SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
+1 202 736 8000
+1 202 736 8711 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 202 736 8465
CTBROWN@SIDLEY.COM

VIA EMAIL: DOJ-CPB@doj.nh.gov

November 29, 2022

SUPPLEMENTAL NOTICE OF SECURITY INCIDENT

Dear Attorney General Formella,

I am writing to provide an update to the Notice of Security Incident sent to your office on August 16, 2022 on behalf of my client, Hanesbrands Inc. ("HBI"). As described in the initial notice, HBI experienced a ransomware incident on May 24, 2022. As also described in HBI's initial notice, while our manual review of data and rolling notification was ongoing, we had at that time identified 154 New Hampshire residents.

As an update, our review of the data is now complete, and we identified an additional 76 New Hampshire residents. HBI provided these individuals with notice and an offer of credit monitoring via US mail on or before November 23, 2022. For your convenience, we reattach the sample notice letter, which was enclosed in our initial notice of security incident filing.

If you have any questions, please do not hesitate to contact me at ctbrown@sidley.com.

Sincerely,

Colleen Theresa Brown
Partner

HANES Brands Inc
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 16, 2022

i2038-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ALL OTHER STATES
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF SECURITY INCIDENT

Dear Sample A. Sample:

I am writing about the data security incident previously disclosed by HanesBrands. We have determined this incident, which has been contained, impacted your personal information. At this time, **we have no indication of fraud or misuse of your personal information resulting from this incident**. We are notifying you to explain the circumstances and to inform you of the steps we have taken and the resources we are making available to you.

What Happened?

On May 24, 2022, HanesBrands detected a ransomware incident impacting certain internal IT systems. We took prompt action to contain the incident, secure our systems, restore and resecure impacted data, and implement our business continuity plans. We also reported the incident to law enforcement and have been cooperating with their investigation. After working to restore and resecure impacted data, we conducted a review and recently identified that some of your personal information was impacted in the event.

What Information May Have Been Involved?

The impacted information varies by individual, and may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes.

What We Are Doing

The safety of your personal information is of the utmost importance to us. We promptly reported the incident to law enforcement and began an investigation to understand the scope and impact. We have also taken a number of steps to even further strengthen the security of our networks. We are continuing to monitor the dark web for any indication of misuse of personal information in connection with this incident, and to date have not identified any such misuse.

As an added precaution to help protect your identity, we are offering a complimentary two-year membership of Experian's IdentityWorks. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal data please follow the steps below:

- Ensure that you **enroll by: November 30, 2022** (as your code will not work after this date).
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**:

0000001

What You Can Do

While we have no indication of fraud resulting from this incident, in addition to enrolling in the identity theft protection services described above, we encourage you to remain vigilant with respect to your personal accounts. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to your relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information

We take the security of your information seriously and regret any inconvenience or concern. We are committed to protecting your information. Should you have questions or concerns, please do not hesitate to contact us at (844) 955-2743. Please be prepared to reference engagement when speaking with an agent.

Sincerely,

Stephen B. Bratspies
Chief Executive Officer

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports

Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
Equifax.com	Experian.com	Transunion.com

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft:*

A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional information required by state laws, including for residents of Iowa, Maryland, Massachusetts, New Mexico, North Carolina, Oregon, Rhode Island, and Vermont.

This notice was not delayed due to any law enforcement investigation request.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.