OK AS TO FORM
AMH 7-9-2026

DATA PRIVACY ADDENDUM - GOFAN

This Data Privacy Addendum ("**DPA**") is entered into by and between Wayne-Finger Lakes BOCES ("**Customer**") and Huddle Tickets, LLC, a Georgia limited liability company ("**Company**", and together with Customer, the "**Parties**" and each a "**Party**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the underlying Digital Tickets Sales Standard Terms and/or any applicable Order Forms (together, the "**Agreement**").

This DPA is an addendum to, and forms part of, the Agreement and sets out the terms that apply when Customer Personal Information (as defined below) is Processed by Company under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Information are Processed.

This DPA does not apply to Personal Information processed by Company in its role as a Controller of Personal Information obtained directly from end-users ("**Company Controller Data**"), including:

1. by browsing Company's websites and mobile applications,
2. by utilizing Company's underlying services,
3. by purchasing tickets, subscriptions, streaming events or other products from Company, or
4. otherwise by contacting Company or providing Personal Information directly to Company in a separate customer relationship.

Company Controller Data shall be Processed in accordance with the Company Privacy Policy located at https://gofan.co/privacy-policy.

DATA PROCESSING TERMS:

1 Definitions

1.1 Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1.2 For the purposes of this DPA the following words and phrases shall have the following meanings:

"Consumer" means a natural person or resident or "data subject" as the term is understood under Data Protection Laws and Regulations.

"Controller" shall mean the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Information;

"Customer Personal Information" means the Personal Information of Consumers provided directly by Customer to Company in connection with the performance of the Services under the Agreement;

"Data Protection Laws and Regulations" means all applicable federal and state laws and regulations binding on a Party with respect to the Party's processing, protection, or privacy of the Personal Information, including where applicable, binding guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. Data Protection Laws and Regulations includes, but is not limited to, the California Consumer Privacy Act of 2018, as amended and supplemented by the California Privacy Rights Act of 2020, as may be further amended from time to time, and their implementing regulations ("**CCPA**");

"Services" has the meaning set forth in the Agreement; and

"Business Purpose," "Processing", "Processed," "Process," "Personal Information," "Sell," "Service Provider," "Share," "Subcontractor" shall have the same meaning as those terms in the CCPA or other Data Protection Laws and Regulations.

2 Processing of Customer Personal Information

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Customer Personal Information as is necessary for providing the Services, Customer is the Controller, Company is the Service Provider.

2.2 **Data Minimization**. Customer recognizes and agrees that: (1) the Services generally do not involve substantial Processing of Customer Personal Information; and (2) Company generally does not expect to collect, store, or otherwise process Customer Personal Information in any substantial amount. Customer shall endeavor to, and shall train its personnel to, exercise all possible care in minimizing Company's access to or Processing of any Customer Personal Information to the extent solely and strictly necessary for the performance of the Services.

2.3 **Customer's Processing of Customer Personal Information.** Customer, as Controller, shall: (i) be responsible for ensuring that it has complied, and will continue to comply, with all applicable Data Protection Laws and Regulations; (ii) ensure it has, and will continue to have, the right to process, transfer, and/or provide access to, the Customer Personal Information to Company for Processing in accordance with the terms of the Agreement and this DPA; and (iii) have sole responsibility for the accuracy, quality, and legality of Customer Personal Information and the means by which Customer acquired Customer Personal Information.

2.4 **Company's Processing of Customer Personal Information**. Company shall treat Customer Personal Information as Confidential Information and shall Process Customer Personal Information on behalf of Customer as is necessary for providing the Services and only in accordance with Customer's documented instructions as set out in this DPA. Any Processing required outside of the scope of these instructions will require prior written agreement between the Parties. The Parties acknowledge and agree that Company's Processing of Customer Personal Information is as a Service Provider for a Business Purpose (i.e., performing services on behalf of Customer).

2.5 **Data Protection Impact Assessments**. Upon Customer's request and if required by applicable Data Protection Laws and Regulations, Company shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation to carry out a data protection impact assessment related to Customer's use of the Services.

3 Details of Data Processing.

3.1 **Categories of Consumers and Customer Personal Information**:

3.1.1 The Consumers whose Customer Personal Information may be Processed by Company under the Agreement include Consumers acting in an employment capacity on behalf of the Customer to initiate and facilitate the Agreement. Customer Personal Information Processed in this context includes identification and contact information (name, email, title).

3.1.2 In limited circumstances, such as in the instance of a restricted event offered via the GoFan Solution, Customer may provide minimal Customer Personal Information on a category of permissible attendees, including students, to Company for the legitimate interest of Company's provision of the Services. In this context, Customer shall provide only Customer Personal Information as is necessary for the Company to perform the

Services and which qualifies as Directory Information under the Family Educational Rights and Privacy Act of 1974, as amended, enacted as section 444 of the General Education Provisions Act. This may include a Student ID, provided solely for the purpose of a student's ability to access the GoFan Solution for purchase of an event ticket. Company agrees to:

(i) **Encrypt** the Student ID in flight and at rest using a secure, industry-standard encryption algorithm.

(ii) **Restrict Use of** the encrypted Student ID solely to:

(A) Verify eligibility to purchase an event ticket; and

(B) Facilitate the purchase of an event ticket.

In no event shall the Company's use of a Student ID allow access to educational records or otherwise identify a student.

3.2 **Retention Period.** In connection with the termination or expiration of the Agreement for any reason, Company will cease any and all Processing of Customer Personal Information which is not strictly necessary to enable Company to comply with any obligations under this DPA or the Agreement. Upon Customer's request, Company will return to Customer and/or securely destroy all Customer Personal Information within 30 calendar days of the end of the services relating to the Processing or within 30 calendar days of Customer's request, except to the extent that applicable legal requirements require storage of the Customer Personal Information, in which case Company will (a) to the extent legally permitted, inform Customer of the legal requirement and of the particular Customer Personal Information records that Company intends to retain, (b) not Process the Customer Personal Information for any purpose other than compliance with the applicable legal requirements, and (c) at the choice of Customer, return to Customer or securely destroy such Customer Personal Information as soon as practicable.

4 Company Personnel

4.1 **Confidentiality.** Company shall ensure that its personnel engaged in the Processing of Customer Personal Information are informed of the confidential nature of the Customer Personal Information, have received appropriate training on their responsibilities, and have executed written confidentiality agreements.

5 Subcontractors

5.1 **Use of subcontractors.** Customer acknowledges and agrees that: (i) Company's Affiliates may be retained as subcontractors, and (ii) Company and Company's Affiliates may engage third-party subcontractors in connection with the provision of the Services. If such subcontractors are engaged in the Processing of Customer Personal Information, Company shall ensure such subcontractors are informed of the confidential nature thereof and have executed written confidentiality terms.

5.2 **Liability**. Company shall be liable for its subcontractors to the same extent Company would be liable if performing the services of each subcontractor directly under the terms of this DPA.

6 Security

6.1 **Controls for the Protection of Customer Personal information.** Company shall maintain reasonable and appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer

Personal information), confidentiality and integrity of Customer Personal information in accordance with Appendix A Security Policy.

6.2 **Personnel.** Company shall take all reasonable steps to ensure the reliability of any Company personnel who may have access to, or are authorized to process, Customer Personal information. Company shall ensure that such Company personnel are bound by appropriate contractual confidentiality, data protection, and data security obligations in accordance with applicable Data Protection Laws and Regulations and this DPA.

6.3 **Compliance Monitoring.**

6.3.1 Upon Customer's reasonable request, Company shall make available to Customer all information in Company's possession necessary to demonstrate Company's compliance with its obligations under this DPA and Data Protection Laws and Regulations.

6.3.2 Upon written request, Customer may monitor Company's compliance with this DPA through regular assessments to be conducted in the form of a written questionnaire once per year.

7 CCPA Specific Provisions.

7.1 **Scope**. The following provisions apply to Customer Personal Information that is subject to the CCPA, or to any other Customer Personal Information to the extent required by other Data Protection Laws and Regulations. Company shall not:

7.1.1 Sell or Share Customer Personal Information or any other similar concepts defined in Data Protection Laws and Regulations except to perform the Business Purposes specified in this DPA and the Agreement;

7.1.2 Combine Customer Personal Information that Company receives from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a Consumer, except to perform the Business Purposes specified in this DPA and the Agreement;

7.1.3 Retain, use, or disclose Customer Personal Information that it receives from, or on behalf of, Customer for any purpose, including any commercial purpose, other than the Business Purposes specified in this DPA, the Agreement, or as otherwise permitted by the CCPA or outside of the direct business relationship between Customer and Company.

7.2 **Notification.** Upon determination by Company that it can no longer comply with CCPA or any Data Protection Laws and Regulations, Company shall notify Customer without undue delay.

7.3 **Certification.** Company certifies that it understands the restrictions set forth in this DPA and the CCPA and shall comply with these restrictions.

7.4 **Remediation.** Upon notice, Customer reserves the right to take reasonable and appropriate steps to stop and remediate Company's unauthorized use of Customer Personal Information.

8 Customer Personal information Incident Management and Notification

8.1 Company shall notify Customer without undue delay, and no later than 72 hours, after becoming aware of a confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Information (a "**Customer Personal Information Incident**").

8.2 To assist Customer in relation to any personal data breach notifications Customer is required to make under the Data Protection Laws and Regulations, Company shall include in the notification such information about the Customer Personal Information Incident as is required by such Data Protection Laws and Regulations, to the extent that such information is reasonably available to Company and shall take all reasonable and necessary steps to remediate the cause of such Customer Personal Information Incident, to minimize further Customer Personal Information Incidents. Where and insofar as Company cannot provide all the information relevant to a Customer Personal Information Incident at the same time, it may provide such information in phases without undue further delay.

9 General Provisions

9.1 Except as amended by this DPA, the Agreement will remain in full force and effect.

9.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

9.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

9.4 This DPA will automatically terminate on the termination or expiry of the Agreement.

9.5 This DPA shall only become legally binding between Customer and Company when the Parties have executed below.

Appendix A
Security Policy

This Security Policy ("**Security Policy**") outlines particular administrative, logical, technical and security requirements ("**Security Requirements**") that Company shall maintain to protect the availability, confidentiality and integrity of all Company systems, applications, and platforms ("**Company Network**"). Any capitalized terms used but not defined herein shall have the meaning set forth in the applicable DPA. In the event of any conflict between the terms of the DPA and this Security Policy, this Security Policy shall govern.

1. Access Controls

1.1. Authentication

Overview. Company requires authentication for access to all application pages on the Company Network, except for those intended to be public.

Secure Communication of Credentials. Company currently uses TLS-encrypted requests to transmit authentication credentials to the Company Network.

Password Management. Company has processes designed to enforce minimum password requirements for the Company Network. Company currently enforces the following requirements and security standards for end user passwords on the Company Network:

- Passwords must be a minimum of 8 characters in length and include a mix of uppercase and lowercase letters as well as numbers and symbols;
- Multiple logins with the wrong username or password will result in a locked account, which will be disabled for a period of time to help prevent a brute-force login, but not long enough to prevent legitimate users from being unable to use the application;
- Email-based password reset links are sent only to a user's pre-registered email address with a temporary link;
- Company rate limits multiple login attempts from the same email address; and
- Company prevents reuse of recently-used passwords.

Password Hashing. User account passwords stored on the Company Network are hashed with a random salt using industry-standard techniques.

Single Sign-On. In some instances, Security Assertion Markup Language (SAML) Single Sign-On (SSO) may be implemented through Company's SSO provider.

1.2. Session Management

Overview. Each time a user signs into the Company Network, the system assigns them a new, unique session identifier, currently consisting of 64 bytes of random data designed for protection against brute forcing.

Session Timeout. All sessions are designed to have a hard timeout. SSO sessions are configured with an inactivity timeout. There is an optional setting to terminate any sessions after 10 minutes of inactivity.

Sign Out. When signing out of the Company Network, the system is designed to delete the session cookie from the client and to invalidate the session identifier on Company servers.

2. Network and Transmission Controls

Company monitors and updates its communication technologies periodically with the goal of providing network security.

2.1. TLS and AES

Company encrypts all data at rest and in transit. Data is stored in AWS RDS and encrypted with custom keys from AWS KMS. All database connections use TLS. HSTS is used to ensure browsers' encryption of communication.

2.2. Network Security

Company regularly updates network architecture schema and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

2.3. Infrastructure Security

Company uses an Intrusion Detection System (IDS) and Endpoint Detection and Response (EDR), and other security monitoring tools on the production servers hosting the Company Network.

3. Data Confidentiality and Job Controls

3.1. Internal Access to Data

Access to customer data is restricted within Company to employees and contractors who have a need to know this information to perform their job function, for example, to provide customer support or to maintain infrastructure.

Company currently requires the use of SSO, strong passwords and/or 2-factor authentication for all employees to access production servers for the Company Network.

3.2. Job Controls

Company has implemented several employee job controls to help protect the information stored on the Company Network:

- All Company employees are required to sign confidentiality agreements prior to accessing Company's production systems;
- All Company employees are required to receive security and privacy training at time of hire, as well as quarterly security and/or privacy awareness training;
- Employee access to production systems that contain your data is logged and audited;
- Company employees are subject to disciplinary action, including but not limited to termination, if they are found to have abused their access to customer data; and
- Company employees are subject to background check prior to employment, where permitted by law.

4. Security in Engineering

4.1. Product Security Overview

The engineering process for the Company services follows industry-standard code development processes designed to ensure security at the product development and engineering levels. All changes to servers and infrastructure are implemented as code using industry standard tools and undergo the systems development lifecycle process as changes to the software.

4.2. Code Assessments

The software Company develops for the Company Network is continually monitored and tested using processes designed to proactively identify and remediate vulnerabilities. Company regularly conducts:

- Source code analysis designed to find common defects;
- Peer review of all code prior to being pushed to production;
- Manual source code analysis on security-sensitive areas of code; and
- Third-party application security assessments and penetration tests.

5. Availability Controls

5.1. Disaster Recovery

The infrastructure for the Company Network is designed to minimize service interruption due to hardware failure, natural disaster, or other catastrophes. Features include:

- ***Cloud providers:*** Company currently uses Amazon Web Company Network, which is trusted by thousands of enterprises to store and serve their data and services.
- ***Data replication:*** To help ensure availability in the event of a disaster, the cloud provider replicates data across multiple data centers.
- ***Backups****:* Company's cloud provider performs daily, weekly, and monthly backups of data stored on the Company Network.

5.2. Incident Response

Company has an incident response plan designed to promptly and systematically respond to security and availability incidents that may arise. The incident response plan is tested and refined on a regular basis.

6. Segregation Controls

6.1. Data Segregation

The Company Network is designed to logically separate each customers' data from that of other customers. Company's application logic is designed to enforce this segmentation by permitting each end user access only to accounts that the user has been granted access to.

6.2. User Roles

User roles specify different levels of permissions that the customer can use to manage the users on the Company Network account. Customer can invite users to customer's Company account without giving all team members the same levels of permissions.

7. Physical Security

Company uses a third party cloud platform (currently Amazon Web Company Network ("**AWS**")) to host its production systems for the Company Network. Access to AWS's data centers is limited to authorized

personnel only, as verified by biometric identity verification measures. Physical security measures for AWS data centers include: on-premises security guards, closed circuit video monitoring, and additional intrusion protection measures. Company relies on their third party attestations of their physical security. Within Company's physical office, Company employs a number of industry-standard physical security controls.

8. Patch and Vulnerability Management

Vulnerabilities meeting risk criteria defined by Company trigger alerts and are prioritized for remediation based on their potential impact to the Company Network. Upon becoming aware of such vulnerabilities, Company will use commercially reasonable efforts to address any vulnerabilities within a reasonable timeframe. Vulnerabilities which Company deems to be critical in nature will be remediated or mitigated within 30 days. Regardless of severity, Company remediates or mitigates all vulnerabilities within 90 days.

Digital Ticketing Proposal

3-Year

School Name *

School Address *

Street Address

City

State

Please Select

Zip Code

Primary Contact *

First Name

Last Name

Primary Contact Email *

example@example.com

Primary Contact Title *

Primary Contact Role *

Primary Contact Phone Number *

Area Code - Phone Number

Primary Contact Mobile Number *

Area Code - Phone Number

Financial Contact *

First Name Last Name

Financial Contact Email *

example@example.com

Financial Contact Phone Number

Area Code - Phone Number

Date of first event you plan to host on GoFan *

mm-dd-yyyy

Date

GoFan Order Form

Term

- July 1, 2026 - June 30, 2029
- School option for annual renewal

Digital Ticket Sales

- Custom school ticketing page to be used for athletics, performing arts and/or additional school events.
    - Online Ticket Sales
    - Season Ticket Sales

- Onsite Ticket Sales (Box Office)

Event Reporting

- Real-time online ticket sales status
- Post event digital ticket sales
- Automated for financial tracking and reconciliation

Financial Management

- Regular, electronic transfer of funds (Check Payment Available)
- Full documented support for refunds, cancellations and event disruption

Support

- Full on-boarding and training content
- Access to growing base of user knowledge to share best practices
- Dedicated account management resource(s)

Ticket Fees

Type	Fee
General Admission Tickets ($10.00 or less)	$1.00 (Per Ticket)
General Admission Tickets ($10.01 or more)	5% + $1.00 (Per Ticket)
Season Tickets / Passes	5% + $2.00 (Per Ticket or Pass)
Concessions	3% + $0.30 (Per Transaction)
Reserved Seating (Single Event)	5% + $1.00 (Per Ticket)
Donations ($10.00 or less)	$1.00 (Per Donation)
Donations ($10.01 or more)	5% + $1.00 (Per Donation)
Playoff Events	*Rates may vary depending on your state.

Sponsorship Revenue Share

- Generate more revenue for your school
- High impact opportunities for sponsors
- GoFan will secure a sponsor for you
- FAQ & See Examples
- Standard Terms and Conditions

I agree to Standard GoFan Sponsorship Terms & Conditions *

Please Select

Please list the name of at least one business to which you would like us to offer this special, exclusive opportunity

Date *

05-26-2026

GoFan Standard Terms & Conditions

☐ I agree to the Standard Terms & Conditions and GoFan Privacy Policy. *

SUBMIT

playon
There for Every Moment

2080MED-01 VIKUMAR

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 3/12/2026

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
Aon Risk Services Northeast, Inc. One Liberty Plaza 165 Broadway, Suite 3201 New York, NY 10006	PHONE (A/C, No, Ext):	FAX (A/C, No):
	E-MAIL ADDRESS:	

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Hartford Underwriters Insurance Company	30104
INSURER B : Trumbull Insurance Company	27120
INSURER C : Hartford Casualty Insurance Co	29424
INSURER D : Twin City Fire Insurance Company	29459
INSURER E :	
INSURER F :	

INSURED

2080 Media Inc.
2990 Brandywine Road
Atlanta, GA 30341

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	$ 1,000,000
	[ ] CLAIMS-MADE [X] OCCUR	X		10UUNBD3RC6	8/1/2025	8/1/2026	DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 3,000,000
	X POLICY [ ] PRO-JECT [ ] LOC						PRODUCTS - COMP/OP AGG	$ 3,000,000
	OTHER:							$
B	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	X ANY AUTO			10UENBN7VMV	8/1/2025	8/1/2026	BODILY INJURY (Per person)	$
	[ ] OWNED AUTOS ONLY [ ] SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	[ ] HIRED AUTOS ONLY [ ] NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
							Coll./Comp Ded.	$ 1,000
C	X UMBRELLA LIAB X OCCUR						EACH OCCURRENCE	$ 10,000,000
	[ ] EXCESS LIAB [ ] CLAIMS-MADE			10RHUBF2FW0	8/1/2025	8/1/2026	AGGREGATE	$ 10,000,000
	[ ] DED X RETENTION $ 10,000							$
D	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N						X PER STATUTE [ ] OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) N	N/A		10WEAN1KCY	8/1/2025	8/1/2026	E.L. EACH ACCIDENT	$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Certificate Holder is included as Additional Insured in accordance with the policy provisions of the General Liability policy.

CERTIFICATE HOLDER

Board of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville, KY 40218

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services Northeast Inc.

AGENCY CUSTOMER ID: 2080MED-01 VIKUMAR

LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Aon Risk Services Northeast, Inc.	2080 Media Inc. 2990 Brandywine Road Atlanta, GA 30341
POLICY NUMBER SEE PAGE 1	
CARRIER: SEE PAGE 1 / NAIC CODE: SEE P 1	EFFECTIVE DATE: SEE PAGE 1

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

Cyber Liability
Policy Number: C4LQ7018566CYBER2025
Policy Period: 11/15/2025 to 11/15/2026
Insurer: Fortegra Specialty Insurance Company
Aggregate Limit: $10,000,000 (Claims Made)
SIR: $100,000. (SIR applies per policy terms & conditions)

E&O Technology
Policy Number: 596862634
Policy Period: 11/15/2025 to 11/15/2026
Insurer: Continental Casualty Company
Aggregate Limit: $10,000,000 (Claims Made)
SIR: $100,000. (SIR applies per policy terms & conditions)