

February 18, 2022

**VIA EMAIL**

Attorney General John M. Formella  
Office of the Attorney General  
Attn: Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301  
Email: [DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov)

**Re: Notice Pursuant to NH Rev Stat § 359-C:20**

Dear Attorney General Formella:

Pursuant to New Hampshire Revised Statute section 359-C:20, we write on behalf of Meyer Corporation, U.S. (“Meyer”) to notify you of a data security matter, which we believe impacted approximately one (1) New Hampshire resident. Meyer is a cookware distributor located at 1 Meyer Plaza, Vallejo, CA 94590.

On or around October 25, 2021, Meyer was the victim of a cybersecurity attack by an unauthorized third party that impacted its systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, our investigation identified potential unauthorized access to Meyer employee information including employees of Meyer’s subsidiaries Hestan Commercial Corporation, Hestan Smart Cooking, Hestan Vineyards, and Blue Mountain Enterprises, LLC. The types of personal information that may have been accessed during this incident will depend on the types of information the employee provided to their employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver’s license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding dependents (including Social Security numbers).

On or around January 14, 2022, we confirmed that the impacted population includes a New Hampshire resident. Notification of this matter was mailed to the impacted resident on or around February 15, 2022. A copy of this notification is attached as Exhibit A.

# manatt

Attorney General John M. Formella  
February 18, 2022  
Page 2

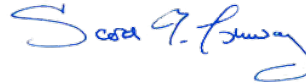
Meyer takes the protection of its employees' personal information seriously. Meyer is offering two years of identity protection services, at no cost, to affected employees and their dependents. In response to this data security matter, Meyer has taken steps to further enhance its security protocols. We are also in the process of evaluating and investigating this matter further in order to prevent a similar occurrence in the future.

Below is the contact information for John M. Compagno, General Counsel, at Meyer:

John M. Compagno  
General Counsel  
(707) 551-2840  
JohnC@meyer.com

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,



Scott Lashway

# **Exhibit A**



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

13 1 2546 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



February 15, 2022

## **RE: NOTICE OF DATA BREACH**

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Meyer Corporation, U.S. (“Meyer”) and to provide you information about steps you can take to help protect your information.

### **What Happened?**

On or around October 25, 2021, Meyer was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of our cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, our investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

### **What Information Was Involved?**

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver’s license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

### **What We Are Doing**

The security of our employees’ information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

### **What You Can Do**

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [\*\*www.experianidworks.com/credit\*\*](http://www.experianidworks.com/credit)
- Provide your **activation code**:

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [\*\*www.experianidworks.com/minorplus\*\*](http://www.experianidworks.com/minorplus)
- Provide your **activation code**:
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

Additional information regarding Experian IdentityWorks is enclosed.

### **Other Important Information**

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

### **For More Information**

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

*Chris Banning*

Chris Banning  
Managing Director

## ADDITIONAL DETAILS REGARDING THE 24-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **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™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. 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 Identity Restoration support is available to you for 24 months 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

*\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

## ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission (“FTC”), the credit reporting agencies, or your state’s regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
<b>Federal Trade Commission</b> Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a>		
Credit Reporting Agencies		
<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>

**Order Your Free Annual Credit Report.** You can order your free annual credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: [www.ftc.gov](http://www.ftc.gov). You can also visit the Consumer Financial Protection Bureau’s website for more information on how you can obtain your credit report for free: [www.consumerfinance.gov](http://www.consumerfinance.gov). Once you receive your credit reports, review them carefully for any 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 agency.

**Review Your Accounts and Report Unauthorized Activity.** We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state’s attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

**Consider Placing a Security Freeze on Your Credit File.** You also may consider implementing a security freeze (also called a “credit freeze”). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be



required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

**Remain Vigilant and Lookout for Phishing Schemes.** We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

**For Maryland Residents.** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents:** You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

**For North Carolina Residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-5-NO-SCAM  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Rhode Island Residents:** You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
1-401-274-4400  
[riag.ri.gov](http://riag.ri.gov)







Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

13 1 2535 \*\*\*\*\*SNGLP

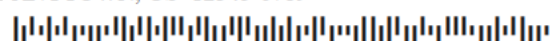
SAMPLE A. SAMPLE - L02

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



February 15, 2022

## **RE: NOTICE OF DATA BREACH**

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Hestan Commercial Corporation (“Hestan Commercial”) and to provide you information about steps you can take to help protect your information.

### **What Happened?**

On or around October 25, 2021, Meyer Corporation, U.S. (“Meyer”), Hestan Commercial’s parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

### **What Information Was Involved?**

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver’s license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

### **What We Are Doing**

The security of our employees’ information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

### **What You Can Do**

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [www.experianidworks.com/credit](http://www.experianidworks.com/credit)
- Provide your **activation cod**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [www.experianidworks.com/minorplus](http://www.experianidworks.com/minorplus)
- Provide your **activation code**:
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076 by April 30, 2022**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

Additional information regarding Experian IdentityWorks is enclosed.

### **Other Important Information**

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

### **For More Information**

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,



Eric Deng  
President

## ADDITIONAL DETAILS REGARDING THE 24-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **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™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. 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 Identity Restoration support is available to you for 24 months 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

*\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

## **ADDITIONAL RESOURCES**

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission (“FTC”), the credit reporting agencies, or your state’s regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

<b>Federal Trade Commission</b>		
<b>Federal Trade Commission</b> Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a>		
<b>Credit Reporting Agencies</b>		
<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>

**Order Your Free Annual Credit Report.** You can order your free annual credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: [www.ftc.gov](http://www.ftc.gov). You can also visit the Consumer Financial Protection Bureau’s website for more information on how you can obtain your credit report for free: [www.consumerfinance.gov](http://www.consumerfinance.gov). Once you receive your credit reports, review them carefully for any 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 agency.

**Review Your Accounts and Report Unauthorized Activity.** We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state’s attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

**Consider Placing a Security Freeze on Your Credit File.** You also may consider implementing a security freeze (also called a “credit freeze”). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be

required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

**Remain Vigilant and Lookout for Phishing Schemes.** We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

**For Maryland Residents.** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents:** You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

**For North Carolina Residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-5-NO-SCAM  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Rhode Island Residents:** You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
1-401-274-4400  
[riag.ri.gov](http://riag.ri.gov)







Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

13 1 2547 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L05

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



February 15, 2022

## **RE: NOTICE OF DATA BREACH**

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Hestan Smart Cooking Inc. (“Hestan Smart Cooking”) and to provide you information about steps you can take to help protect your information.

### **What Happened?**

On or around October 25, 2021, Meyer Corporation, U.S. (“Meyer”), Hestan Smart Cooking’s parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

### **What Information Was Involved?**

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver’s license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

### **What We Are Doing**

The security of our employees’ information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

### **What You Can Do**

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [www.experianidworks.com/credit](http://www.experianidworks.com/credit)
- Provide your **activation code**:

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [www.experianidworks.com/minorplus](http://www.experianidworks.com/minorplus)
- Provide your **activation code**:
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number proof of eligibility for the identity restoration services by Experian.

Additional information regarding Experian IdentityWorks is enclosed.


### **Other Important Information**

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

### **For More Information**

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,



Scott Kim  
Managing Director

## ADDITIONAL DETAILS REGARDING THE 24-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **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™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. 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 Identity Restoration support is available to you for 24 months 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

*\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

## **ADDITIONAL RESOURCES**

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission (“FTC”), the credit reporting agencies, or your state’s regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

<b>Federal Trade Commission</b>		
<b>Federal Trade Commission</b> Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a>		
<b>Credit Reporting Agencies</b>		
<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>

**Order Your Free Annual Credit Report.** You can order your free annual credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: [www.ftc.gov](http://www.ftc.gov). You can also visit the Consumer Financial Protection Bureau’s website for more information on how you can obtain your credit report for free: [www.consumerfinance.gov](http://www.consumerfinance.gov). Once you receive your credit reports, review them carefully for any 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 agency.

**Review Your Accounts and Report Unauthorized Activity.** We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state’s attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

**Consider Placing a Security Freeze on Your Credit File.** You also may consider implementing a security freeze (also called a “credit freeze”). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from

accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

**Remain Vigilant and Lookout for Phishing Schemes.** We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

**For Maryland Residents.** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents:** You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

**For North Carolina Residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-5-NO-SCAM  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Rhode Island Residents:** You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
1-401-274-4400  
[riag.ri.gov](http://riag.ri.gov)







Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

11 1 2334 \*\*\*\*\*AUTO\*\*ALL FOR AADC 945

SAMPLE A. SAMPLE - L04

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



February 15, 2022

## **RE: NOTICE OF DATA BREACH**

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Hestan Vineyards LLC (“Hestan Vineyards”) and to provide you information about steps you can take to help protect your information.

### **What Happened?**

On or around October 25, 2021, Meyer Corporation, U.S. (“Meyer”), Hestan Vineyards’ parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

### **What Information Was Involved?**

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver’s license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

### **What We Are Doing**

The security of our employees’ information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to



your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

### **What You Can Do**

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **oll: [www.experianidworks.com/credit](http://www.experianidworks.com/credit)**
- Provide your **activation code**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **[www.experianidworks.com/minorplus](http://www.experianidworks.com/minorplus)**
- Provide your **activation code**:
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076 by April 30, 2022**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

Additional information regarding Experian IdentityWorks is enclosed.

### **Other Important Information**

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

### **For More Information**

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,



Ann Hitchcock  
Director of Operations

## ADDITIONAL DETAILS REGARDING THE 24-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **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™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. 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 Identity Restoration support is available to you for 24 months 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

*\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

## **ADDITIONAL RESOURCES**

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission (“FTC”), the credit reporting agencies, or your state’s regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

<b>Federal Trade Commission</b>		
<b>Federal Trade Commission</b> Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a>		
<b>Credit Reporting Agencies</b>		
<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>

**Order Your Free Annual Credit Report.** You can order your free annual credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: [www.ftc.gov](http://www.ftc.gov). You can also visit the Consumer Financial Protection Bureau’s website for more information on how you can obtain your credit report for free: [www.consumerfinance.gov](http://www.consumerfinance.gov). Once you receive your credit reports, review them carefully for any 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 agency.

**Review Your Accounts and Report Unauthorized Activity.** We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state’s attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

**Consider Placing a Security Freeze on Your Credit File.** You also may consider implementing a security freeze (also called a “credit freeze”). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be

required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

**Remain Vigilant and Lookout for Phishing Schemes.** We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

**For Maryland Residents.** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents:** You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

**For North Carolina Residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-5-NO-SCAM  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Rhode Island Residents:** You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
1-401-274-4400  
[riag.ri.gov](http://riag.ri.gov)



# BLUE MOUNTAIN ENTERPRISES

Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

13 1 2545 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L03

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



February 15, 2022

## RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Blue Mountain Enterprises, LLC (“Blue Mountain”) and to provide you information about steps you can take to help protect your information.

### **What Happened?**

On or around October 25, 2021, Meyer Corporation, U.S. (“Meyer”), Blue Mountain’s parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

### **What Information Was Involved?**

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver’s license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

### **What We Are Doing**

The security of our employees’ information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to your employer, we are also offering identity protection services for your dependent(s). We have also



taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

### **What You Can Do**

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [www.experianidworks.com/credit](http://www.experianidworks.com/credit)
- Provide your **activation cod**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [www.experianidworks.com/minorplus](http://www.experianidworks.com/minorplus)
- Provide your **activation code**:
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian. Additional information regarding Experian IdentityWorks is enclosed.

### **Other Important Information**

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

### **For More Information**

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,



Stephanie MacLean  
Chief Executive Officer



## ADDITIONAL DETAILS REGARDING THE 24-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **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™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. 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 Identity Restoration support is available to you for 24 months 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

*\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

## **ADDITIONAL RESOURCES**

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission (“FTC”), the credit reporting agencies, or your state’s regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

<b>Federal Trade Commission</b>		
<b>Federal Trade Commission</b> Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a>		
<b>Credit Reporting Agencies</b>		
<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>

**Order Your Free Annual Credit Report.** You can order your free annual credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: [www.ftc.gov](http://www.ftc.gov). You can also visit the Consumer Financial Protection Bureau’s website for more information on how you can obtain your credit report for free: [www.consumerfinance.gov](http://www.consumerfinance.gov). Once you receive your credit reports, review them carefully for any 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 agency.

**Review Your Accounts and Report Unauthorized Activity.** We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state’s attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

**Consider Placing a Security Freeze on Your Credit File.** You also may consider implementing a security freeze (also called a “credit freeze”). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

**Remain Vigilant and Lookout for Phishing Schemes.** We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient’s email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

**For Maryland Residents.** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents:** You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

**For North Carolina Residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General’s Office:

North Carolina Attorney General’s Office  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-5-NO-SCAM  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Rhode Island Residents:** You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
1-401-274-4400  
[riag.ri.gov](http://riag.ri.gov)

