Performance Food Group
Customized Distribution
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
R825701

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 19, 2018

Dear John Sample,

Notice of Data Breach

We are writing to you because of an incident at Performance Food Group, Inc. ("PFG"), specifically within the PFG Customized segment ("PFG Customized").

What Happened

On August 20, 2018, we learned that an unauthorized individual took advantage of vulnerability in the configuration of the app that PFG uses for PFG Customized team members to access their email remotely. As a result, we have reason to believe that one or more unauthorized individuals may have accessed email of current and former employees dating as far back as 2011. Because we cannot be certain who within the PFG Customized segment may have been affected, we are notifying all current and former PFG Customized employees out of an abundance of caution.

What Information was Involved

We do not have specific detail about the information that may have been affected, but it is possible that the following may have been affected: name, address, Social Security number, and driver's license number.

What We Are Doing

In addition to providing you this notice, we have notified law enforcement and have been working with the FBI and local law enforcement to investigate this incident. This notice has not been delayed by a law enforcement investigation.

Furthermore, promptly following discovery of the system vulnerability, we made changes to the remote access system to prevent further unauthorized access, and we required all employees to update their passwords.

What You Can Do

We recommend that you place a fraud alert on your credit files as soon as possible, as it is possible that your Social Security number was involved in this breach. The applicable numbers for the credit reporting agencies are listed on the insert enclosed with this letter titled, "*Information About Identity Theft Protection.*"

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-9831 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-9831 using the following redemption code: [redacted]

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

We want to make you aware of other steps you may take to guard against identity theft or fraud. Please review the attachment to this letter for further information on steps you can take to protect your information, including toll-free numbers and addresses for each of the three credit reporting agencies (Equifax, Experian and TransUnion), and the Federal Trade Commission. You can obtain additional information from these sources about steps to avoid identity theft.

We encourage you to remain vigilant, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Finally, as always, we urge you to be cautious with your on-line accounts. You should use complex passwords for your accounts that are unique for each account. You should not share your password with anyone. And, you should notify PFG's Information Security department at Information_Security@pfgc.com immediately if you suspect any issues with the privacy or security of any PFG electronic systems.

For More Information

We take our responsibility to safeguard personal information seriously, and we regret any inconvenience or concern this incident may cause you and remain committed to protecting the privacy and security of personal information. If you have any questions about this situation, please do not hesitate to contact us by emailing Debbie Roberts, Vice President, HR, at droberts@pfgcd.com or call our dedicated assistance line at 1-855-836-9831, Monday through Saturday, 9 a.m. through 9 p.m. ET.

Sincerely,

Craig Hoskins
President & CEO, PFG Customized

INFORMATION ABOUT IDENTITY THEFT PROTECTION

There are other steps you can take to further protect yourself against identity theft or other unauthorized use of personal information.

- We recommend that you remain vigilant and regularly review your account statements and credit reports for any unauthorized activity. Promptly report incidents of suspected identity theft or fraud to your local law enforcement agency, the Federal Trade Commission, your financial institution and to one of the three nationwide consumer reporting agencies listed below to have it removed from your credit file.

- You may contact the fraud departments of the three nationwide credit reporting agencies to discuss your options. You have the right to place a free 90-day fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. It also may delay your ability to obtain credit. To place a fraud alert on your credit report contact the three credit reporting agencies above.

- You may obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or going online to www.annualcreditreport.com. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may want to obtain copies of your credit report to ensure the accuracy of the report information. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report.

- You can create an account with Credit Karma by visiting https://www.creditkarma.com/ to track your TransUnion and Equifax credit accounts daily. You can also receive credit alerts if anything important changes on your TransUnion credit report that can help you spot identity theft.

- You have a variety of rights under the federal Fair Credit Reporting Act (FCRA). For more information on your FCRA rights, visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

- You may place an alert with ChexSystems. Chex Systems, Inc. is a consumer-reporting agency governed by the FCRA and other laws (the Federal Trade Commission enforces the FCRA) which provides account verification services to its financial institution members to aid them in identifying account applicants who may have a history of account mishandling (for example, people whose accounts were overdrawn and then closed by them or their bank). In short, ChexSystems is like the credit reporting agencies (Equifax, Experian, TransUnion) but specific to checking/savings history instead of credit/loan history. ChexSystems has two protections available:

    - **Consumer Report Security Alert.** This puts a flag on your consumer file stating the banking institution needs to take additional steps to confirm it is you who is initiating the action (much like placing a fraud alert with the credit reporting agencies). You may request a 90-day alert, which is the default, though you may extend it to 7 years if you complete the ChexSystems ID Theft affidavit form (available online), have the affidavit notarized, and send the notarized affidavit to ChexSystems. To set the Consumer Report Security Alert, call (888) 478-6536 or online by visiting https://www.chexsystems.com.

- **Consumer Report Security Freeze**. This will prohibit ChexSystems from releasing any information in your consumer file without your express authorization, meaning you have to contact ChexSystems and lift the freeze in order for your information to be released (much like placing a freeze with the credit reporting agencies). You should be aware that taking advantage of this right may delay or prevent timely approval from any user of your consumer report that you wish to do business with. The third party will receive a message indicating that you have blocked your information. To set the Consumer Report Security Freeze, call (800) 887-7652 or online by visiting https://www.chexsystems.com.

- To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Experian
Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

TransUnion
Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

For other inquiries:
Experian
(888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

For other inquiries:
Equifax
(877) 478-7625
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

For other inquiries:
TransUnion
(800) 680-7289
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

- In order to request a security freeze, you will need to provide the following information:

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, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, report it to your local police department and obtain a copy of the police report, investigative report or complaint. Send a copy of the police report, investigative report, or submitted complaint concerning identity theft to each consumer reporting agency;
8. If you are not a victim of identity theft, include payment for the fees by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail. Fees are specified by each of the major consumer reporting agencies. Fees vary based on where you live, but commonly range from $5 to $10.

- The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. 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.

- To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (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 or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

- To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For More Information

- To learn more about fraud alerts, security freezes, and protecting yourself from identity theft and to report incidents of identity theft, you can visit the Federal Trade Commission's website at www.consumer.gov/idtheft, or www.ftc.gov/credit, or call 1-877-IDTHEFT (1-877-438-4338). You may also receive information from the Federal Trade Commission by writing to:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

- For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

- For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077