



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

December 31, 2024

VIA E-Mail Reporting

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: IDtheft@oag.state.md.us

RE: Central Valley Meat Co. Inc. - Notice of Data Event

Dear Sir or Madam:

We represent Central Valley Meat Co. Inc. and its affiliates, Coelho Meat Company, CLW Foods Incorporated, and Triple C Trucking (collectively, "CVM"), which are a full line beef harvesting operation based in Hanford, California. This submission is provided pursuant to Maryland Personal Information Protection Act, MD. CODE ANN. COM. LAW §14-3501, *et seq*, which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

On May 23, 2024, CVM identified unusual activity on its computer systems that impacted company operations. CVM took prompt steps to confirm the security of its systems and initiated a comprehensive investigation to determine the extent of impact to its network. From the investigation, CVM learned that certain files and folders were taken from its network before its systems were disrupted and rendered inaccessible. After confirming some of the accessed locations included employee information, CVM commenced a thorough review of the files to determine what information was present and to whom the information related. CVM completed the review, and subsequent address lookup, on November 26, 2024. While it has no evidence of misuse of any data, CVM is notifying potentially affected individuals of this incident out of an abundance of caution. The data points potentially impacted for those individuals are name and Social Security number.

On or about December 30, 2024, CVM provided notice via U.S. regular mail of the incident to the potentially affected individuals. A sample copy of the notice is attached as Exhibit "A" for

www.fmglaw.com



Maryland Office of Attorney General
December 31, 2024
Page 2

your records. CVM provided this notification to a total of 18,821 individuals, twelve (12) of whom are residents of the State of Maryland.

As an added precaution, CVM offered the affected individuals twelve (12) months of complementary identity monitoring and protection services (through Equifax). The notice to the affected individuals includes instructions on the use of this product as well as encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, immediately reporting errors or suspicious activity to the financial institution or issuing bank, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. CVM also included contact information for the major consumer reporting bureaus, state-specific regulators, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so.

After discovering the incident, CVM partnered with computer forensic specialists to conduct a comprehensive investigation into the nature and scope of the event. CVM reported the incident to federal law enforcement. CVM also commenced a thorough review of the files that were taken to determine what information was present and to whom the information related and notified those individuals out of an abundance of caution. CVM continues to utilize multi-factor authentication and will continue to assess its policies and procedures already in place for ways to defend against evolving threats. CVM is notifying other state regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit “A”



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

December 30, 2024

Dear [REDACTED]:

Re: Notice of Data Event

Central Valley Meat Co. Inc. and its affiliates is writing to notify you of a recent network event that impacted the security of certain information stored on our company's network. This letter provides an overview of the event and steps we are taking in response, including offering you complimentary access to credit monitoring services. Enrollment instructions for these complimentary services are included within this letter.

What Happened?

On May 23, 2024, Central Valley Meat identified unusual activity on our computer systems that impacted company operations. We took prompt steps to confirm the security of our systems and initiated a comprehensive investigation to determine the extent of impact to our network. From our investigation, we learned that certain files and folders were taken from our network before our systems were disrupted and rendered inaccessible. After confirming some of the accessed locations included employee information, we commenced a thorough review of the files to determine what information was present and to whom the information related. We completed the review, and subsequent address lookup, on November 26, 2024. While we have no evidence of misuse of any data, we are notifying potentially impacted individuals out of an abundance of caution.

What Information Was Involved?

Our investigation confirmed your name, and Social Security number were contained within HR files taken from our network. We reiterate that we have no indication any information was misused, but we are notifying you so that you may take advantage of the resources we are offering you.

What We Are Doing.

We value the privacy and security of employees' information. Upon identifying the unusual activity, we commenced a comprehensive investigation into the nature and scope of the event. We reported to federal law enforcement and will cooperate with any investigation. We continue to utilize multi-factor authentication and will continue to assess our policies and procedures already in place for ways to defend against evolving threats.

As an added precaution, we are offering you 12 months of complimentary identity monitoring and protection services through Equifax. More information on the services, and instructions for how to enroll are enclosed.

What You Can Do.

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing account statements and monitoring free credit reports for suspicious activity and errors. If you find any errors or unauthorized activity, you should contact your financial institution or the appropriate service provider. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed *Additional Steps to Help Protect Your Information* for resources you may take advantage of to protect your information from misuse, should you find it appropriate to do so.

For More Information.

We understand you may have questions about the event. If you have additional questions, please contact our dedicated assistance line at 855-295-4465, which is available from 6:00 AM to 6:00 PM Pacific Time, Monday through Friday (excluding major U.S. holidays). For English Language Learners (ELL), Spanish speaking bi-lingual agents will be available to assist Spanish speaking callers. You may also contact us at 10431 8 ¾ Avenue, Hanford, CA 93230.

Sincerely,

Central Valley Meat Co. Inc.



Enter your Activation Code: [REDACTED]

Enrollment Deadline: [REDACTED]

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of [REDACTED] then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your 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 your email address, create a password, and 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 your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services

LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax
1-888-298-0045
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
1-800-680-7289
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Starting September 21, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. Starting September 21, 2018, you can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **District of Columbia residents:** District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; <https://oag.dc.gov>; 202-727-3400.
- **Maryland residents:** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; <https://www.marylandattorneygeneral.gov> or 1-410-528-8662 or 1-888-743-0023.
- **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 information 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, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; 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 additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; and by contacting Consumer

Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.

- ***New York residents:*** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov>; or 1-800-771-7755.
- ***North Carolina residents:*** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; <https://ncdoj.gov>; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***Rhode Island residents:*** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag.ri.gov or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately [REDACTED] Rhode Island residents potentially impacted by this incident.
- ***All U.S. residents:*** The Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC, 20580; www.identitytheft.gov; 1-877-ID-THEFT; and TTY 1-866-653-4261. This notice has not been delayed by law enforcement.