.ftc.gov/credit *for an explanation of dispute procedures.*

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit.*

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at +1 (888) 5-OPTOUT (+1 (888) 567-8688).*

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active duty military personnel have additional rights. *For more information, visit* www.ftc.gov/credit.

Source: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

If you are a resident of Massachusetts, you have additional rights:

Under Massachusetts state law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

If you are a resident of Oregon, you have additional rights:

You can reach the Attorney General of the State of Oregon at +1 (877) 877-9392 or by mail at help@oregonconsumer.gov.

If you are a resident of Rhode Island, you have additional rights:

You can reach the Attorney General of the State of Rhode Island by phone at +1 (401) 274-4400 or online at www.riag.ri.gov.

If you are a resident of Maryland, you have additional rights:

You may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling +1 (410) 576-6491. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General by mail at:

Identity Theft Unit
Office of the Attorney General

200 St. Paul Place
16th Floor
Baltimore, MD 21202

If you are a resident of North Carolina, you have additional rights:

You can reach the Attorney General of the State of North Carolina by mail at:

9001 Mail Service Center
Raleigh, NC 27699-9001
+1 (919) 716-6400
http://www.ncdoj.gov