

November 6, 2023

VIA EMAIL: idtheft@oag.state.md.us

The Honorable Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Notice of Data Breach

Dear Attorney General Brown:

I am writing on behalf of Performance Food Group, Inc. (“PFG” or the “Company”), with its headquarters located at 12500 West Creek Parkway, Richmond, VA 23238, to provide a report of a recent data breach. PFG is a food products distributor. On June 21, 2023, PFG’s information technology team discovered that, beginning on May 16, 2023, a Company email account had been compromised and used by an unauthorized individual to send large quantities of “phishing” emails. PFG then engaged a professional forensic investigator and working with that team, identified several more accounts that appeared to be accessed without authorization. The forensic investigator provided an initial report on October 9, 2023 regarding the personal information that was contained in the involved accounts.

So far, there is no evidence that any personal information was exfiltrated or otherwise removed from PFG’s servers but it does appear that the unauthorized individual had access to it. PFG has no indications that any of the data has been used for fraudulent purposes, nor are we aware of any resulting identity theft, fraud, or financial losses. Nevertheless, out of an abundance of caution, the Company is notifying the individuals whose information was located in the impacted accounts that their personal information may have been exposed.

The impacted accounts included the personal information of 44 Maryland residents. The personal information disclosed in the incident included name together with some combination of the following: date of birth, driver's license or state issued ID number, financial account number, financial institution name, Social Security Number, credit/debit card number, digital signatures, and treatment information/diagnosis. Formal, written notices are being sent to the impacted individuals on November 8, 2023.

PFG has taken actions to mitigate the incident, including successfully locking out the unauthorized users from the Company’s system and undertaking a full forensic investigation of

the incident. In addition, the Company is offering the impacted individuals a complimentary 12-month membership to Kroll's Credit Monitoring, Fraud Consultation, and Identity Theft Restoration, as well as a current credit report.

A copy of the template form of the notification letter that will be sent to the affected Maryland residents is included with this notice. As you will see, among other things, the letter (i) describes various steps that affected individuals can take to protect themselves, (ii) provides contact information for consumer reporting agencies and relevant governmental agencies, and (iii) provides information about enrolling in 12 months of credit monitoring services, which the Company is offering to the affected individual at no cost. An appendix is also enclosed with the letter, which will serve as a key for your reference to the "text" field in the letter, which is a variable depending on the particular personal information involved.

If you have any questions about the information provided in this letter, or this incident generally, please feel free to contact me at the email or phone numbers listed above.

Sincerely,



Janet P. Peyton

Enclosures: Template Form Notification Letter and Appendix



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

I am writing to you on behalf of Performance Food Group, Inc. ("PFG" or the "Company") with important information about a data security incident that occurred at PFG. PFG takes the protection and proper use of your personal information very seriously. We are, therefore, contacting you to explain the incident and provide you information about security measures you can take to protect yourself and your personal information.

What Happened:

On June 21, 2023, PFG's information technology team discovered that, beginning on May 16, 2023, a Company email account had been compromised and used by an unauthorized individual to send large quantities of "phishing" emails. PFG then engaged a professional forensic investigator and working with that team, identified several more accounts that appeared to be accessed without authorization. The forensic investigator provided an initial report on October 9, 2023, regarding the personal information that was contained in the involved accounts. This notice was not delayed as the result of a law enforcement investigation.

What Information Was Involved:

So far, there is no evidence that any personal information was exfiltrated or otherwise removed from PFG's servers, but it does appear that the unauthorized individual had access to it. PFG has no indications that any of the data has been used for fraudulent purposes, nor are we aware of any resulting identity theft, fraud, or financial losses. Personal information potentially disclosed as a result of this incident included your: <<b2b_text_1(data elements)>>. Again, while we do not know whether your personal information was in fact accessed or used for any unauthorized purpose, we are sending you this notice as a precautionary action.

What We Are Doing:

We have taken actions to mitigate the incident, including successfully locking out the unauthorized users from the Company's system and undertaking a full forensic investigation of the incident.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

What You Can Do:

Please review the "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also report any suspected incident of identity theft to law enforcement, and you can obtain a copy of any resulting police report. If you do suspect that you have been the victim of identity theft, you should also notify your state Attorney General and the FTC.

For More information:

If you have questions, please call [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

We sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "A. Brent King". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

A. Brent King
Executive Vice President, General Counsel and Secretary

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: This incident impacted 23 Rhode Island residents. You may contact the RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400; <http://www.riag.ri.gov/ConsumerProtection/About.php#>

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

ChexSystems

If your bank account information was involved in the incident, you may place a security alert and/or security freeze with ChexSystems by visiting <https://www.chexsystems.com> or calling (800) 428-9623.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Appendix to Notification Letter for Maryland Residents

Text 1 = One of the following:

- date of birth
- date of birth, driver's license or state issued ID number, account number, and financial institution name
- date of birth, Social Security number, account number, financial institution name, and credit/debit card number
- digital signatures
- Social Security number
- treatment information/diagnosis

December 11, 2024

VIA EMAIL: idtheft@oag.state.md.us

The Honorable Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Supplemental Notice of Data Breach

Dear Attorney General Brown:

I am writing on behalf of Performance Food Group, Inc. (“PFG” or the “Company”), with its headquarters located at 12500 West Creek Parkway, Richmond, VA 23238, to provide a updated report of a data breach. This notice is to supplement our previous notice dated November 6, 2023. As indicated in our November 6 letter to you, PFG sent notification letters to many of the impacted individuals on November 8, 2023. At the time, however, there were a number of individuals for whom PFG did not have a mailing address readily available. Shortly thereafter, PFG engaged a third-party vendor to search public records to find mailing addresses for the remaining individuals.

Upon completion of its extensive research, the vendor provided PFG an updated report with mailing addresses for additional impacted individuals on November 8, 2024. The missing address results have revealed 34 additional Maryland residents whose information was impacted in the incident, bringing the total impacted Maryland residents to 78. A copy of the template form of the notification letter that will be sent to these individuals on December 12, 2024, is attached with this notice. The types of personal information involved for these 78 Maryland residents included a combination of the following: date of birth, driver's license or state issued ID number, financial account number, financial institution name, Social Security Number, credit/debit card number, digital signatures, incidental health reference, treatment information/diagnosis, treatment cost information, and treating/referring physician. All of the other information provided in our initial letter remains the same.

The Honorable Anthony G. Brown
December 11, 2024
Page 2

If you have any questions about the information provided in this letter, or this incident generally, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

A handwritten signature in blue ink, appearing to read "Janet P. Peyton", with a stylized flourish at the end.

Janet P. Peyton

Enclosures: Template Form Notification Letter and Appendix

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: Notice of Data Breach

Dear <<first_name>> <<last_name>>:

I am writing to you on behalf of Performance Food Group, Inc. (“PFG” or the “Company”) with important information about a data security incident that occurred at PFG. PFG takes the protection and proper use of your personal information very seriously. We are, therefore, contacting you to explain the incident and provide you information about security measures you can take to protect yourself and your personal information.

What Happened:

On June 21, 2023, PFG’s information technology team discovered that, beginning on May 16, 2023, a Company email account had been compromised and used by an unauthorized individual to send large quantities of “phishing” emails. PFG then engaged a professional forensic investigator and working with that team, identified several more accounts that appeared to be accessed without authorization. The forensic investigator provided an initial report on October 9, 2023 regarding the personal information that was contained in the involved accounts. Unfortunately, we did not have current mailing addresses readily available for some people that were identified in that report. To date, our records indicate that we did not have an accurate address for you when the initial notifications were sent. Since then, PFG has continued to work both internally and with an outside vendor to identify current addresses for each of the impacted individuals. Our vendor identified this address for you on November 8, 2024. This notice was not delayed as the result of a law enforcement investigation.

What Information Was Involved:

So far, there is no evidence that any personal information was exfiltrated or otherwise removed from PFG’s servers but it does appear that the unauthorized individual had access to it. PFG has no indications that any of the data has been used for fraudulent purposes, nor are we aware of any resulting identity theft, fraud, or financial losses. Personal information potentially disclosed as a result of this incident included your: <<b2b_text_1 (data elements)>>. Again, while we do not know whether your personal information was in fact accessed or used for any unauthorized purpose, we are sending you this notice as a precautionary action.

What We Are Doing:

Throughout the remainder of 2023, we took steps to mitigate the incident, including successfully locking out the unauthorized users from the Company’s system and undertaking a full forensic investigation of the incident.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do:

Please review the “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also report any suspected incident of identity theft to law enforcement, and you can obtain a copy of any resulting police report. If you do suspect that you have been the victim of identity theft, you should also notify your state Attorney General and the FTC.

For More information:

If you have questions, please call **(866) 347-8057**, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

We sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,



A. Brent King
Executive Vice President, General Counsel and Secretary

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, <http://www.equifax.com>, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: This incident impacted twenty-six (26) Rhode Island residents. You may contact the RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400; <http://www.riag.ri.gov/ConsumerProtection/About.php#>

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

ChexSystems

If your bank account information was involved in the incident, you may place a security alert and/or security freeze with ChexSystems by visiting <https://www.chexsystems.com> or calling (800) 428-9623.

**TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Appendix to Notification Letter for Maryland Residents

Text 1 = One of the following:

- Date of Birth
- date of birth, driver's license or state issued ID number, account number, and financial institution name
- date of birth, Social Security number, account number, financial institution name, and credit/debit card number
- Date of Birth, Treatment Information/Diagnosis, Treating/Referring Physician, and Treatment Cost Information
- digital signatures
- Incidental Health Reference
- Social Security number
- Treatment Information/Diagnosis