

Dominic A. Paluzzi  
Direct Dial: 248-220-1356  
E-mail: [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com)

June 28, 2019

**VIA U.S. MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Incident Notification**

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Hauser, Inc. ("Hauser"). I am writing to provide notification of an inadvertent disclosure incident involving the personal information of ten (10) New Hampshire residents. The investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Hauser does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Hauser was retained by The Hershey Company ("Hershey") to assist with determining appropriate health and welfare partners for Hershey's medical, prescription drug, dental and vision coverage plans through a Request for Proposal process ("RFP"). On or about May 15, 2019, Hershey learned that on or about April 30, 2019, during the RFP, Hauser's subcontractor obtained and subsequently provided certain documents to potential dental and vision providers, in a secure transmission, which inadvertently contained Hershey employees' and their dependents' personal information. Upon learning of the issue, Hershey and Hauser commenced an investigation. All potential dental and vision providers that received the documents, which inadvertently contained personal information, provided Hauser either with signed affidavits of destruction of those documents or assurances that the information would be secured and not distributed or shared further. In addition, all of the dental and vision providers are bound by strict confidentiality terms in their relevant contracts with Hauser. The information included the notified residents' full names, Social Security numbers, dates of birth, and health insurance information.

Hauser has no evidence that any of the personal information has been misused or that there is any risk of harm to the notified residents or their information, and this notification was not delayed for any reason. Nevertheless, out of an abundance of caution, Hauser wanted to inform you (and the notified residents) of the incident and to explain the steps that it is taking to help safeguard the notified residents against identity fraud. Hauser is providing the notified residents with written notification of this incident commencing on June 28, 2019 in substantially

RECEIVED

JUL 05 2019

CONSUMER PROTECTION

Attorney General Gordon MacDonald  
Office of the Attorney General  
June 28, 2019  
Page 2

the same form as the letter attached hereto. Hauser is providing the notified residents with a dedicated response line to call with questions. Hauser is offering the notified residents a complimentary one-year membership with a credit monitoring service through Experian. Hauser is advising the notified residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The notified residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority. Hauser is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Hauser continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com). Thank you for your cooperation.

Sincerely,

A handwritten signature in blue ink, appearing to read "D. Paluzzi".

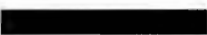
Dominic A. Paluzzi

Encl.

Hauser, Inc.  
Mail Handling Services  
777 E Park Dr  
Harrisburg, PA 17111



Notice of Data Security Incident

Dear 

We are writing with important information regarding a recent security incident that involved your personal information. Although we believe that there is minimal risk of misuse of your personal information due to this incident, we are writing to make sure that you are fully informed. This letter contains information about the incident and explains the services that are being made available to you; please read it carefully.

What Happened?

Hauser, Inc. (“Hauser” or “we” or “us”) was retained by The Hershey Company (“Hershey”) to assist with determining appropriate health and welfare partners for Hershey’s medical, prescription drug, dental and vision coverage plans through a Request for Proposal process (“RFP”). On or about May 15, 2019, Hershey learned that on or about April 30, 2019, during the RFP, Hauser’s subcontractor obtained and subsequently provided certain documents to potential dental and vision providers, in a secure transmission, which inadvertently contained Hershey employees’ and their dependents’ personal information. We regret that this incident occurred, and assure you that the security of your personal information is of the utmost importance to us and to Hershey.

What We Are Doing.

Upon learning of the issue, Hershey and Hauser commenced an investigation. All potential dental and vision providers that received the documents, which inadvertently contained personal information, provided Hauser either with signed affidavits of destruction of those documents or assurances that the information would be secured and not distributed or shared further. In addition, all of the dental and vision providers are bound by strict confidentiality terms in their relevant contracts with Hauser.

**We have no evidence that any of your personal information has been misused or that there is any risk of harm to you or your information,** and this notification to you was not delayed for any reason.

What Information Was Involved?

The documents provided to the potential dental and vision providers inadvertently contained some of your personal information, including your full name, Social Security number, date of birth, and health insurance information.

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft.

IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to 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.

We regret any inconvenience that this incident may cause you. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

*For More Information.*

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 [REDACTED]. This response line is staffed with professionals familiar with this incident. The response line is available Monday through Friday, 8am – 5pm Eastern Time.

Sincerely,

Hauser, Inc.

- OTHER IMPORTANT INFORMATION -

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

**Activate IdentityWorks Credit 3B Now in Three Easy Steps**

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [REDACTED]
3. PROVIDE the **Activation Code**: [REDACTED]

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 [REDACTED]. Be prepared to provide engagement number [REDACTED] proof of eligibility for the identity restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **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.

**Activate your membership today at [REDACTED]  
or call [REDACTED] to register with the activation code above.**

**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 [REDACTED] for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [REDACTED].

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## 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 90-day “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 105069  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

### **Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

### **TransUnion LLC**

P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

## 3. Consider 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**

PO Box 105788  
Atlanta, GA 30348  
<https://www.freeze.equifax.com>  
1-800-349 -9960

### **Experian Security Freeze**

PO Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
1-888-397-3742

### **TransUnion Security Freeze**

P.O. Box 2000  
Chester, PA 19016  
<http://www.transunion.com/securityfreeze>  
1-888-909-8872

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 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.

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](http://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](http://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.

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: (515) 281-5164

**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](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**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, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://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, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.