**NOTICE OF DATA SECURITY INCIDENT**

March 31, 2021

«First\_Name» «Last\_Name»

«Street\_Address»

«City», «State» «Postal\_Code»

Re: Your Wegmans.com Login Information

Dear «First\_Name»:

Wegmans Food Markets, Inc. (“Wegmans”) is writing to inform you of an issue involving the email address and password used for your Wegmans.com account. We take the security of your data seriously, so we ask that you please take a moment to review the summary of this incident attached to this letter.

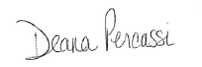
As a result of this incident, we are providing you with credit monitoring for one year. The attached instruction sheet will provide you with important information regarding these services, as well as information on steps that can be helpful in reducing the potential risk of identity theft.

We sincerely apologize for any concern this incident may have caused you. If you have questions please contact Wegmans Customer Care at 1-800-934-6267. We welcome your call and look forward to speaking with you.

Thank you.

Respectfully,

Wegmans Food Markets, Inc.



Deana Percassi

Director, Consumer Affairs

Enc.

**SUMMARY OF WHAT HAPPENED**

Beginning in mid-February 2021, Wegmans became aware of unusual activity involving its website. Following a careful investigation, we learned that an unauthorized party may have used your email address and password to access your Wegmans.com account. Based on our investigation, the credentials used did not come from Wegmans. Instead, it is likely that your login credentials were taken from another source, for example, the compromise of another company or website, where you may have used the same or similar login credentials. This is known as a “credential stuffing” attack, which can occur when individuals use the same login credentials on multiple websites.

**WHAT INFORMATION WAS INVOLVED?**

In addition to your login credentials taken from another source, the unauthorized party may have accessed certain information in your Wegmans.com account. Such information may include: your name, phone number, address, date of birth, and Wegmans Shoppers Club Number.

If you saved your payment card (credit, debit, or stored value card), the attacker was not able to view your payment card information because such information is not stored by Wegmans. Wegmans retains only a “token,” which is linked to your payment card and only our third-party payment card processor retains payment card details. This token cannot be used to make any purchases other than with Wegmans. Accordingly, your credit card information is not at risk because of this incident.

**WHAT ARE WE DOING?**

Immediately upon discovery, Wegmans began an investigation of the incident and worked with law enforcement, Microsoft, and its internal security team to block access by the attackers to Wegmans.com accounts. To restore the confidentiality and security of our systems and prevent any future logins, Wegmans forced a password reset for all affected accounts – including yours – and we are currently monitoring our systems for any further unauthorized logins to Wegmans.com accounts.

**WHAT YOU CAN DO**

In the meantime, you may wish to take some or all of the below actions to help reduce your risk of identity theft.

* Change your password for your Wegmans.com account as well as other online accounts where you used the same email address and password, such as your email, banking, social media, and other retailer accounts. You should not reuse passwords for different online or mobile accounts. We recommend that you review your Wegmans.com account transaction history for unauthorized charges, especially in and around February 2021. If you suspect that any unauthorized charges were made using your account, please contact a Wegmans representative using the contact information below.
* Remain vigilant, especially over the next 12 months, and review your bank accounts, credit card bills and free credit reports for unauthorized activity. Promptly report any suspected identity theft to your local law enforcement agency, the U.S. Federal Trade Commission, the State Attorney General, your financial institution, and to the Fraud Alert phone line of a consumer reporting agency. Telephone numbers for the three national reporting agencies are:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Equifax**  1-800-525-6285  P.O. Box 740256  Atlanta, GA 30374  [www.equifax.com](http://www.equifax.com/) |  | **Experian**  1-888-397-3742  P.O. Box 4500  Allen, TX 75013  [www.experian.com](http://www.experian.com) |  | **TransUnion**  1-800-680-7289  2 Baldwin Place  P.O. Box 1000  Chester, PA 19016  [www.transunion.com](http://www.transunion.com) |

* Periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted. Information relating to our offer of free credit monitoring for a period of one year follows below.
* Place a fraud alert on your credit file by contacting any of the three credit reporting agencies listed above. A fraud alert temporarily, for a period of 90 days, requires potential creditors to take additional steps to verify your identity before issuing credit in your name.
* Place a security freeze on your consumer report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, a security freeze may delay your ability to obtain credit. Please contact one of the three credit reporting agencies listed above for further information.
* Request and carefully review your free annual consumer credit report by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228.

You can also contact the Federal Trade Commission to obtain information about preventing identity theft and, specifically, setting up fraud alerts and security freezes. The contact information for the Federal Trade Commission is as follows:

**Federal Trade Commission**

600 Pennsylvania Avenue, NW

Washington, D.C. 20580

1-877-382-4357

www.ftc.gov

**OTHER IMPORTANT INFORMATION**

As a result of this incident, and to help protect your identity, we would like to offer you a complimentary one-year membership of Experian’s® IdentityWorksSM. This product provides you with superior services pertaining to 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: **6/30/2021** (Your code will not work after this date.)
* Visit the Experian IdentityWorks website to enroll: [https://www.experianidworks.com/credit](https://protect-us.mimecast.com/s/Z1xeC4xKnEtJ4E3QtOsVdn?domain=experianidworks.com).
* Provide your activation code: **«Activation\_Code»**
* Provide the engagement number: **B010864**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian’s customer care team at 877-890-9332 by **6/30/2021**. Be prepared to provide engagement number **B010864** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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.[[1]](#footnote-1)
* 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 ExtendCARETM: 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[[2]](#footnote-2): Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. 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 one year 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 . You will also find self-help tips and information about identity protection at this site.

FOR MORE INFORMATION

If you have questions, please contact us at 1-800-934-6267. Our mailing address is 1500 Brooks Avenue, P.O. Box 30844, Rochester, NY 14603-0844.

Thank you.

1. Offline members will be eligible to call for additional reports quarterly after enrolling. [↑](#footnote-ref-1)
2. 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. [↑](#footnote-ref-2)