PIERSON FERDINAND

JONATHAN E. (JED) DAVIS
PARTNER

Mail
612 10TH STREET
BROOKLYN NY 11215

Office
PIERSON FERDINAND LLP
1270 AVENUE OF THE AMERICAS
7TH FLOOR—1050
NEW YORK, NY 10020

Direct: 917-725-1340
Email: JED.DAVIS@PIERFERD.COM

January 24, 2024

VIA MAINE-AG PORTAL

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

To the Office of the Maine Attorney General:

Pierson Ferdinand LLP represents Bake 'N Joy Foods, Inc. ("Bake 'N Joy"), located at 351 Willow Street South, North Andover, MA 01845, with respect to a data security incident at third-party ecommerce provider, CommerceV3, Inc ("CV3"). Bake 'N Joy takes very seriously the security and privacy of its customers' information. As further described below, it has worked extensively to assure that affected customers receive clear notification despite the underlying data's complexity. In addition, Bake 'N Joy is reviewing its future ecommerce options after having previously secured CV3's written assurances that it has overhauled its cybersecurity.

Description of the Incident.

CV3 receives and processes online orders placed by (among others) online customers of Bake 'N Joy' baked goods marketed under the Boston Coffee Cake brand. On or about June 27, 2023, CV3 provided Bake 'N Joy with a data file listing the names of numerous Boston Coffee Cake customers, their address information and credit card information. CV3 indicated that the file resulted from a forensic investigation on its behalf into an unauthorized access data incident involving its platform.

As Bake 'N Joy has since learned, CV3's forensic investigation determined that from in or about and between November 24, 2021 and December 14, 2022, an unauthorized third party had persistent access to CV3's ecommerce platform. CV3's investigation, which encompassed a data mining exercise, established that during the 13 months in question, the unauthorized person may have accessed and/or acquired details entered by online customers of Boston Coffee Cake, including payment card number, CVV code, expiration date, together with customer name, email address and billing address.

As of this writing, Bake 'N Joy has received no reports indicating that fraud or identity theft resulted from the above intrusion.

Number of Maine residents affected.

Bake 'N Joy's analysis establishes that the cybersecurity incident at CV3 may have resulted in the unauthorized exposure of information pertaining to 149 Boston Coffee Cake customers who are residents of Maine. Notification letters to these individuals are being mailed today, January 24, 2024, via First Class Mail. A sample copy of the notification letter is attached as **Exhibit A**.

Steps taken.

Bake 'N Joy collaborated at length and extensively with a data contractor and counsel to develop a dataset that had enabled it to issue mailed notifications that apprise each of the approximately 21,914 potentially affected Boston Coffee Cake customers of the date(s) of their respective purchases within the 13-month window of compromise at CV3. This took more time and effort than many incident notification efforts, due to hidden assumptions and missing order dates in CV3's June 2023 production, compounded by the frequency with which customers placing multiple orders rendered the same names and addresses differently. Solving these challenges, however, made it possible for Bake 'N Joy to provide customers with requisite notice. Each notification letter informs its recipient exactly when a stated order was placed. Likewise important, letters to the many customers who ordered multiple times in the subject interval have been sent customized letters that consolidate notice about most or all of their respective order dates.

Bake 'N Joy is also offering to all of its potentially affected customers the option to enroll for one year, prepaid, in credit monitoring services provided by CyberScout.

In addition, Bake 'N Joy is working to keep its ecommerce function secure. It has obtained written assurance from CV3 that it has made a series of cybersecurity upgrades to its platform. Bake 'N Joy is also evaluating options for when it next puts its ecommerce account out for bid.

Contact information.

Please contact me should you have any questions or concerns about this matter. My email address is Jed.Davis@PierFerd.com and my phone number is (917) 725-1340.

Sincerely,

PIERSON FERDINAND LP

Jonathan E. Davis

_____

By: Jonathan E. Davis

Attachment

EXHIBIT A

Bake 'N Joy Foods, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998
Via First-Class Mail
P
JOHN DOE
103 ROE ST
DOMANIA NY

January 24, 2024

Notice of Data Breach
Boston Coffee Cake Order(s) Dated:
10/02/2022 17:31

0000101102G0500

P

Dear John Doe:

We write to inform you of a recent data security incident at our e-commerce provider, CommerceV3 ("CV3") that may have affected your personal information. Based on our current review, we have no indication that your personal information has been or will be used inappropriately, but we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on the steps you can take to help protect your information. We take the protection and proper use of your information seriously and are working to prevent a recurrence of the incident. This notification was not delayed by law enforcement.

Why Does CommerceV3 Have my Information?

You are a customer of ours who via our website, purchased our Boston Coffee Cake brand baked goods. CV3 is a third-party provider of an e-commerce platform that we use to receive and process Boston Coffee Cake order details, including payment card information, that you enter online.

What Happened

On June 27, 2023, CV3 informed us that it had concluded an investigation with the assistance of third-party cybersecurity experts establishing that an unauthorized person had access to CV3's ecommerce platform from November 24, 2021 through December 14, 2022. The investigation determined that the data accessible to the unauthorized person included credit card details that our customers and customers of other CV3 clients had submitted with their orders. These types of incidents are unfortunately becoming increasingly common, such that even organizations with highly sophisticated IT infrastructure available are affected.

In the course of its June 2023 disclosure, CV3 provided us with a data file listing information identifying Boston Coffee Cake customers whose order details may have been impacted. That file, however, did not indicate when or how often during the above period our customers, including you, had placed orders. Since that disclosure, we have worked to obtain and intensively analyze this and additional CV3 data together. This in turn has enabled us to notify you about each of your order dates and if you placed multiple orders, to consolidate notifications to you in one notification or few.

What Information Was Involved

The elements of your personal information that may have been impacted may have included, and potentially were not limited to your payment card number, CVV code and expiration date, together with your name, email and billing address. Note that we have no evidence that your personal information was misused due to the incident.

Our analysis established that under name and address listed above, you ordered Boston Coffee Cake Products from our online store on the following date(s) between November 24, 2021 and December 14, 2022:**10/02/2022 17:31**.

What We Are Doing

We take this incident seriously. We have required CV3 to provide written assurance that it has enhanced its cybersecurity in ways that reduce the likelihood of another incident. We are also monitoring CV3's performance.

In an abundance of caution, we are also making available to you, free of charge, enrollment for twelve months from Cyberscout through Identity Force, a TransUnion company. This package includes credit monitoring, a credit report, credit score and identity fraud protective services that provide proactive antifraud assistance and remediation to help with any questions that you might have or in the event that you become a victim of fraud.

What You Can Do

We know of no person who has been defrauded as a result of the unauthorized access to CV3's system. Data frauds are not uncommon, however. We therefore recommend that you review the next few pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes on your personal credit cards.

To enroll in the complimentary services we are offering you, please visit **https://secure.identityforce.com/benefit/bnjf** and follow the instructions. When prompted please provide this code: **CHTUEMLCVR.** To receive the above monitoring services, you must enroll within ninety (90) days from the date on this letter. This service will not affect your credit score.

To activate monitoring services, you will need an internet connection and e-mail account. You may also be required to provide your name, date of birth, and Social Security number to confirm your identity. Under privacy laws, we cannot register you directly. Certain services might be unavailable to individuals without a credit file at the credit bureaus or an address in the United States (or its territories) and a valid Social Security number.

For More Information

We regret any inconvenience or concern this incident may cause. Protecting your personal information is our top priority. If you have questions, please call 1-833-961-6695, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Mark Forman

Director, Business Development and Ecommerce
Bake 'N Joy Foods, Inc.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with
Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
TransUnion (https://www.transunion.com/fraud-alerts);
or Experian (https://www.experian.com/fraud/center.html).
A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, 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 requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia*:It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Maryland, Rhode Island, Illinois, New York, and North Carolina*: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.