LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

April 18, 2020

VIA E-MAIL
Gordon MacDonald, Attorney General
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent PrimoHoagies Franchising, Inc. ("PrimoHoagies"), an Italian specialty sandwich shop headquartered in Westville, New Jersey. This letter is being submitted pursuant to N.H. Rev. Stat. §§ 359-C:19-21, because PrimoHoagies recently learned that a data security incident may have affected customer payment card information, including approximately twenty (20) New Hampshire residents. Based on PrimoHoagies' investigation, it appears that payment cards used by customers for online purchases between July 15, 2019 and February 18, 2020 may be involved. The incident did not impact cards used for in-store purchases. The affected payment card information may have included names, addresses, card numbers, card expiration dates, and security codes.

On February 18, 2020, PrimoHoagies learned that it had been the victim of a malware intrusion after receiving reports from a few cardholders of unusual activity. Immediately upon discovering this, PrimoHoagies worked with industry-leading cybersecurity firms to assist with an investigation. PrimoHoagies also contacted payment card brands (Visa, Mastercard, American Express, Discover) so steps could be taken to prevent fraudulent activity on any affected cards. After the investigation revealed that unauthorized parties had been able to access payment card information, PrimoHoagies then worked to identify potentially impacted customers based on order transactions during the relevant timeframe. On March 23, 2020, PrimoHoagies was able to identify the group of cardholders who could have been affected. In addition to resolving the site security issue, PrimoHoagies also placed additional security on its online payment platform to prevent a similar incident from happening in the future.

PrimoHoagies is completing substitute notice to the potentially affected New Hampshire residents through the use of a press release and a link to the enclosed letter on PrimoHoagies' website and email where an address is known. The home page can be accessed at

https://www.primohoagies.com/orders/important-privacy-notice.php. PrimoHoagies is also offering all impacted customers twelve (12) months of complimentary identity protection and credit monitoring services through ID Experts. These services include: Credit Monitoring, Dark Web Monitoring, Identity Theft Insurance, and Fully-Managed Identity Recovery. PrimoHoagies has established a dedicated call center included in the press release and website notification to provide further information and to assist customers with enrollment in these services.

Please contact me should you have any questions.

Sincerely,

/s/ Richard Goldberg

Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Substitute Notice Letter; Press Release

PrimoHoagies Franchising, Inc.

NEWS RELEASE

PrimoHoagies Notifies Customers of Data Security Incident

Westville, NJ (April __, 2020): PrimoHoagies Franchising, Inc. ("PrimoHoagies" or the "Company") announced today that it had suffered a data security incident, enabling unauthorized parties to access payment card information. Immediately upon discovering this, PrimoHoagies worked with industry-leading cybersecurity firms to assist with an investigation. The Company also contacted payment card brands so steps could be taken to prevent fraudulent activity on any affected cards. In addition, the Company notified law enforcement about this criminal activity and will continue to provide whatever cooperation is necessary to hold the malicious actors accountable.

PrimoHoagies has been working closely with cybersecurity experts and the payment card brands to protect its customers' payment cards. The incident was limited to payment cards used for online purchases only and did not impact cards used for in-store purchases. The issue has since been resolved. PrimoHoagies has also adjusted the payment platform.

Based on the Company's investigation, it appears that payment cards used by customers for online purchases between July 15, 2019 and February 18, 2020 may be involved. The affected payment card information may have included names, addresses, payment card numbers, expiration dates, and security codes.

PrimoHoagies encourages customers to carefully review and monitor their payment card account statements. If a customer believes his or her payment card may have been affected, the customer should immediately contact his or her bank or card issuer. PrimoHoagies has notified payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the identified timeframe. PrimoHoagies is offering complimentary identity protection and credit monitoring services for its customers. Further information for customers including how to enroll in these free services can be found at the PrimoHoagies website at https://www.primohoagies.com/orders/important-privacy-notice.php or by calling its dedicated call center at 1-833-979-2218, Monday through Friday (except holidays) between 9am - 9pm Eastern Time.

About PrimoHoagies:

PrimoHoagies is an Italian specialty sandwich shop headquartered in Westville, New Jersey, with restaurants in eight states across the East Coast.

###

Skip to main content

OLD FASHIONED STYLE
PrimoHoagies
ITALIAN SPECIALTY SANDWICHES

- Start Over
- My Account
- FAQs
- Contact/Questions

Online Ordering

Important Privacy Notice

Customer Notice of Data Security Incident

PrimoHoagies Franchising, Inc. (“PrimoHoagies”) recently learned that its online payment platform had been affected by malware, and that customer payment card information may have been affected. Only online orders were at risk. At PrimoHoagies, we strive to maintain your trust by demonstrating our continued commitment to your security and satisfaction. We are providing this information and offering free resources to help our customers protect their payment card information.

On February 18, 2020, PrimoHoagies learned that it had been the victim of a malware attack, enabling unauthorized parties to access payment card information after receiving notice of unusual payment card activity from a few customers who ordered online. Immediately upon discovering this, we worked with industry-leading cybersecurity firms to assist with an investigation. We also contacted payment card brands so steps could be taken prevent fraudulent activity on any affected cards used for online purchases. In addition, we notified law enforcement about this criminal activity and will continue to provide whatever cooperation is necessary to hold the malicious actors accountable.

The problem with the online payment system has been resolved and the security for online ordering has been improved to prevent a similar incident from happening in the future.

Based on our investigation, it appears that payment cards used by customers for online purchases between July 15, 2019 and February 18, 2020 may be involved. The affected payment card information may have included names, addresses, payment card numbers, expiration dates, and security codes.

We encourage our customers to carefully review and monitor their payment card account statements. If a customer believes their payment card may have been affected, they should immediately contact his or her bank or card issuer. We have notified payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the identified timeframe. We are also offering complimentary identity protection and credit monitoring services for our customers. Further information for customers including how to enroll in these free services can be found by calling our dedicated call center at 1-833-979-2218, Monday through Friday (except holidays) between 9am - 9pm Eastern Time.

The privacy and protection of customer information is essential for us. We deeply regret any inconvenience or concern this incident may cause.

We are also providing the following information to help those wanting to know more about steps they can take to protect themselves:

What steps can I take to protect my personal information?

- If you detect any suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- Obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed below.
- Please notify your financial institution immediately of any unauthorized transactions made or new accounts opened in your name.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identity theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification below.

What should I do to protect myself from payment card/credit card fraud?

We suggest you review your debit and credit card statements carefully for any unusual activity. If you see anything you do not understand or that looks suspicious, you should contact the issuer of the debit or credit card immediately.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is also included below:

Equifax
P.O. Box 105851
Atlanta, GA
30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Free Annual Report
P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

How do I put a fraud alert on my account?

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

How do I put a security freeze on my credit reports?

You also have the right to place a security freeze on your credit report. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. A security freeze may be placed or lifted free of charge.

You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian Security Freeze
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion (FVAD)
PO Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

Additional Free Resources:

You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state:

Federal Trade Commission
600 Pennsylvania Ave, NW Washington, DC 20580
consumer.ftc.gov, and www.ftc.gov/idtheft
1-877-438-4338

Residents of Maryland can obtain more information from their Attorney General using the following contact information: Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, oag.state.md.us, 1-888-743-0023.

Residents of North Carolina can obtain more information from their Attorney General using the following contact information: North Carolina Attorney General, 9001 Mail Service Center, Raleigh, NC 27699, https://ncdoj.gov, 1-877-566-7226.

Residents of Rhode Island can obtain more information from their Attorney General using the following contact information: Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.