



Baker McKenzie LLP
300 East Randolph St.
Ste. 5000
Chicago, IL 60601
United States
Tel: +1 312.861.8000
www.bakermckenzie.com

April 29, 2024

VIA EMAIL

Maryland Attorney General
idtheft@oag.state.md.us

RE: Data Breach Reporting

Dear Mr. Brown:

We are writing on behalf of our client Panda Restaurant Group, Inc. ("PRG") to provide notice regarding a data security incident involving **three-thousand one-hundred and sixty-six (3166)** Maryland residents. By providing this notice, PRG does not waive any rights or defenses regarding the applicability of Maryland law and/or waive the attorney-client privilege and/or work product doctrine.

Nature of the Incident

On March 10, 2024, PRG detected a data security incident that resulted in the encryption of PRG's virtual corporate network (the "Incident"). Upon discovery of the Incident, PRG immediately engaged Baker McKenzie ("Counsel") to provide legal advice and conduct a privileged investigation. Counsel engaged third-party experts on behalf of PRG and under privilege to help respond to the Incident. These vendors worked at the direction of Counsel. After a thorough investigation, PRG determined that certain information maintained on its corporate network was accessed by an unauthorized actor ("UA") between March 7-11, 2024. PRG also cooperated with federal law enforcement in their active investigation of the UA responsible for this incident.

On April 15, PRG concluded its review of impacted data and determined that the personal information of **three-thousand one-hundred and sixty-six (3166)** Maryland residents was involved in the Incident. The information subject to unauthorized access included social security number, passport number, other identification numbers issued by the federal government, driver's license number, state identification card number, financial account number, health information, and health insurance policy number.

In response to the Incident, PRG has taken steps to prevent reoccurrence, including, but not limited to, implementing technical safeguards such as password resets and rotations, additional firewall segmentation, and deploying additional endpoint monitoring and threat hunting technologies across the corporate network. PRG has also engaged a third-party to conduct ongoing dark web monitoring and threat intelligence services.

Notification to Three-Thousand One-Hundred and Sixty-Six (3166) Maryland Residents

PRG is providing customized notice to each affected individual which includes the specific data elements impacted for each individual. Additionally—even though the law may not require it in all jurisdictions—PRG is providing **all** individuals impacted with a minimum of twelve (12) months of free identity-theft protections services. Notice to these individuals will be mailed by USPS on or about April 30, 2024. Enclosed for your reference is a sample of the notice.

Contact Information

Please feel free to contact me with any questions at Justine.Phillips@bakermckenzie.com or (310) 201-4728.

A handwritten signature in black ink that reads "Justine Phillips". The script is fluid and cursive, with the first letters of each word being capitalized and prominent.

Justine Phillips,
Partner

Baker & McKenzie LLP is a member of Baker & McKenzie International.



<<Name 1>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>,

Panda Restaurant Group, Inc., and its affiliates, subsidiaries and related entities ("Panda") is writing to inform you of a data security incident that involved your personal information. Panda is committed to protecting your personal information, which is why we are writing to explain what happened, what information was involved, our response, and resources available to further protect your personal information.

WHAT HAPPENED?

On March 10, 2024, Panda detected a data security incident that impacted certain corporate systems. The incident did not impact our in-store systems, operations or guest experience. Upon detecting this incident, we took immediate action to secure our environment, activated our remediation and recovery efforts, and launched a thorough investigation in partnership with third-party cybersecurity specialists to determine the nature and scope of the incident. We also worked with law enforcement.

After a thorough investigation, we determined that certain information maintained on our corporate systems was accessed by the unauthorized actor between March 7-11, 2024. With the support of third-party experts, we then began a thorough review of the data affected to identify the specific information and individuals impacted. On April 15, we concluded our review of impacted data and determined that your personal information was involved.

WHAT INFORMATION WAS INVOLVED?

The types of information involved include your first and last name, in combination with your <<Breached Elements>><<Variable Data1>>. Although we have no evidence of misuse of the information involved in this incident, we include steps you can take to further protect your personal information.

WHAT WE ARE DOING.

We have taken the steps necessary to address the incident and are committed to protecting the information you have entrusted to us. Immediately upon detecting this incident, we took steps to secure our environment from further risk, began remediation and recovery efforts, and launched a thorough investigation in partnership with third-party cybersecurity experts. We continue to work with law enforcement who are conducting an active investigation into the unauthorized actor responsible for this incident. Panda also implemented additional technical safeguards to further enhance the security of information in our possession and to help prevent similar events from happening in the future.

In addition, we are offering you a complimentary <<12/24>>-month membership of CyEx's Identity Defense Total – 3 Bureau credit monitoring and identity protection services. Steps to enroll in this service are detailed below. This service helps detect possible misuse of your personal information, provides you with identity protection support and helps with resolution of identity theft. Its services include credit reports, credit monitoring, and identity restoration support.

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/panda and follow these instructions:

- 1. Enter Your Unique Activation Code <<Activation Code>>**
Enter your Activation Code and click 'Redeem Code'.
- 2. Create Your Account**
Enter your email address, create your password, and click 'Create Account'.
- 3. Register**
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
- 4. Complete Activation**
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>> you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at (866) 622-9303.

WHAT YOU CAN DO.

In addition to utilizing the credit monitoring and identity theft protection program above, we recommend that you remain vigilant against incidents of identity theft and fraud by regularly reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We are providing additional information below about steps you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report.

FOR MORE INFORMATION.

We deeply regret any concern this incident may cause. If you have any further questions regarding this incident, please call the dedicated and confidential toll-free telephone line at (888) 680-7642. The response line is available from 6 am PT to 6 pm PT.

Sincerely,
PANDA RESTAURANT GROUP, INC.



Bryan Lim
Vice President of Information Systems

Steps You Can Take to Protect Against Identity Theft and Fraud

Order Credit Report

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Place A Fraud Alert

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742.	1-800-525-6285 or 1-888-766-0008	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division PO Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.experian.com/fraud/center.html	https://www.equifax.com/personal/credit-report-services/	https://fraud.transunion.com/fraudAlert/landingPage.jsp

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Place A Security Freeze

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all your credit files. To find out more on how to place a security freeze, you can use the following contact information:

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.experian.com/freeze/center.html	https://www.equifax.com/personal/credit-report-services	https://www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security Number
3. Date of Birth
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Social Security Card, pay stub, or W2
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, via their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that 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 can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; Telephone: 1-888-743-0023; www.oag.state.md.us/Consumer

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway, 3rd Floor New York, NY 10271 (800) 771-7755 www.ag.ny.gov	New York Department of State Division of Consumer Protection 99 Washington Avenue, Suite 650 Albany, NY 12231 (800) 697-1220 www.dos.ny.gov
---	--

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: 1-919-716-6400; www.ncdoj.gov

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us

Washington D.C. Residents: You can obtain additional information about the steps you can take to avoid identity theft from the DC Office of the Attorney General at <https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>. You may also contact the DC Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and oag@dc.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.