

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

December 27, 2022

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Discovery Clothing Company – Data Security Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Discovery Clothing Company (“Discovery”). I am writing to provide notification of an incident at Discovery that may affect the security of personal information of approximately 2 Maryland residents. This notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Discovery does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On October 3, 2022, Discovery experienced unauthorized access to its network that involved ransomware. Upon learning of this issue, Discovery immediately commenced a prompt and thorough investigation. As part of its investigation, Discovery has worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation, Discovery discovered on December 5, 2022 that certain impacted files may have been removed from the network by an unauthorized entity. The files contained personal information of Maryland residents including full name, SSN, health insurance information and credit/debit card number.

Discovery is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Discovery wanted to inform you (and the affected residents of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Discovery is providing the affected residents with written notification of this incident on December 28, 2022 in substantially the same form as the letter attached hereto. Discovery is offering the affected residents complimentary one year membership with a credit monitoring service. Discovery will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Discovery will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

December 27, 2022

Page 2

At Discovery, protecting the privacy of personal information is a top priority. Discovery is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Discovery continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 220-1360 or cczuprynski@mcdonalddhopkins.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Christine Czuprynski", written in a cursive style.

Christine N. Czuprynski

Encl.

Dear [REDACTED]:

We are writing to inform you of a recent security incident affecting a portion of our stored electronic data. That data may have included your personal information, the privacy and security of which are of the utmost importance to Discovery Clothing Company. We wanted to provide you with information about the incident, explain the services we have made available to you, and let you know that we continue to take significant measures to help protect your information.

What Happened?

Discovery Clothing Company recently experienced a cybersecurity incident involving ransomware.

What We Are Doing.

Upon learning of this issue, we quickly contained the threat by disabling all unauthorized access to the network and immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the information on our network. Though our investigation is still ongoing, we concluded on December 5, 2022 that your personal information may have been accessed or acquired in connection with this incident.

What Information Was Involved?

The potentially acquired information included your personal information, specifically your [REDACTED]

What You Can Do.

To date, we are not aware of any misuse of your information as a result of this incident. Out of an abundance of caution, however, and to help protect you from potential misuse of your information, we are offering a complimentary one-year membership of identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We apologize for the inconvenience caused by this attack, which occurred despite our focused efforts to combat this criminal behavior. We remain committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. In response to this incident, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts, including resetting account passwords and strengthening our password security policies, ensuring compliance with multi-factor authentication for network access, upgrading our firewall, and deploying endpoint detection software.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1 [REDACTED], Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Discovery Clothing Company

– OTHER IMPORTANT INFORMATION –

1. Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year.

Visit [REDACTED] to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105788
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion LLC

P.O. Box 6790
Fullerton, PA 92834-6790

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888) 298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, HYPERLINK "<http://www.doj.state.or.us/>" www.doj.state.or.us/, Telephone: 877-877-9392.