<<Name 1>> <<Name 2>> <<Date>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

NOTICE OF PAYCOR SECURITY EVENT

Dear <<Name 1>> <<Name 2>>:

We are writing to inform you of a security event that involves your personal information. Matthews International (Matthews) has been notified that our payroll processor, Paycor Inc. (Paycor), inadvertently shared your personal information with an unauthorized third party. Matthews takes this event and the security of your personal information very seriously. This letter explains what happened, our response, and resources available to you to help protect your information, including an identity protection service that Matthews will pay for.

What Happened?
Paycor contacted Matthews and notified us that on January 9, 2024, a third party impersonating a Matthews employee contacted Paycor by telephone to request a payroll report for the Matthews payroll unit that includes you. Believing the actor was an authorized Matthews employee, the Paycor representative emailed the report to the unauthorized third party. Matthews was first informed of this unauthorized event on January 25, 2024, after Paycor's internal investigation confirmed the breach and Paycor's failure to follow its established policies for the security of personal information.

Since being notified, Matthews has thoroughly investigated the incident and its impact on you, other employees and our company. Our review also determined that no Matthews systems were compromised in this event, and that the breach was confined to the information shared by Paycor and this single Matthews payroll group. We also confirmed that there were no communications from Matthews' systems with the email address that the third-party provided Paycor.

What Information was Involved.
Paycor has advised that the following types of information was impacted: full name, address, birth date, social security number, compensation details, hire date, and in some cases, telephone number.

What We Are Doing.
While we have no evidence that any of your personal information has been misused, we take this event and the security of your personal information very seriously. Here are actions that we are taking:

- Matthews is providing you with Allstate Identity Protection, free of charge for up to two (2) years.
- We commenced our own investigation into the event and immediately initiated our response to the security incident, including notifying you and other affected individuals.
- As required by law, we have notified state regulators.
- We confirmed that our standards and processes for vendors who handle sensitive information meet industry standard practices.
- We confirmed with Paycor that protective measures are in place to prevent further impersonation of Matthews employees with access to sensitive personal information in the future.
- We conducted a complete access review of the individuals with Paycor access to confirm that only authorized Matthews' personnel have access to employee information at Paycor.
- We will be closely monitoring Paycor's actions going forward and holding Paycor to strict compliance with our vendor standards and their policies.

What You Can Do.

1. *Activate Your Allstate Identity Protection coverage.* This coverage provides identity, privacy, and device protection. In the next week or so, you will receive a Welcome Activation email from CustomerCare@aip.com with your Allstate Member ID and a link to log in to your online portal. You will also receive a welcome letter in the mail soon after. ***You must complete the activation process yourself, Matthews is not permitted to activate your services on your behalf.***

2. *Remain vigilant.* We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors.

For information on how to activate your Allstate Identity Protection and regarding credit and identity monitoring, review the enclosed *Steps You Can Take to Help Protect Your Information*.

For More Information.

If you have additional questions, or need assistance, please contact the Matthews HR Service Center by email (HRService@matw.com) or phone (1.855.435.7440, option 2). The Service Center is available Monday through Friday, 8:00 a.m. and 5:00 p.m. Eastern Time, excluding major U.S. holidays.

We apologize for any inconvenience to you and remain dedicated to protecting the information in our care.

Sincerely,

Ronald C. Awenowicz
Senior Vice President – Human Resources
Matthews International Corporation
Two NorthShore Center
Pittsburgh, PA 15212

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Allstate Identity Protection

This coverage provides identity, privacy and device protection. In the next week or so, you will receive a Welcome Activation email from CustomerCare@aip.com with your Member ID and a link to log in to your online portal. This is a legitimate communication, and you can expect to receive identity alerts from this email address in the future. You will also receive a welcome letter in the mail soon after.

Your coverage includes:

- Comprehensive identity monitoring
- Cyber protection for personal mobile devices
- Credit monitoring
- Unlimited TransUnion reports and scores
- Dark web monitoring
- High-risk transaction monitoring
- Financial transaction monitoring
- Allstate Security Pro℠ for real-time emerging threat alerts
- Allstate Digital Footprint℠ for privacy management
- Social media monitoring
- IP address monitoring
- Full service 24/7 fraud remediation
- Up to $2 million identity theft and ransomware expense reimbursement
- Pre-existing conditions covered at no additional charge

You must complete the activation process yourself, Matthews is not permitted to activate you in these services on your behalf.

If you have trouble logging in or have additional questions, please call Allstate Identity Protection at 1.855.907.3282 or email clientservices@aip.com. They are available 24/7 to ensure you have help when you need it most.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1.877.322.8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert or learn more about fraud alerts, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a

credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

EQUIFAX	**EXPERIAN**	**TRANSUNION**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1.888.298.0045	1.888.397.3742	1.800.916.8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1.877.ID.THEFT (1.877.438.4338); and 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1.410.528.8662 or 1.888.743.0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

***For New York residents**,* the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1.800.771.7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1.877.566.7226 or 1.919.716.6000; and www.ncdoj.gov.