

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL
jloyal@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

A Mid-Atlantic Litigation Firm

DANIEL HAIER
dhaier@c-wlaw.com

Phone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

www.C-WLAW.com

May 20, 2022

Via Email (idtheft@oag.state.md.us)

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

RE: Security Breach Notification

To Whom It May Concern:

We serve as counsel for D&H Company ("D&H"), located at P.O. Box 1688, Tupelo, MS 38802. We write to provide notification of a recent data security incident. By providing this notice, D&H does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about January 8, 2022, D&H experienced a sophisticated ransomware attack that impacted its ability to access certain files on its corporate network. Upon discovery, D&H immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the incident. The investigation and review of the information potentially at risk was concluded on April 22, 2022, at which time D&H began confirming address information for potentially impacted individuals.

At this time, D&H is aware of personal information related to approximately 21 residents of Maryland who may have been impacted by this incident. While the information potentially impacted varies by individual, it may include first and last name and one or more of the following data elements: date of birth, Social Security number, driver's license number, and/or financial account number and routing number.

D&H provided written notice to the potentially impacted individuals via First Class Mail on May 20, 2022. A copy of the notice is attached as ***Exhibit A***. While D&H has no reason to believe that any personal information was misused as a result of this incident, D&H is offering the potentially impacted Maryland residents complimentary credit monitoring and identity protection services for 12 months.

In response to this incident, D&H changed account passwords, enhanced security protocols, and is reviewing its policies and procedures related to data protection.

Thank you for your attention to this matter and please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.



John Loyal, Esq.
610-567-0700
jloyal@c-wlaw.com

Exhibit A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

D&H Company writes to notify you of a recent incident that may have involved your personal information as described below. We take this incident seriously and are providing you information about the incident, our response, and steps you can take to help protect your information.

On or about January 8, 2022, we experienced a sophisticated ransomware attack that impacted our ability to access certain files on our corporate network. We immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the disruption. We also reported the incident to law enforcement. Although we have no evidence of misuse of information as a result of this incident, the investigation was unable to rule out unauthorized access to limited areas of our corporate network. Therefore, in an abundance of caution, we conducted a thorough review of the contents of the potentially impacted network locations to determine the information contained therein and to whom the information related.

On April 22, 2022, the review was completed, and we immediately began working to confirm address information for potentially impacted individuals so we could notify them of this incident. The information potentially impacted included your first and last name and one or more of the following: <<Breached Elements>>.

In response to this incident, we changed account passwords and enhanced security protocols, and we are reviewing our policies and procedures related to data protection.

Although we have no evidence of misuse of information as a result of this incident, in an abundance of caution, we are providing you access to 12 months of credit monitoring and identity protection services at no cost to you. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed *"Steps You Can Take to Protect Your Information."*

Should you have any questions regarding this matter, you may contact our dedicated assistance line at 888-303-5842, Monday through Friday from 7am to 7pm MT (excluding major U.S. holidays), or write to us at P.O. Box 1688, Tupelo, MS 38802.

We sincerely regret any concern this incident may cause you. Unfortunately, these types of criminal attacks on companies large and small have become increasingly common, and this incident is similar to those experienced by many other companies across the country. However, the privacy and security of information is deeply important to us, and we will continue to take steps to protect information in our care.

Sincerely,

D&H Company

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Engagement Number>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements or suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. D&H Company may be contacted at P.O. Box 1688, Tupelo, MS 38802.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

To the Parent or Guardian of:

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Dear Parent/Guardian of <<Name 1>>:

D&H Company writes to notify you of a recent incident that may have involved your minor child's personal information as described below. We take this incident seriously and are providing you information about the incident, our response, and steps you can take to help protect your minor child's information.

On or about January 8, 2022, we experienced a sophisticated ransomware attack that impacted our ability to access certain files on our corporate network. We immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the disruption. We also reported the incident to law enforcement. Although we have no evidence of misuse of information as a result of this incident, the investigation was unable to rule out unauthorized access to limited areas of our corporate network. Therefore, in an abundance of caution, we conducted a thorough review of the contents of the potentially impacted network locations to determine the information contained therein and to whom the information related.

On April 22, 2022, the review was completed, and we immediately began working to confirm address information for potentially impacted individuals so we could notify them of this incident. The information potentially impacted included your minor child's first and last name and one or more of the following: <<Breached Elements>>.

In response to this incident, we changed account passwords and enhanced security protocols, and we are reviewing our policies and procedures related to data protection.

Although we have no evidence of misuse of information as a result of this incident, in an abundance of caution, we are providing potentially impacted individuals complimentary access to 12 months of identity protection services. Instructions about how to enroll in these services and other precautionary measures you can take to help protect your minor's personal information are included in the enclosed "*Steps You Can Take to Protect Your Minor's Information.*"

Should you have any questions regarding this matter, you may contact our dedicated assistance line at 888-303-5842, Monday through Friday from 7am to 7pm MT (excluding major U.S. holidays), or write to us at P.O. Box 1688, Tupelo, MS 38802.

We sincerely regret any concern this incident may cause you. Unfortunately, these types of criminal attacks on companies large and small have become increasingly common, and this incident is similar to those experienced by many other companies across the country. However, the privacy and security of information is deeply important to us, and we will continue to take steps to protect information in our care.

Sincerely,

D&H Company

STEPS YOU CAN TAKE TO PROTECT YOUR MINOR'S INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and your explanation of benefits forms for suspicious activity and to detect errors. Although minors typically do not have a credit report, under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

1. Enroll in Identity Protection



Enter your Activation Code: <<Enrollment Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Child Monitoring Package

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications to the primary adult member of activity on the child's Equifax credit report

Enrollment Instructions

Parent/guardian Go to www.equifax.com/activate

Enter your unique Activation Code of <ACTIVATION CODE> then click "Submit" and follow these 4 steps:

1. Register:
Complete the form with parent/guardian contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. Create Account:
Enter parent/guardian email address, create a password, and to accept the terms of use.
3. Verify Identity:
To enroll in your product, we will ask you to complete our identity verification process.
4. Checkout:
Upon successful verification of parent/guardian identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling.
The confirmation page shows parent/guardian completed enrollment.
Click "View My Product" to access the product features and enroll minor children.

How to Add Minors to Your Equifax Child Monitoring Package

You will be able to add minors to your Equifax Child Monitoring Package through your product dashboard.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child"
3. From there, enter your child's first name, last name, date of birth and social security number.
Repeat steps for each minor child (up to four)

Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can add up to 4 children under the age of 18 with your Equifax Child Monitoring Package.

2. Place a Credit Freeze on Your Minor's Credit File

You have the right to place a **credit freeze** on your minor's file, which will prohibit a credit bureau from releasing information in the credit file without your express authorization. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on a credit file. To request a credit freeze for your minor, you will need to provide the following information for both you and your minor:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth; and
4. Address for the prior two to five years.

Include for your identification:

5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. Proof that you are the parent or legal guardian of the minor.

Include for your minor's identification:

8. A copy of your minor's Social Security card and
9. A copy of your minor's birth certificate.

Should you wish to contact the credit reporting bureaus or place a credit freeze, please contact the bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348
---	--	--

3. Additional Information

You can further educate yourself regarding identity theft, credit freezes, and the steps you can take to protect your minor's personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if your minor experiences identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that your minor has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. D&H Company may be contacted at P.O. Box 1688, Tupelo, MS 38802.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.