<<Date>> (Format: Month Day, Year)
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information that we have in our possession because you are an employee of College Park. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident. We are notifying you out of an abundance of caution since at this time we do not have any specific knowledge that your personal information has actually been compromised.

What happened?
We recently learned that on or about January 24, 2024 an unauthorized third-party accessed information on a server belonging to College Park. We engaged a cybersecurity and forensic consulting firm to investigate and assess the security incident and contain any further threats to College Park's systems, including any systems containing your information. Certain personally identifiable information ("PII") contained on our systems was impacted by the incident. At this time, we are not aware that this information has been published on any public websites, including on the dark web, or has otherwise been misused. Our internal teams continue to work diligently with their third-party cybersecurity consultants to further fortify College Park's systems, including implementing new technical safeguards, and updating policies and procedures.

What information was involved?
The information that may have been compromised potentially includes your first, middle, and last name, email address, physical address, date of birth, and social security number, and whether you opted into health, dental, or vision insurance. However, the compromised information did not include your financial account number, credit or debit card number, access code, password that would permit access to any of your financial accounts, or any healthcare information.

What we are doing:
Upon detecting the incident, and to mitigate any potential harm, we took action to secure the affected systems and contain the incident. We then notified other stakeholders, and, as noted above, retained a third-party cybersecurity and forensic consultant to investigate the nature and scope of the incident and secure the data environments. Additionally, we engaged a law firm to assist with notifying law enforcement, preparing regulatory notices, and notifying those who may have been impacted by this incident.

Further, at our expense, College Park would like to offer you a free one year subscription to Aura's Identity Defense Total, a credit monitoring and identity theft protection service. Identity Defense Total provides essential monitoring and protection of not only credit data, but also monitors the dark web and alerts you if your social security number, credit cards, and bank account numbers are found in unsecure online locations.

Identity Defense Total features include:

- Dark Web Monitoring
- High Risk Transaction Monitoring
- Customer Support & Victim Assistance
- 3-Bureau Credit Monitoring
- $1 Million Identity Theft Insurance*
- Monthly Credit Score
- Identity & Authentication Alerts
- Security Freeze Capability

If you wish to take advantage of this monitoring service, you must enroll by **August 20, 2024.**

To activate this coverage please visit the website listed below and enter the activation code. The activation code is required for enrollment and can only be used one time by the individual addressed.

Web Site: app.identitydefense.com/enrollment/activate/cpin
Activation Code: XXXXXXXXXXXXX

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Activation Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today.

Additionally, please see the insert attached with details on recommended steps to protect against identity fraud. It is essential to remain vigilant by monitoring your accounts and free credit reports.

If you have any further questions regarding this incident, please call College Park Monday through Friday at 800-728-7950 between the hours of 8:30 a.m. to 5:30 p.m., Eastern Time, or send a letter to 27955 College Park Drive, Warren, MI 48088.

Sincerely,
College Park Industries

_____

Bill Carver
President/Management Representative

*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to app.identitydefense.com/enrollment/activate/cpin and follow the instructions for enrollment using your Enrollment Code provided.

2. Activate the credit monitoring provided as part of your Aura identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, Aura will be able to assist you.

3. Telephone. Contact Aura at 1-844-939-3681 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in Aura's identity protection, notify them immediately by calling or by logging into the Aura's website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order 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 or to the Attorney General.

5. Place Fraud Alerts with one of the three credit bureaus listed below. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

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.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. Federal Reporting and Support. Please report suspected identity theft to local law enforcement and the Federal Trade Commission by visiting https://www.identitytheft.gov/. Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

8. For residents of the following states, please be aware of the following:

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Illinois Residents: Please be aware that six Illinois employees were affected by this incident. Please be vigilant and use the resources communicated throughout the letter.

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

New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Texas Residents: Please be aware that seven Texas employees were affected by this incident. All Texas employees affected have been provided notice, and asked to be vigilant and use the resources communicated throughout this letter.

Utah Residents: Please be aware that five Utah employees were affected by this incident. Please be vigilant and use the resources communicated throughout this letter.

Massachusetts Residents:
In order to request a security freeze, you will need to provide some or all of 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 in order 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, through 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 of time 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 of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.