[Date]
[First Name Last Name]
[Address]
[City, State Zip]

Dear [First Name]

Notification of Security Incident
Dynamark Monitoring, a Becklar, LLC company ("Dynamark", "we", and "us") takes the security and protection of your personal information seriously. We are providing you with this notice to make you aware of a security incident that may have resulted in the unauthorized access and download of your personal information.

What Happened
On Friday, September 26, 2025, Dynamark first discovered a security incident that impacted a limited number of its information resources (the "Incident"). Upon discovery of the Incident, Dynamark immediately terminated the unauthorized access and engaged a trusted third-party forensics firm ("Forensics") to assist in investigating the scope and impact of the Incident. Based on the investigation, Dynamark learned that the incident was made possible by an unauthorized third party leveraging a system exploit to gain certain access to Dynamark information resources. The unauthorized access began on September 26, 2025 and was terminated shortly after, upon discovery on the same date. Through its investigation, Dynamark learned that during this access period, the unauthorized third party accessed records relating to former and current employees, employment candidates, and a limited number of customers. Once aware of the Incident and its potential impact on personal information, we began analyzing the impacted files to better understand what information was potentially at risk. We have since worked with Forensics to secure all systems, remediate risks, and mitigate the risk of recurrence, which we did in very short fashion.

What Information Was involved
The unauthorized intruder accessed, viewed, and may have potentially downloaded the following categories of personal information: first and last name, mailing address, email address, telephone number, Social Security number, and payment card information. To date, Dynamark has received no reports of further misuse of any of this information. Because we understand that such access was possible during the period of access, we are providing notice and an offer of identity theft protection out of an abundance of caution so that you may safeguard against this vulnerability.

What We Did and What We Are Doing
Upon learning of the Incident, we immediately took protective measures to understand the Incident's scope and to secure our systems and data. We engaged Forensics to assist in conducting an internal investigation to verify the root cause, determine the scope of potentially accessed information, and remedy any existing identifiable security vulnerabilities. We continue to closely monitor our network and information systems for unusual activity, which we have seen no related activity of. We will continue to implement recommendations from Forensics to further enhance Dynamark's administrative, technical, and physical safeguards.

What You Can Do
We sincerely regret any concern or inconvenience the Incident causes you. Although we have not received reports or indication of any such activity, the risks related to unauthorized use of sensitive information, such as Social Security numbers or tax identification numbers, may include identity theft, financial fraud, and tax fraud. We encourage you to remain vigilant in reviewing activity on all accounts in which you keep sensitive information, including your credit files.

Please also take care when submitting tax returns to protect against possible fraudulent submissions made on your behalf. To assist you in this effort, we have provided complimentary credit monitoring and ID theft prevention services through TransUnion. You can access those benefits by following the instructions in the attached letter from TransUnion.

If you have concerns about identity theft, you can contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

For More Information
You can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit reporting agencies at one of the phone numbers listed below or visiting their respective websites.

Equifax PO Box 740241 Atlanta, GA 30374 800-525-6285 www.equifax.com	Experian PO Box 4500 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion PO Box 2000 Chester, PA 19016 877-322-8228 www.transunion.com

Steps You Can Take To Further Protect Your Information
Credit Reports. You can request credit reports be sent to you free of charge from all three credit bureaus. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Security Freeze. Under state law, a security freeze (or a credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. To place a security freeze, you may need to provide the following information:

1. Your full name;
2. Social Security number;
3. Date of birth;
4. Mobile number;
5. Current postal address;
6. Email address; and
7. Any other information that the credit bureau may require.

The credit bureaus have one business day after your request to place a security freeze if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three business days. The credit bureaus must also send written confirmation to you within five business days.

To lift the security freeze, in order to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) 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. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one hour. If you request the thaw by regular mail, the credit bureaus have three business days after receiving your request to lift the security freeze

for those identified entities or for the specified period of time.

Free Resources on Identity Theft. The Federal Trade Commission (FTC) provides more information about how to protect your identity at https://consumer.ftc.gov/identity-theft-and-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of *Identity Theft – A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

For District of Columbia Residents: You may also contact the Attorney General for the District of Columbia for more information about how to protect your identity by using the information below: Attorney General's Office 400 6th Street, NW Washington, DC 20001 Phone: (202) 727-3400 Website: https://oag.dc.gov/	For Maryland Residents: You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 200 St. Paul Place Baltimore, MD 21202 Phone: 410-528-8662 Website: https://www.marylandattorneygeneral.gov/
For New York Residents: You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Toll Free Phone Number: (800) 771-7755 Website: https://ag.ny.gov/	For North Carolina Residents: You may also contact the North Carolina Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Toll Free in NC: 1-877-566-7226 Outside NC: 919-716-6000 Website: https://ncdoj.gov/

Again, we sincerely regret that this Incident has occurred. If you have any questions, please contact us at:

Email: privacy@Dynamarkmonitoring.com
Telephone: 1-800-405-6108
Address: 525 Northern Ave., Hagerstown, MD 21742

Thank you for your continued support,

Rich Watts
VP of IT and Information Security
Becklar, LLC

CREDIT MONITORING SERVICES FROM TRANSUNION

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE> In** order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What if I want to speak with <OUR COMPANY> regarding this incident?

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

172367081v1