

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

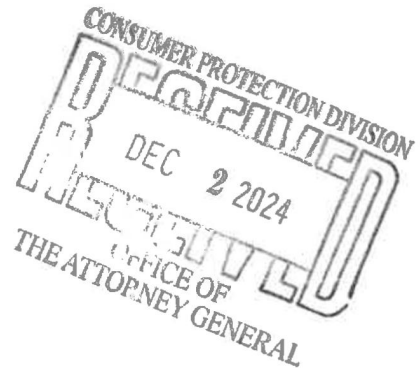
HILARY F. HIGGINS
hhiggins@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

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

MUSHU HUANG
mhuang@c-wlaw.com

November 25, 2024



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

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

RE: Notice of Data Security Incident

To Whom It May Concern:

We serve as counsel for MI HoldCo, Inc. ("MI") located at 2 City Place Drive, Suite 400, St. Louis, MO 63141, and provide this notification of a recent data security incident. By providing this notice, MI does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On October 16, 2024, MI discovered that certain systems were inaccessible. Upon discovery, MI immediately began working with its I.T. team and third-party forensic specialists to secure the network, restore its systems to full operability, and investigate the full nature and scope of the incident. MI also reported this incident to federal law enforcement. The investigation determined that certain MI data may have been subject to unauthorized access during the attack. MI then began a thorough review of the potentially impacted files to identify what type of information was contained therein, and to whom that information belonged. Through this review, MI learned that data related to certain current and former employees, their beneficiaries, and applicants may have been impacted. The comprehensive review process was completed on November 8, 2024.

At that time, MI determined that information related to 15 Maryland residents may have been subject to unauthorized access. The information believed to be at risk may include a first and last name, in combination with one or more of the following: Social Security number, financial account details, driver's license, passport, date of birth, username and password, health information, and/or health insurance details.

On November 19, 2024, MI sent written notices of this incident to the potentially impacted Maryland residents pursuant to Maryland law. The notice letters included an offer of complimentary credit monitoring and identity protection services for 24 months. A template copy of the individual notification letters sent to potentially impacted individuals in Maryland is attached hereto as "Exhibit A."

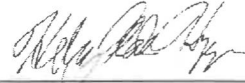
In response to this incident, MI conducted a full forensic investigation, changed passwords, implemented new technical safeguards, and is continuing to review its policies and procedures related to data protection.

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

Very truly yours,

CIPRIANI & WERNER, P.C.

By:

A handwritten signature in dark ink, appearing to read 'Hilary Higgins', is written over a horizontal line.

Hilary Higgins, Esq.

Exhibit A



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

November 19, 2024



M4163-L04-0000004 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L04 FORMER EMPLOYEE
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Extra 1: Notice of Data Breach CA ONLY

Dear Sample A. Sample:

Instinct Pet Food (“Instinct”), formally known as Nature’s Variety, writes to inform you of a recent event at Instinct. You are receiving this letter because certain information collected in connection with your previous or potential employment with Instinct was identified in connection with this matter. This letter includes information about the event, our response, and resources we are making available to you, including access to credit monitoring services as discussed below.

What Happened?

On October 16, 2024, Instinct detected unauthorized activity on our computer network. We took swift action, engaging third-party forensic experts to thoroughly investigate. This investigation confirmed that an unauthorized individual gained access to a limited amount of data. A subsequent review of this data indicated that certain employee information was impacted.

What Information Was Involved?

Based on our investigation, the information that was affected includes personal data collected from employees, which may include your name, together with [Extra2].

What We Are Doing

In response, Instinct has promptly enacted containment measures, including resetting passwords and securing accounts, and conducted a full investigation into the activity. We are also notifying relevant regulatory authorities as required. Additionally, we have implemented strengthened security measures to further safeguard against similar incidents in the future.

Additionally, Instinct is offering you access to 24 months of credit monitoring and identity protection services through Experian IdentityWorksSM at no cost to you. Due to privacy laws, Instinct cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring services is enclosed. We have also provided below information about steps you can take to help protect yourself against fraud and identity theft should you feel it appropriate to do so.



What You Can Do. Instinct recommends that you remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your accounts, please promptly contact your financial institution or credit/debit card company. You can also review the enclosed "Recommended Actions You Should Immediately Take to Help Protect Your Information" for additional information and resources.

For More Information. We understand you may have additional questions about this matter. Should you have questions or concerns, please contact our dedicated assistance line at 833-918-1091, which is available from Monday to Friday, between 8 AM and 8 PM Central Time (excluding major U.S. holidays). Our support line will help you with any questions you have activating your ID protection service or any other questions relating to this matter.

Instinct sincerely regrets any concern this incident may cause you.

Sincerely,

Instinct Pet Food, formally known as Nature's Variety

RECOMMENDED ACTIONS YOU SHOULD IMMEDIATELY TAKE TO PROTECT YOUR INFORMATION

Enroll in Offered Monitoring Services

Please note that Identity Restoration 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by February 28, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1091 by February 28, 2025. Be prepared to provide engagement number B135295 as proof of eligibility for the Identity Restoration services by Experian.

Additional Details regarding Your 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, Equifax and Transunion files for indicators of fraud.
- **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™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

*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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for 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	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	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 <https://www.marylandattorneygeneral.gov/>. Instinct Pet Food is located at 2 Cityplace Drive, Suite 400, Saint Louis, Missouri 63141.

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.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 5 Rhode Island residents impacted by this incident.

